



SECUROS

Version 10

Administration Guide

SecurOS Administration Guide (AG - EN, build 49 on 17.12.2019).

© Copyright Intelligent Security Systems, 2019.

Printed in US.

Intelligent Security Systems reserves the right to make changes to both this Manual and to the products it describes. System specifications are subject to change without notice. Nothing contained within this Manual is intended as any offer, warranty, promise or contractual condition, and must not be taken as such.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any human or computer language in any form by any means without the express written permission of the copyright holder. Unauthorized copying of this publication may not only infringe copyright but also reduce the ability of Intelligent Security Systems to provide accurate and up-to-date information to both users and operators.

Contents

1 Preface	11
1.1 Scope	11
1.2 Target Audience	11
1.3 Using This Manual	11
1.4 Getting Technical Support	11
1.5 SecurOS Editions Naming Convention	13
1.6 Design Convention	13
1.7 Design Elements	14
2 Purpose, Implementation And Operation Principles	15
2.1 SecurOS Architecture	15
2.1.1 Types Of Servers And Workstations	15
2.1.1.1 Classification by Functionality	15
2.1.1.1.1 Video Server	15
2.1.1.1.2 Operator Workstation	16
2.1.1.2 Classification of Roles in Configuration Management	16
2.1.1.2.1 Configuration Server	16
2.1.1.2.2 Managing Network Configuration by Configuration Server	16
2.1.1.2.2.1 How To Configure Servers When Deploying Network	16
2.1.1.2.2.2 Configuration Update Procedure	17
2.1.1.2.2.3 Restoring Configuration from Backup Copy	17
2.1.2 Software Implementation	17
2.2 Software And Hardware Platform	18
2.2.1 Video Server System Requirements	18
2.2.2 Operator Workstation System Requirements	19
2.2.3 Audio Subsystem Requirements	20
2.2.4 Notification Subsystem Requirements	20
2.2.5 ACS Requirements	20
2.2.6 Environment Requirements	20
2.2.6.1 Computer Name Restrictions	20
2.3 SecurOS' Subsystems	21
3 SecurOS Installation and Update	22
3.1 Installing, Configuring and Launching Configuration Server	22
3.1.1 Hardware Installation	22
3.1.1.1 Guardant Key Installation	23
3.1.1.2 Installing Guardant Key in Manual Mode	23
3.1.2 License Key	23
3.1.2.1 The Key is a part of a product	24
3.1.2.2 Request the key by e-mail	24
3.1.3 Software Installation	25
3.1.3.1 Using Current Parameters of the Windows User Account needed for PostgreSQL	25
3.1.3.2 Using Current Parameters of the Database and Administrator User Account	26
3.1.3.3 Software Installation On The Configuration Server	27
3.1.4 Initial Configuration	34
3.1.4.1 Initial Configuration Using The System Configuration Wizard	34
3.1.4.2 Restoring Configuration	42
3.1.4.3 Start with Empty Database	42
3.1.5 Launching SecurOS On The Configuration Server	42

3.2 Installing, Configuring And Launching Peripheral Servers.....	44
3.2.1 Adding To The Network And Configuring Peripheral Servers.....	45
3.2.2 SecurOS Installation On Peripheral Servers.....	46
3.2.3 Launching And Configuring SecurOS On Peripheral Servers.....	47
3.3 Installing, Configuring and Launching Operator Workstations	48
3.3.1 SecurOS Installation On Operator Workstation	49
3.3.2 Operator Workstation Profiles	50
3.3.2.1 Use Restrictions	50
3.3.2.2 Creating Operator Workstation Profile.....	50
3.3.3 Fixed Operator Workstations.....	51
3.3.3.1 Adding To The Network And Configuring Fixed Operator Workstations.....	51
3.3.3.4 Launching SecurOS On Operator Workstation.....	52
3.4 Installing Additional Multimedia Components	54
3.5 SecurOS Update Order	54
4 SecurOS Administration Overview	55
4.1 Working With Control Panel	55
4.1.1 Control Panel Activation, Configuring and Hiding	56
4.1.2 Opening and Closing Administration Center.....	57
4.1.3 Changing Operator Workspace	59
4.1.4 User Session Administration and Client Shutdown.....	59
4.1.5 System Shutdown.....	60
4.1.6 Getting Help.....	60
4.2 Administration Center	62
4.2.1 Working with Objects	63
4.2.1.1 Creating Objects	65
4.2.1.2 Editing Object Settings	65
4.2.1.3 Deleting Objects	65
4.2.1.4 Disabling/Enabling Objects	66
4.2.1.5 Renaming Objects	66
4.2.1.6 Searching Objects.....	66
4.2.2 Working with Object Table Parameters	68
4.2.3 IP-Device Manager	68
4.2.3.1 Specification	69
4.2.3.2 Basic Operations.....	72
4.2.3.2.1 Launching IP-Device Manager	72
4.2.3.2.2 Searching Devices in the Network.....	73
4.2.3.2.3 Adding IP Device.....	74
4.2.3.2.4 Editing IP Device Parameters	76
4.2.3.2.5 Copying IP Device.....	76
4.2.3.2.6 Deleting IP Device.....	78
4.3 Users and Rights	78
4.3.1 SecurOS Users	78
4.3.1.1 Changing Superuser Password	79
4.3.2 User Registration and Configuring User Rights	80
4.3.3 Configuration of Network Domain User Rights	85
4.3.3.1 Settings for Windows NT Provider	85
4.3.3.2 Settings for LDAP Provider	85
4.4 SecurOS Logging.....	86
4.5 Updating License Key on All Servers.....	86
4.5.1 License Expiration Reminder.....	87
4.6 Health Monitor self-diagnostic Module	88
4.6.1 Video Server	94
4.6.2 Camera.....	100
4.6.3 Microphone	102

4.6.4 Sensor	102
4.6.5 Remote System	103
4.6.6 Concentrator	103
4.7 SecurOS Files Synchronization	103
5 Core Subsystem	105
5.1 Working Principles	105
5.2 Object Reference	105
5.2.1 System	106
5.2.2 Security Zone	108
5.2.2.1 General Tab	109
5.2.2.2 Servers to Connect Tab	110
5.2.2.3 Connection Restrictions Tab	112
5.2.3 Database	113
5.2.4 Department	115
5.2.5 User Account	116
5.2.6 Active Directory / LDAP	117
5.2.7 User Rights	118
5.2.8 Computer	122
5.2.8.1 Archive	125
5.2.8.2 Auto login	130
5.2.9 Event Filter	130
5.2.10 SNMP agent	133
5.2.10.1 Setting up Windows Management and Monitoring Tools	134
5.2.11 External application	135
5.2.12 Databases Replicator	136
6 Interface Subsystem	138
6.1 Object Reference	138
6.1.1 Desktop	138
6.1.1.1 Desktop Setup Operations	140
6.1.2 Map	145
6.1.2.1 Maps Working Principles	147
6.1.2.2 Drawing Map Layers	147
6.1.2.3 Working with Map Layers	148
6.1.2.4 Working with Objects	150
6.1.3 Map Window	152
6.1.4 Event Viewer	153
6.1.5 External Window	155
6.1.6 HTML Form	156
6.1.7 HTML5 FrontEnd	157
7 Video Subsystem	160
7.1 Hardware Decoding	160
7.1.1 Setting up Hardware Decoding	163
7.2 Multi-streaming	164
7.3 Frame Rate Reduction	164
7.4 Working Principles of Motion Detection Zones	165
7.4.1 Creating Zones	165
7.5 SecurOS Archives	165
7.6 Camera Local Storage (Edge Storage)	166
7.6.1 System Requirements to Provide Edge Storage Use	166
7.6.2 Configuring System to Use Edge Storage	167
7.7 Special Settings for Video Subsystem Components	170

7.7.1 Camera Image Control	170
7.7.2 Archive Recording.	170
7.7.2.1 Disk Volume Settings.	170
7.7.2.2 Video Recording Settings.	170
7.8 Object Reference	171
7.8.1 System Objects	171
7.8.1.1 Video Capture Device	172
7.8.1.1.1 AC Recorder	176
7.8.1.2 Camera	176
7.8.1.2.1 General Tab	177
7.8.1.2.2 Stream Tab	179
7.8.1.2.3 Recording Tab.	183
7.8.1.2.4 Audio Tab	186
7.8.1.2.5 Detectors Tab.	187
7.8.1.2.6 PTZ Tab	189
7.8.1.2.7 Advanced Tab.	191
7.8.1.2.8 Multicast	197
7.8.1.2.9 Configuring Panoramic Cameras.	198
7.8.1.3 Defocus detector	199
7.8.1.3.1 Fine Tuning Recommendations.	201
7.8.1.4 Layout	202
7.8.1.5 View	204
7.8.1.6 Zone	204
7.8.1.7 Light Detector	208
7.8.1.8 Archive Converter	209
7.8.1.8.1 Digital Signature	217
7.8.1.8.2 Displaying Subtitles in Exported Video	217
7.8.1.9 Archive Export Profile	218
7.8.1.10 Archiver	218
7.8.1.11 Image Processor	224
7.8.1.12 RTSP Server	224
7.8.1.13 ONVIF Server	226
7.8.1.14 EdgeStorage Sync.	227
7.8.1.15 EdgeStorage Gate.	227
7.8.2 User Interface Objects.	228
7.8.2.1 Media Client	228
7.8.2.1.1 Display options Tab.	229
7.8.2.1.2 Layouts Tab.	234
7.8.2.1.3 Views Tab	237
7.8.2.1.4 Cameras Tab.	239
7.8.2.1.5 Archive export Tab.	242
7.8.2.1.6 Audio Tab	244
7.8.2.1.7 About Views	245
7.8.2.1.8 Working with Views.	246
7.8.2.1.8.1 Creating View	248
7.8.2.1.8.2 Editing View	248
7.8.2.1.8.3 Renaming View.	249
7.8.2.1.8.4 Deleting View	249
7.9 Configuration Examples	250
7.9.1 Standalone Configuration.	250
7.9.2 Video Server and Operator Workstations	251
7.9.3 Setting Up Camera	252
7.9.3.1 Adding Video Capture Device	252
7.9.3.2 Adding Camera to System.	253
7.9.3.3 Selecting Camera to Work with Media Client.	254
7.9.3.4 Adding User Rights	256
7.9.3.5 Setting up telemetry.	258
7.9.3.5.1 Setting up telemetry for IP devices	258

7.9.3.5.1.1 Shared Telemetry Control	260
7.9.3.5.1.2 Exclusive Telemetry Control	260
7.9.4 Joystick Configuration	261
8 Audio Subsystem	263
8.1 Operation Modes	263
8.1.1 Synchronized Audio/Video Recording and Playback	263
8.1.2 Separate Audio Recording and Playback	263
8.2 Object Reference	264
8.2.1 Audio Capture Device	264
8.2.2 Microphone	266
8.3 Example of System Configuration for Synchronized Audio/Video Recording and Playback	268
9 I/O Subsystem	269
9.1 Object Reference	269
9.1.1 Sensor	269
9.1.2 Relay	271
9.1.3 CCTV Keyboard or joystick	272
9.1.3.1 Bosch Intuikey	272
9.1.3.2 Hikvision DS-1100KI	276
9.1.3.3 Panasonic WV-CU950	277
9.1.3.4 Pelco KBD300A	278
9.2 Configuring System to Work with Wiper	279
10 Notification Subsystem	280
10.1 Object Reference	280
10.1.1 HTML Dialog	280
10.1.2 E-mail Message Service	282
10.1.3 E-mail Message	283
10.1.4 Short Message Service	285
10.1.5 Short Message	285
10.1.6 Audible Notification Service	286
10.1.7 Emergency service	287
10.1.7.1 Incident Types List. File Format	290
11 Automation Subsystem	293
11.1 Object Reference	293
11.1.1 Schedule	293
11.1.2 Macro	296
11.1.3 VB/JScript program	297
11.1.4 IIDK Interface	299
11.1.5 HTTP Event Gate	300
11.1.6 REST API	301
11.2 Setting up Macros and Scripts	302
11.2.1 Macros	302
11.2.2 VB/JScript programs	303
12 Computer Vision	304
12.1 General Recommendations on Camera Configuration and Location	304
12.2 Tracking Kit III Plugin	305
12.2.1 Configuring Plugin and Video Analytics Detectors	305
12.2.1.1 Configuring Tracking Kit III Plugin	305
12.2.1.1.1 Scene Tab	308

12.2.1.1.2 Tracker Tab	313
12.2.1.1.3 Classification Tab	314
12.2.1.2 Configuring Video Analytics Detectors	315
12.2.1.2.1 Configuring Controlled Zone	317
12.2.1.2.2 Running Detector	322
12.2.1.2.3 Left Behind and Removed Object Detector	324
12.2.1.2.4 Loitering Detector	326
12.2.1.2.5 Intrusion Detector	328
12.2.1.2.6 Crowd Detector	329
12.2.1.2.7 Object Counter	331
12.2.1.2.8 Line Crossing Detector	333
12.2.1.2.9 Dwell Time Detector	334
12.2.1.2.10 Wrong Direction Detector	336
12.2.2 Representation of video analytics detector operation results	338
12.3 Smoke Detector	339
12.3.1 Recommendations on Camera Configuration for Smoke Detector	340
13 Monitoring & Control Center	341
13.1 Direct Connection	345
13.1.1 Limitations	345
13.1.2 Setting Up Direct Connection	345
13.1.2.1 Remote System	347
13.1.2.3 Setting Up to Work with SecurOS Auto	349
13.2 VC/VR-connection	351
13.2.1 Setting Up VC/VR-connection	352
13.2.1.1 Remote System	354
13.2.1.2 Monitoring Center Agent	355
14 Redundancy	357
14.1 Failover Cluster	357
14.1.1 Cluster Structure	357
14.1.1.1 Cluster Configuration	358
14.1.1.2 Cluster Operation. Quorum	358
14.1.1.3 Recommendations	359
14.1.2 Configuring Cluster	359
14.1.2.1 Creating Cluster	360
14.1.2.1.1 Creating Cluster in Existing SecurOS Configuration	361
14.1.2.1.2 Creating Cluster and SecurOS Configuration From the Scratch	361
14.1.2.2 Getting Current Cluster Configuration	361
14.1.2.3 Creating Security Zone	362
14.1.2.4 Adding Host	363
14.1.2.5 Removing Host	363
14.1.2.6 Switching to Video Server Mode	364
14.1.2.7 Adding Node	364
14.1.2.8 Removing Node	365
14.1.2.9 Getting Node List	365
14.1.2.10 Setting Preferred Host for the Node	365
14.1.2.11 Moving Node to the Host Manually	366
14.1.2.12 Recreating Cluster	366
14.1.2.13 Restoring SecurOS Configuration from File	367
14.1.2.14 Setting Configuration Server	367
14.1.2.15 Converting Independent Video Server to Cluster Node	367
14.1.2.16 Service mode	368
14.1.2.17 Changing Network Interface for Virtual IP Addresses	368
14.1.3 Connecting Operator Workstations to the Cluster Servers	369
14.1.4 Storing Data in Cluster	369
14.1.4.1 iSCSI Drive	370

14.1.4.2 Using iSCSI Drive for Storing Video Archive	371
14.1.4.3 Movable PostgreSQL.....	371
14.1.4.4 Storing Video Archive on the Host's Local Drives.....	372
14.1.5 Cluster Creating and Setting Up Examples.....	373
14.1.5.1 Creating Cluster and SecurOS Configuration From the Scratch. Example.....	373
14.1.5.1.1 Task	374
14.1.5.1.2 Requirements	374
14.1.5.1.3 Computers Parameters.....	374
14.1.5.1.4 Steps	375
14.1.5.2 Creating Cluster in Existing SecurOS Configuration. Example.....	376
14.1.5.2.1 Task	376
14.1.5.2.2 Requirements	376
14.1.5.2.3 Computers Parameters.....	376
14.1.5.2.4 Steps	377
14.1.6 Resolving Common Issues.....	378
14.1.6.1 Quorum Loss.....	378
14.1.6.2 Restoring Operating System from Backup.....	378
14.1.6.3 Unable to Connect Operator Workstation.....	379
14.1.6.4 Updating Software and Hardware within Cluster System.....	379
14.1.7 Limitations.....	379
14.2 Redundant Servers Cluster.....	380
14.2.1 Creating Configuration on the Base of Redundant Servers Cluster	380
14.2.2 Adding Computer to the Redundant Servers Cluster.....	381
14.2.3 Creating "1+1" Cluster from Existing SecurOS Configuration. Example.....	381
14.2.3.1 Task	381
14.2.3.2 Computers Parameters.....	381
14.2.3.3 Steps	382
15 Interaction with External Systems	383
15.1 Interaction with External Emergency Service.....	383
16 Light Integration	386
16.1 General Description.....	386
16.2 Integration Point.....	387
16.3 SecurOS Integrations.....	388
16.3.1 Bolid.....	388
16.3.2 FortNet.....	389
17 Keyboard Shortcuts	391
17.1 Administration Toolbar	391
18 Appendixes	392
18.1 Appendix A. Upgrading/Uninstalling Software.....	392
18.1.1 Upgrading Software	392
18.1.2 Uninstalling Software	392
18.1.3 SecurOS Version Upgrade Features	393
18.1.3.1 Release 9.3 and Earlier Updating Procedure	394
18.1.3.2 Release 9.6 and Earlier Updating Procedure	395
18.1.3.3 Release 10.0 and Earlier Updating Procedure	395
18.1.3.4 Release 10.1 and Earlier Updating Procedure	395
18.1.3.5 Release 10.2 and Earlier Updating Procedure	396
18.1.3.6 Release 10.3 and Earlier Updating Procedure	396
18.2 Appendix B. Quick Video Subsystem Configuration	397
18.3 Appendix C. System Utilities	398

18.3.1 SecurOS Server Manager Utility.....	398
18.3.1.1 Control Toolbar	400
18.3.1.1.1 Working with Host List.....	400
18.3.1.1.2 Managing Cluster.....	401
18.3.1.1.3 Managing Video Server State	402
18.3.1.1.4 Connecting to Host for Configuring	402
18.3.1.1.5 Restoring SecurOS Configuration.....	402
18.3.1.1.6 Managing Nodes.....	403
18.3.1.1.7 Advanced Cluster Host Settings	403
18.3.1.1.8 Search String.....	405
18.3.1.2 Hosts Table.....	405
18.3.2 ISS Hardware Report Utility	407
18.3.3 ISS System Report Utility (ISSInfo).....	407
18.3.4 ISS Media Export Utility	410
18.3.4.1 Export Settings dialog	412
18.3.4.2 Command-line parameters.....	413
18.3.5 DSAdmin Utility.....	416
18.3.6 Database Update Utility.....	420
18.3.7 ISS SecurOS Registration Files Editor.....	422
18.3.8 ISS Server Role Manager Utility.....	427
18.3.9 Server Control Agent Utility	428
18.3.10 Video Archive Index Repair Utility	430
18.3.11 Outdated Audio Archive Updater Utility.....	431
18.3.12 Certificate Generator Utility	433
18.3.13 AuditClient Utility.....	434
18.3.13.1 Configuring Result Table	440
18.3.13.2 User Actions Analysis Example.....	441
18.4 Appendix D. TCP/IP Ports Used by SecurOS.....	442
18.5 Appendix E. Additional Windows Settings	444
18.5.1 Installing Multimedia Components and Services under MS Windows Server 2008 R2	444
18.5.2 Installing Media Foundation under MS Windows Server 2012 R2.....	444
18.5.3 SMTP Mail Server Installation and Configuration.....	445
18.5.4 Disabling Disk Cleanup Master	448
18.6 Appendix F. Error Messages When Launching System.....	448
18.7 Appendix G. Technical Support Information.....	449
Index	451

1 Preface

This section contains general information about this document, the means of its design and use, as well as how to get additional technical support for the product.

1.1 Scope

This manual provides general information about the SecurOS architecture, describes the process of configuring a security network and system objects, and gives some troubleshooting tips and recommendations.

It is assumed that the user has already physically deployed the security network and installed the SecurOS software on all computers of this network.

1.2 Target Audience

This manual is designed for SecurOS system installers and administrators. It is assumed the user has advanced computer skills, has practical experience with TCP/IP networking, serial (COM) ports and general CCTV knowledge.

1.3 Using This Manual

This document is organized in such a way that the user can use both its printed and electronic versions. In the latter case one can use Adobe Reader's Bookmarks feature as well as cross-reference hyperlinks to navigate through content. In several topics this manual refers to other SecurOS manuals (for example, [SecurOS Quick User Guide](#) etc.). One can find these manuals as separate files on the SecurOS installation CD or download them from our website (www.issivs.com).

To get online help (Microsoft HTML Help) just press the **F1** key when running SecurOS in administrative mode. You can get context help for a given object by pressing the **F1** key when its settings window is open.

1.4 Getting Technical Support

If you have any questions after reading this manual, please address them to your system administrator or supervisor.

For any further information you can contact the Intelligent Security Systems Technical Support Team:

Note. To get a quick response to a request use the Technical Support Portal, which www address is listed below.

- **in USA:**

phone: +1 732 855 1111 (Monday to Friday, 8:30am - 6pm EST);
e-mail: support@issivs.com
www: <https://support.issivs.com>

- **in Russia:**

phone: +7 (495) 645 21 21 (Monday to Thursday, 9am - 6pm MST; Friday 9am - 5pm MST);
e-mail: support@iss.ru
www: <https://help.iss.ru>

Note. See the <https://help.iss.ru/user/manual> for the Portal User Guide.

- **in Brazil:**

phone: +55 11 2262 2894 (Monday to Friday, 9am - 6pm BRT);
e-mail: suporte@issivs.com
www: <https://support.issivs.com>

- **in Mexico:**

phone: +52 1 551330 0181 (Monday to Friday, 9am - 6pm CDT);
e-mail: supportlatam@issivs.com
www: <https://support.issivs.com>

- **in Colombia/Ecuador:**

phone: +57 300 442 2808 (Monday to Friday, 9am - 6pm COT/ECT);
e-mail: supportlatam@issivs.com
www: <https://support.issivs.com>

- **in Chile:**

phone: +56 9 6573 2993 (Monday to Friday, 9am - 6pm CLT);
e-mail: supportlatam@issivs.com
www: <https://support.issivs.com>

- **in Ukraine:**

phone: +380 (44) 299 08 10 (Monday to Friday, 9am - 6pm EET);
e-mail: supportua@issivs.com
www: <https://support.issivs.com>

- **in Peru/Bolivia:**

phone: +51 997 111 678 (Monday to Friday, 9am - 6pm PET/BOT);
e-mail: supportlatam@issivs.com
www: <https://support.issivs.com>

- **in Argentina:**

phone: +54 91152528779 (Monday to Friday, 9am - 6pm ART);
e-mail: supportlatam@issivs.com
www: <https://support.issivs.com>

To solve problems faster, we recommend preparing the service information described in the **Technical Support Information** Section before addressing the Technical Support Team.

1.5 SecurOS Editions Naming Convention

This document represents a common manual for several editions of the "SecurOS integrated video management platform" that differ in functional capabilities:

- *SecurOS Monitoring & Control Center;*
- *SecurOS Enterprise;*
- *SecurOS Premium;*
- *SecurOS Professional;*
- *SecurOS Xpress;*
- *SecurOS Lite.*

For product designation regardless of its edition the *SecurOS* general term is used in the framework of the given document.

Sections that describe the functionality available for some editions are marked by a special footnote as in the example below:

The functionality is available in the following editions: *SecurOS Monitoring & Control Center, SecurOS Enterprise, SecurOS Premium, SecurOS Professional, SecurOS Xpress, SecurOS Lite.*

1.6 Design Convention

For representation of various terms and titles the following fonts and formatting tools are used in this document.

Font	Description
bold type	Used in writing workstation names, utilities or screens, windows and dialog boxes as well as the names of their elements (GUI elements).
<i>italic type</i>	Used to mark out the SecurOS objects.
<i>bold italic type</i>	Used to mark out the elements of homogeneous lists.
<code>monospace</code>	Used to mark out macro text and programming code, file names and their paths. Also it is used to specify the necessary options, to mark out values specified by the user from the keyboard (manually).
green	Used to mark out the cross-references within the document and links to the external available ones.

1.7 Design Elements

Warning! Serves to alert the user to information which is necessary for the correct perception of the text set out below. Typically, this information has a warning character.

Note. Note text in topic body.

Additional Information

Used to display additional information. These type of elements contain, for example, the description of options for executing a task or reference to additional literature.

2 Purpose, Implementation And Operation Principles

The SecurOS software is designed to control video surveillance and analytic systems deployed within local or global networks. Simple scaling of software and hardware platforms allows to create video surveillance systems of any complexity – from local systems which are intended to control small- and mid-scale objects, to complex systems that allow to control physical and organizational structures and facilities (e.g. buildings, roads, power plants) needed for the operation of a society or enterprise.

2.1 SecurOS Architecture

This section describes SecurOS's types of servers and workstations and their general features depending on software installation types.

2.1.1 Types Of Servers And Workstations

Computers of the SecurOS network are distinguished by their functionality and have specific roles in the network configuration management procedure.

This section contains general information on the types of SecurOS servers and workstations, their intended purposes, basic capabilities, and operational specifics.

2.1.1.1 Classification by Functionality

All computers connected to the SecurOS network are divided by their functionality into two main categories that define the SecurOS software installation type:

- **Video Server.**
- **Operator Workstation.**

The system administrator defines the installation type while planning the system architecture and sets it during the installation procedure. On each computer on the network only one installation type is allowed. A brief description of the installation types can be seen below.

2.1.1.1.1 Video Server

The *Video Server* is a computer that is used to connect IP cameras, to receive video from them, or to connect audio capture devices. In addition to the direct connection of cameras, this installation type allows to install or connect various security devices (fire alarm system controllers, access control subsystem controllers, etc.) and ISS analytics modules (e. g., SecurOS Auto Module).

2.1.1.1.2 Operator Workstation

The *Operator Workstation* is a client computer in the security network designed for remote viewing of video from surveillance cameras, listening to audio, managing various devices such as PTZ devices, doors, fire alarm and other subsystems.

If privileges to configure system were granted to the operator, **Administration Center** is available to him.

2.1.1.2 Classification of Roles in Configuration Management

The role of the *Video Server* defines its place in the SecurOS network configuration management procedure. One of the *Video Servers* within network must be assigned *Configuration Server*, and all other *Video Servers* – *Peripheral Servers*.

2.1.1.2.1 Configuration Server

Reliable operation of security system within a network consists of several types of servers that allow to configure the system independently. This is possible only if the system configuration is up to date on each of these network servers at any given time.

The procedure to update and synchronize the system configuration on all the servers in the system network is performed by the *Configuration Server*. The *Configuration Server* is a dedicated network server which in addition to standard features, has some advanced functionality as well.

Configuration Server is assigned during system software installation among from *Video Servers* of the SecurOS network.

Warning! System allows only one *Configuration Server*, which must be available for all *Video Servers* and *Operator Workstations*, from which it is intended to configure the system.

The actual system configuration is stored on the *Configuration Server*. Each of *Peripheral Servers* stores the current copy of the system configuration.

In case the *Configuration Server* fails, you can restore it from a backup after carrying out the necessary steps (see **Restoring Configuration from Backup Copy**) or reassign one of the *Peripheral servers* (see **ISS Server Role Manager Utility**).

Warning! The operating period for *Peripheral Servers* not connected to the *Configuration Server* is restricted. If connection with the *Configuration Server* is not restored within 90 days, the system will automatically shutdown on the given *Peripheral Server* and all *Operator Workstations* connected to it.

2.1.1.2.2 Managing Network Configuration by Configuration Server

This section describes the steps for server configuration when deploying a network and also procedures for network management and recovery.

2.1.1.2.2.1 How To Configure Servers When Deploying Network

At the initial system setup, the *Configuration Server* must be installed and configured first (see **Installing And Configuring The Configuration Server** section).

2.1.1.2.2.2 Configuration Update Procedure

The system configuration is updated according to the following set of rules:

Note. The described set of rules is applicable to any type of operations with the objects from the Object Tree, including object creation, editing and deletion.

1. Using any of the *Operator Workstation*, the administrator (or operator) makes changes to the Object Tree for that *Computer* (or *Computers*).
2. If a *Operator Workstation* is used to modify the configuration, then it generates an appropriate request to the *Configuration Server*.

Notes:

1. If the *Configuration Server* is used to modify the configuration, the changes are applied on the *Configuration Server* directly, with no request.
 2. When the *Configuration Server* is unavailable it's not possible to modify the system configuration using a *Operator Workstation*.
-
3. The *Configuration Server* processes the request(s). It applies changes by first renewing its own Object Tree and object settings, then generates and sends to each of the *Peripheral Servers* a command to update the state of their appropriate objects and their settings. If a *Peripheral Server* is switched off when changes must be applied, the command will be sent when connection with the *Configuration Server* will be restored.
 4. Having received the command to update its current configuration, each of the *Peripheral Servers* applies the changes by updating its own Object Tree and/or settings of the appropriate objects.

Note. The update requests are processed by the *Configuration Server* consistently in order of creation. Only one request is processed by the *Configuration Server* at the same time. The processing of the next request is locked until the current request is finished and changes are applied on the *Configuration Server*.

2.1.1.2.2.3 Restoring Configuration from Backup Copy

The configuration can be restored from the backup copy. A backup copy can be created by any of the network servers, but the restore procedure can be executed only on the *Configuration Server*.

Warning! Only a backup copy of the currently installed SecurOS version is applicable. Backup copy creation procedure is described in the [System](#) section.

2.1.2 Software Implementation

SecurOS software consists of two components – *Server part* (further will be referred as *Server*) and *Client application* (further as *Client*).

Server receives and processes video, allows to connect different security devices and intelligent program Modules. This component starts automatically on each *Video Server* after software installation is finished.

Client is installed both on *Video Server* and *Operator Workstation*. When installing SecurOS software on *Video Server*, *Client* is installed automatically. Installation of *Client* on *Operator Workstation* is a separate procedure. Using *Client* one can work with SecurOS objects – *Cameras*, *Maps* etc. with the help of SecurOS interface objects (*Media Client*, *Map Window* etc.). Using *Client* one can also administrate the system, if user has required rights.

Server part is implemented as OS service, namely as *SecurOS Control Service*. This service is started and stopped with the help of **Server Control Agent** utility or by means of OS tools (see **System Shutdown**).

Client part is implemented as *client.exe* application. This application is located in the \SecurOS folder of the product installation root directory.

Warning! It is recommended to use the same character encoding for all *Users* on all *Computers* within SecurOS network. Otherwise some character may be displayed incorrectly on some *Computers* (namely in object or event names etc.).

2.2 Software And Hardware Platform

This section covers software and hardware requirements for computers installing the SecurOS software.

2.2.1 Video Server System Requirements

Table 1. Video Server System Requirements

Parameter	Description
OS	<ul style="list-style-type: none">Windows Server 2008 R2 (Service Pack 1) – Standard Edition, Enterprise Edition;Windows 7 (Service Pack 1) – Home Basic, Home Premium, Professional, Enterprise, Ultimate;Windows 8.1 – all editions;Windows Server 2012 R2 – all editions;Windows 10 – Home, Pro, Enterprise, Education;Windows Server 2016 – Standard, Datacenter. <p>Warning! Only 64-bit versions of operation systems listed above are supported.</p>
CPU	Intel Core i3-4330/AMD FX-4350 or above. Intel Core i5-4670/AMD FX-8320 is recommended. Warning! Hardware decompression of H.264/H.265 stream is not supported by AMD CPUs.
RAM	Not less than 4 GB. 12 GB is recommended
HDD	Not less than 150 GB

Parameter	Description
HDD free space for software installation	Not less than 5 GB Note. Additional intelligent modules require additional disk space.
HDD free space for PostgreSQL installation	Not less than 500 MB
TCP/IP network speed	Not less than 100 Mbps. 1000 Mbps is recommended

2.2.2 Operator Workstation System Requirements

Table 2. Operator Workstation System Requirements

Parameter	Description
OS	<ul style="list-style-type: none"> • Windows Server 2008 R2 (Service Pack 1) – Standard Edition, Enterprise Edition – 64-bit; • Windows 7 (Service Pack 1) – Home Basic, Home Premium, Professional, Enterprise, Ultimate – 32-bit and 64-bit; • Windows 8.1 – all editions; • Windows Server 2012 R2 – all editions; • Windows 10 – Home, Pro, Enterprise, Education; • Windows Server 2016 – Standard, Datacenter.
CPU	<p>Intel Core i3-4130/AMD FX-4350 or above (for example, Intel Core i5-4xxx).</p> <p>Warning! Hardware decompression of H.264/H.265 stream is not supported by AMD CPUs.</p>
RAM	Not less than 4 GB. 8 GB is recommended. Recommended frequency – not less than 1600 MHz
HDD	Not less than 40 GB
HDD free space for software installation	<p>Not less than 5 GB</p> <p>Note. Additional intelligent modules require additional disk space.</p>
Video adapter	Integrated in CPU (see CPU above) or similar discrete video controller Intel/AMD. Intel HD Graphics 4000 (integrated in Intel CPU) or above is recommended

Parameter	Description
Monitor Resolution	<p>Not less than:</p> <ul style="list-style-type: none"> • 1360x760 px – for Windows; • 1280x1024 px – for Linux. <p>Warning! If monitor resolution is less than specified above, the correct displaying of the GUI for setting up and working with the system is not guaranteed.</p>
TCP/IP network speed	Not less than 100 Mbps. 1000 Mbps is recommended to view uncompressed video from several cameras simultaneously

2.2.3 Audio Subsystem Requirements

To capture and playback audio the *Video Server* should have either integrated audio on-board (check the motherboard documentation) or any additional PCI or PCI-E sound card.

Note. Integrated or additional sound card provides audio capture only from one microphone.

2.2.4 Notification Subsystem Requirements

To use the Audible Notification Service (playing audio upon system events) to work on a particular computer, it should have either integrated audio on-board or any additional PCI or PCI-E sound card.

2.2.5 ACS Requirements

The video server should have the required number of free (not used) serial (COM) ports to connect the ACS/alarm/fire alarm controllers.

2.2.6 Environment Requirements

The sections below contain information about the system and requirements for setting up, starting, and correctly using SecurOS.

2.2.6.1 Computer Name Restrictions

Names of computers on which the SecurOS software can be installed, should comply with the following requirements:

1. The length of the name should not exceed 15 symbols.
2. Blank spaces, tabs and the following characters are restricted:
` ~ ! @ # % ^ & * () = + _ [] { } | ; : . ' \ " № , < > / ?
3. The name cannot consist of digits only.

Note. Refer to this section for any questions/concerns regarding the reading/editing/checking of the **computer_name** value.

2.3 SecurOS' Subsystems

Configuration, basic features and objects of different subsystems of the SecurOS system are described separately in the subsequent parts of the document. The following subsystems are part of the SecurOS system structure:

- Core subsystem - contains objects and their settings corresponding to main system components, such as users and computers. Also organization structure of the system and data storage are configured within this subsystem, as well as system statistics collection parameters (see [Core Subsystem](#)).
- Interface subsystem - contains objects responsible for visual representation of system objects which are used by operators working with the system. These include desktops, external application windows, maps, HTML forms and dialogs, system event viewer, etc. (see [Interface Subsystem](#)).
- Video subsystem - contains components which are responsible for main video stream control, video camera displaying and recording process, video playback and live video monitoring, video motion detectors and video archives (see [Video Subsystem](#)).
- Audio subsystem - contains control facilities of audio recording and playback devices (see [Audio Subsystem](#)).
- I/O subsystem - contains objects responsible for input/output peripheral devices (fire alarm controllers, relays and various detectors) (see [I/O Subsystem](#)).
- Notification subsystem - contains objects for notification of users about system events by media messages (see [Notification Subsystem](#)).
- Automation subsystem - contains tools for device integration, compilation and interpretation of the system scripts and macros (see [Automation Subsystem](#)).
- Computer vision subsystem - represents integrated environment that allows to connect and use within the SecurOS system the wide range of various analytics detectors (see [Computer Vision](#)).
- Monitoring and Control subsystem, that allows to deploy a common *Monitoring & Control Center* to supervise a lot of the remote security systems (see [Monitoring & Control Center](#)).

Note. Each section contains a description of the basic operation principles and configuration specifics of the selected subsystem.

3 SecurOS Installation and Update

This section describes in details the sequence of steps, that must be done in order to create and start operation of the SecurOS security network.

Warning! Make sure that all required port are opened in the firewall settings (see [Appendix D. TCP/IP Ports Used by SecurOS](#)).

First of all one it is necessary to prepare *Video Servers* (see [Types Of Servers And Workstations](#)). Order of SecurOS installation on *Video Servers* is described in the following sections:

- [Installing, Configuring and Launching Configuration Server](#);
- [Installing, Configuring And Launching Peripheral Servers](#).

Then, it is necessary to prepare *Operator Workstations*. SecurOS installation order onto *Operator Workstations* is described in corresponding section:

- [Installing, Configuring and Launching Operator Workstations](#).

Warning!

1. All components of all SecurOS Intelligent Modules that are used within the system must be installed on each *Video Server* and *Operator Workstation*.
2. The software language must be the same for all network computers.
3. System time must be synchronized for all *Video Servers* within configuration.
4. Before installing SecurOS software on 64-bit MS Windows 2008 Server R2 it is necessary to install additional multimedia components (see [Installing Multimedia Components and Services under MS Windows Server 2008 R2](#));
5. SecurOS software installation is possible only on those computers which names correspond to the requirements stated in [Computer Name Restrictions](#) section.

3.1 Installing, Configuring and Launching Configuration Server

This section describes installation and configuration of the SecurOS's managing server.

3.1.1 Hardware Installation

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*, *SecurOS Xpress*.

The section provides short information on an additional hardware that can be included in the product delivery set. These are the Guardant keys.

3.1.1.1 Guardant Key Installation

The Guardant key is the electronic device constantly connected to the computer through a USB port. The SecurOS software addresses to a key for check the license information.

The key is necessary to place before the beginning of the SecurOS software installation. To install Guardant key, plug the key into any free (not used) USB port.

The Guardant key driver is installed automatically when the corresponding option from the SecurOS InstallShield Wizard (see [Software Installation](#)) is selected.

3.1.1.2 Installing Guardant Key in Manual Mode

To install Guardant Key driver in manual mode after SecurOS is installed do the following:

1. Browse to the SecurOS root folder, then to the \Drivers\Guardant32 or \Drivers\Guardant64 folders for 32- and 64-bit OS, respectively.
2. Launch GrdDrivers.msi. System will display installation Wizard Welcome window.
3. Click on the **Next** button until Wizard finish installation.
4. When installation will complete system will display appropriate window. Click on the **Finish** button to exit installation Wizard.

3.1.2 License Key

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*, *SecurOS Xpress*.

The license key defines allowed configuration of the security network and is necessary to launch the SecurOS.

The license key is created on the basis of the SecurOS hardware unique codes (Guardant) or combinations of unique codes of the computer hardware on which SecurOS is installed.

License keys are checked according to the priority descending in the following order:

1. Guardant key;
2. key on the basis of the combinations of unique codes of the computer hardware (hardware code).

In addition to the unique hardware codes, the following data is also taken into account during license key generation:

- program language selected on the SecurOS installation;
- default language of the installed operating system (**Language** parameter (*local ID*));
- SecurOS release version;
- SecurOS edition.

The license key is usually provided in one of the following ways:

- in the product delivery set, on the software CD;
- by e-mail.

3.1.2.1 The Key is a part of a product

If the license key is provided on a disk in the delivery set, then it is necessary to specify the key location in the **Installation of the license key file** window at the corresponding step of the SecurOS installation procedure (see [Software Installation](#) section).

3.1.2.2 Request the key by e-mail

In case the license key isn't included in the SecurOS delivery set it is necessary contact Intelligent Security Systems to request it from.

For key request registration perform the following steps:

1. Install the SecurOS hard and software on the computer.
2. To get hardware unique codes, run the **Hardware Report Utility**, thereto click the **Start** button on the Windows Task bar. Consistently choose **All Programs → SecurOS → Hardware Report Utility** menu items.
3. The utility will display the report data in the **ISS Hardware Report Utility** window (for example, see figure 1).

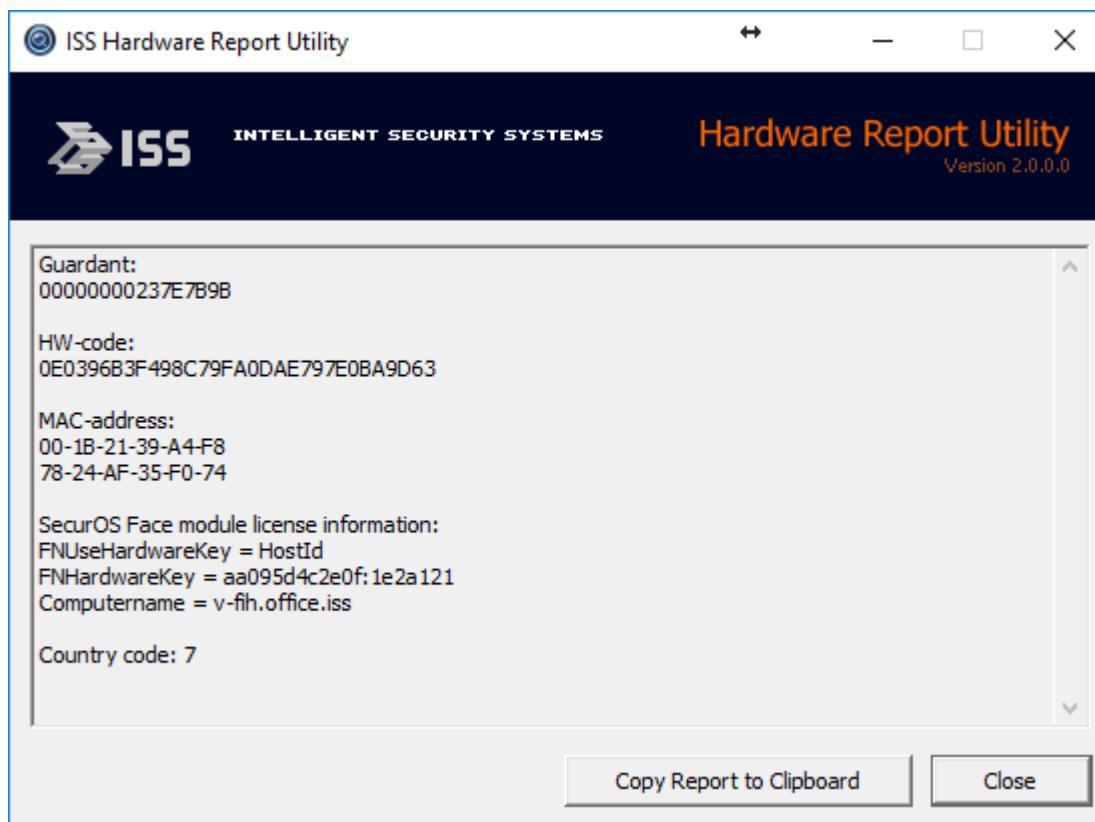


Figure 1. Hardware Report Utility window

4. Click **Copy Report to Clipboard** button in the utility window. The utility will copy the report to clipboard.

5. Create and open a new text file of any format. Paste the clipboard content to the file. Additionally insert the following data into the file:
 - program language selected on the SecurOS installation;
 - SecurOS release number;
 - SecurOS edition.
6. Save the file.
7. Send the file to the Intelligent Security Systems Technical Support Team (see [Getting Technical Support](#) section).

On receiving the license key file copy it to the SecurOS root folder.

3.1.3 Software Installation

This section covers a specifics of the SecurOS installation or upgrading, that make it possible to reuse previously created objects.

Warning! To install the software, you must have administrator rights for Windows OS. Proceed to software installation only when you finish hardware installation and network configuration for any computer.

Note. It is not supported to install the software on Windows Server 2008 R2 if it is a domain controller.

3.1.3.1 Using Current Parameters of the Windows User Account needed for PostgreSQL

During first SecurOS installation Windows user account needed for PostgreSQL operation is created with the name `postgres` and the same password.

Note. If current system security policy does not allow to create user account with default login and password, specify password that meets the requirements of the active system security policy.

If default values were changed, but are supposed to be used further, do the following on the certain step of the software installation:

1. In the **Database update and formatting** window (see figure 2) enter currently used password of the PostgreSQL user account.

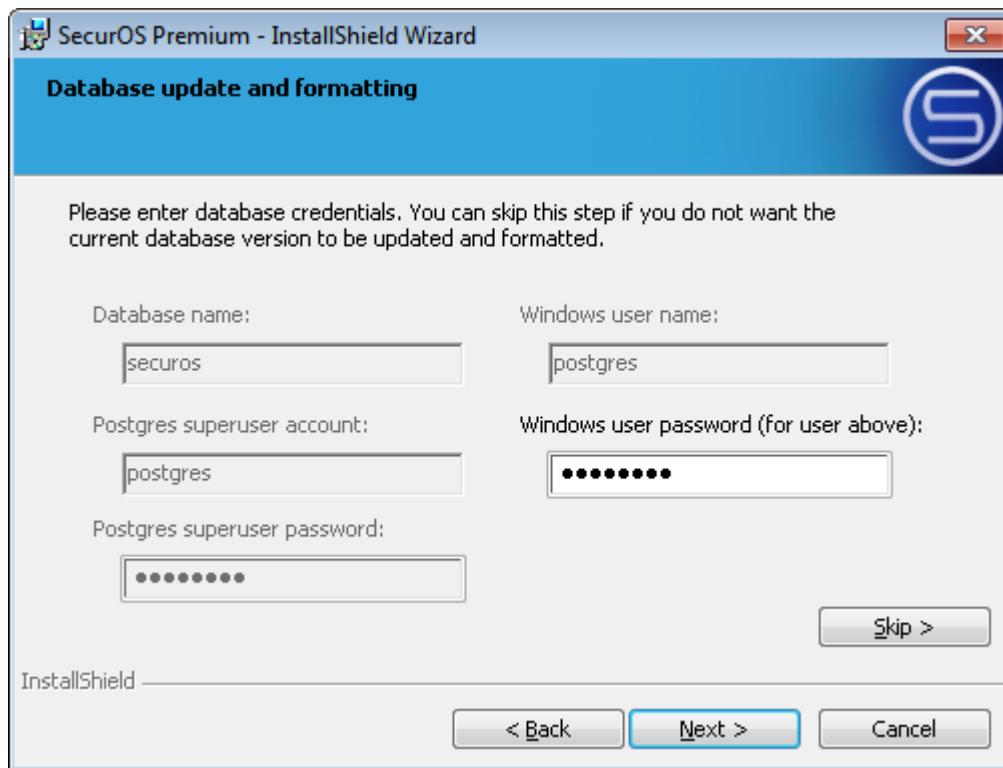


Figure 2. Database update and formatting Window

2. Click **Next** to continue. System will recreate Windows user account with name `postgres` and old password.

Note. This step can be skipped, but in this case current database version will not be updated and reformatted, that makes its further use impossible.

3.1.3.2 Using Current Parameters of the Database and Administrator User Account

During first SecurOS software installation default PostgreSQL administrator's user account is created with the name `postgres` and the same password, database is created with the name `securos`.

If default values were changed, but are supposed to be used further, do the following on the certain step of the software installation:

1. In the **Database update and formatting** window (see figure 3) enter currently used database name and database administrator's credentials.

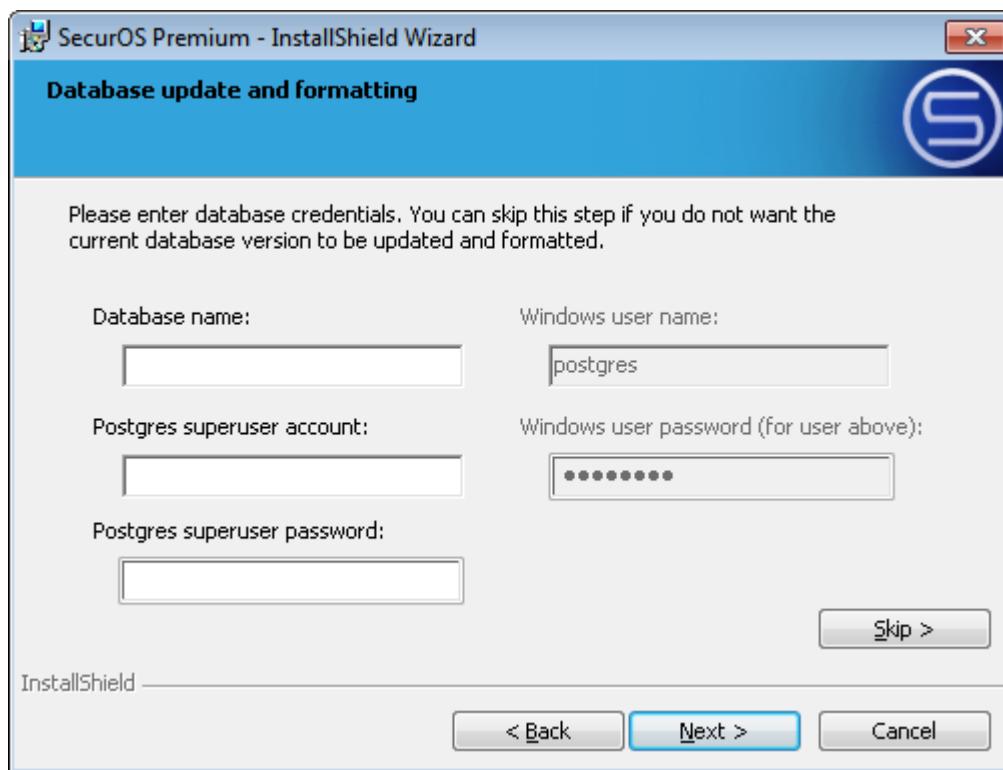


Figure 3. Database update and formatting Window

2. Click **Next** to continue. The database will be updated and reformatted with the old name and administrator's credentials.

Note. This step can be skipped, but in this case current database version will not be updated and reformatted, that makes its further use impossible.

3.1.3.3 Software Installation On The Configuration Server

To install the software on a Video Server do the following:

1. To start the SecurOS software installation run the product setup file. System will display the **Choose Setup Language** window (see figure 4).

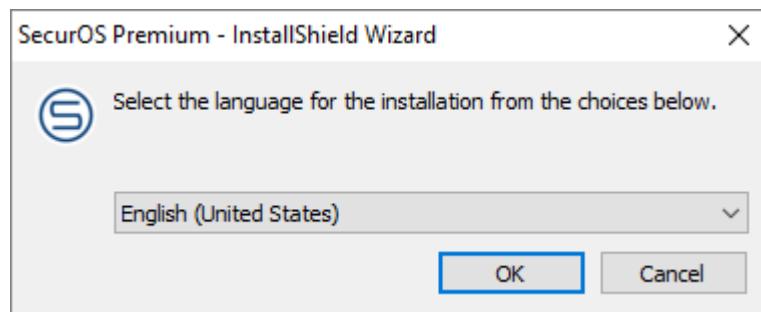


Figure 4. Choose Setup Language window

From the drop-down list select the SecurOS InstallShield Wizard required language. Click the **OK** button.

Additional Information

The Choose Setup Language information messages depends on the OS default language (the **Language** parameter value (*local ID*)).

2. The **Preparing To Install** window will appear, in which the steps of the installation preparation will be displayed.

After the end of procedure of preparation the system will automatically display the **Welcome to the InstallShield Wizard** window (see figure 5).

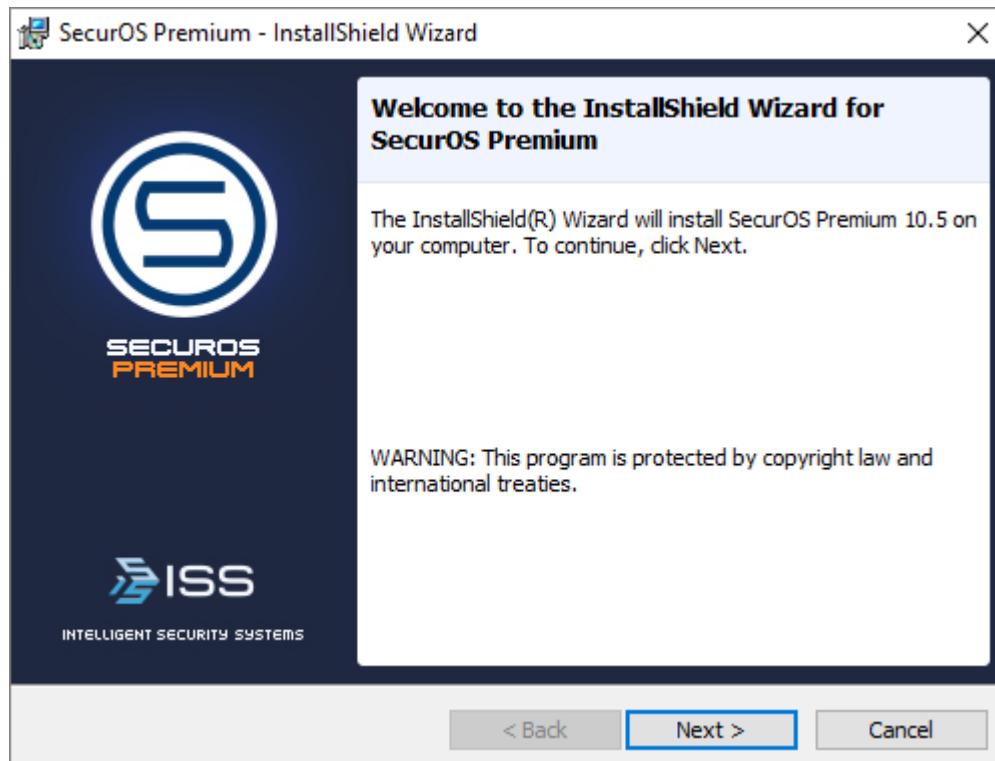


Figure 5. Welcome to the InstallShield Wizard window

Click the **Next** button in the **Welcome to the InstallShield Wizard** window to continue.

3. The **License Agreement** window will appear (see figure 6).

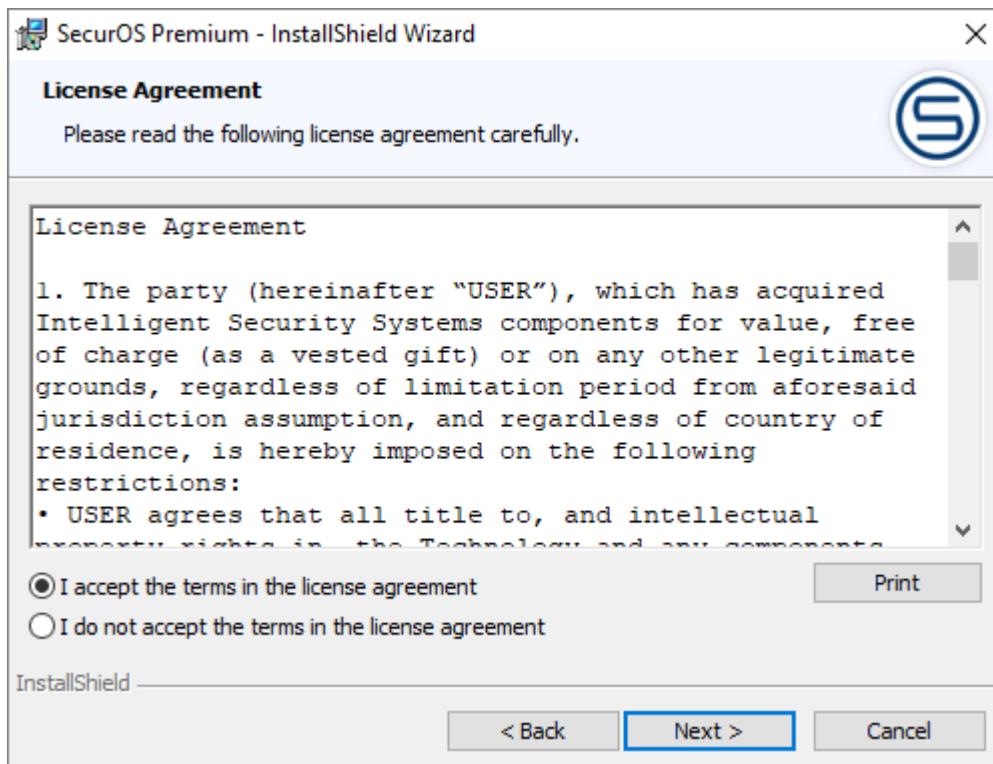


Figure 6. License Agreement window

Read the license agreement carefully. Select **I accept the terms in the license agreement** option if you agree. Click the **Next** button.

4. The **Install Type** window will appear (see figure 7).

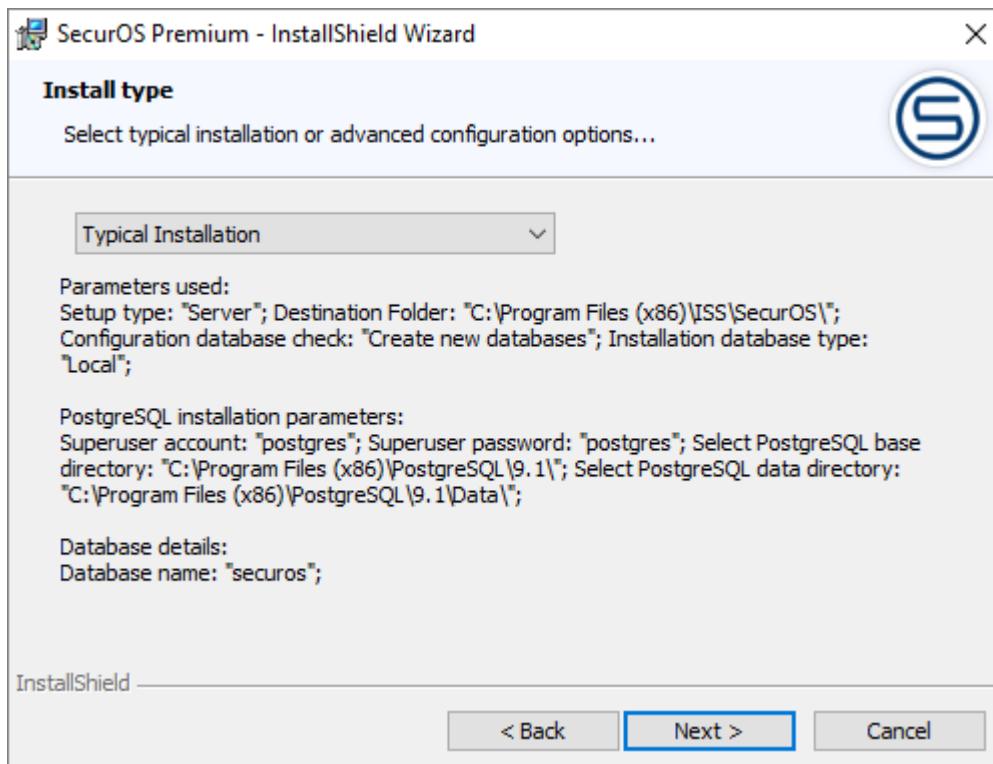


Figure 7. Install Type window

By default the typical installation mode allowing to install Video Server software with default settings is selected. Click the **Next** button.

5. The **Server Type** window will appear (see figure 8).

The item is excluded from the installation procedure in the *SecurOS Xpress*, *SecurOS Lite* editions.

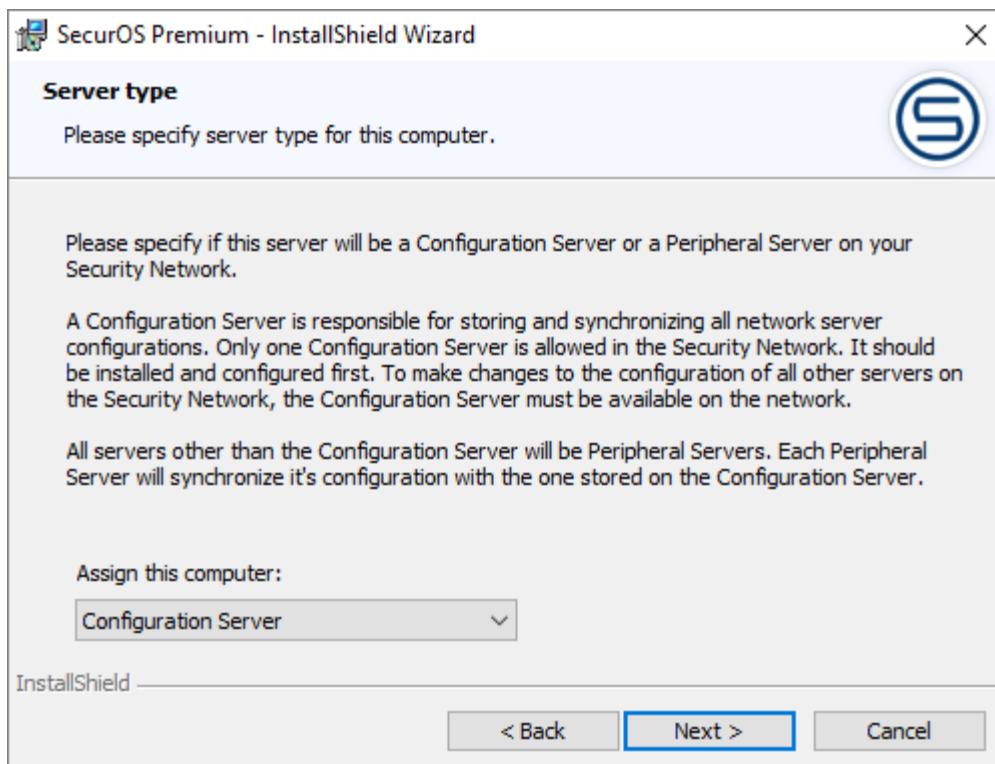


Figure 8. Server Type window

To install *Configuration Server* software select appropriate value from the drop-down list. Click the **Next** button.

6. The **Installation of the license key file** window will appear (see figure 9).

This step is excluded from the installation procedure for the *SecurOS Lite* edition.

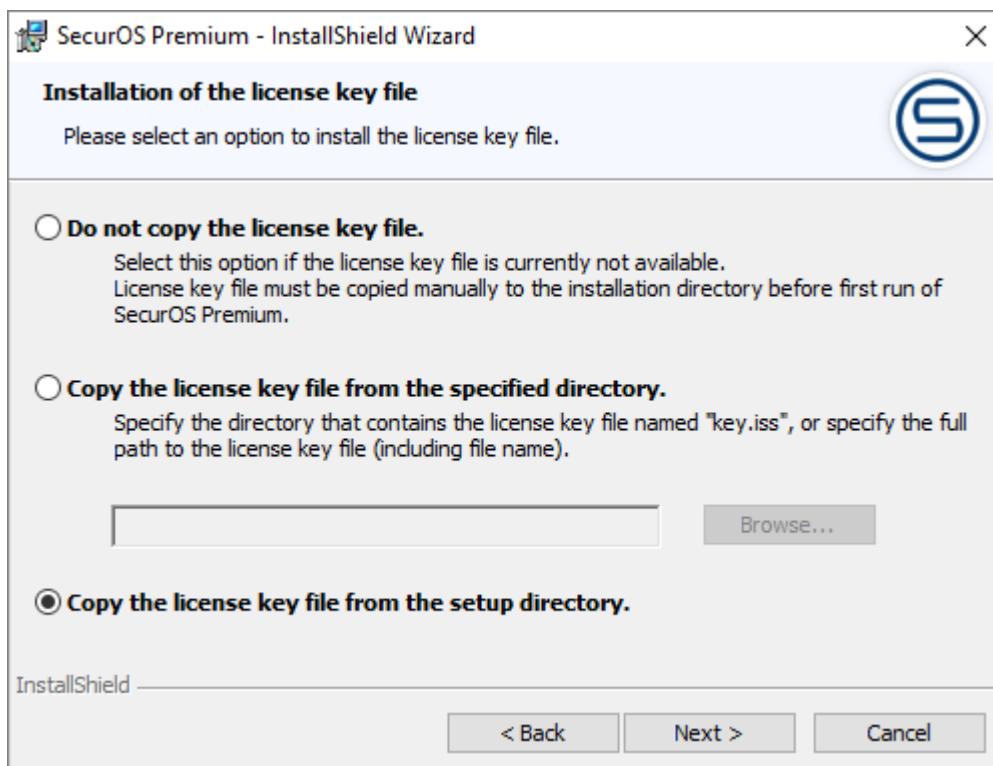


Figure 9. Installation of the license key file window

Depending on the availability of the license key, do one of the following:

- *if the key is available:*
 - select the **Copy the license key from the specified directory** option, click the **Browse** button and specify the directory that contains license key file using file manager;
 - select the **Copy the license key file from the setup directory** option if setup directory contains the license key file.

Additional Information

Copy the license key file from the setup directory option is displayed in the **Installation of the license key file** window only when SecurOS setup directory contains the license key file.

- *if the key is not available –* select the **Do not copy the license key file** option. The key file can be copied in the SecurOS installation directory after installation is complete. For more information about getting license key file see [License Key](#) section.

Click the **Next** button.

7. The **Software language selection** window will appear (see figure 10).

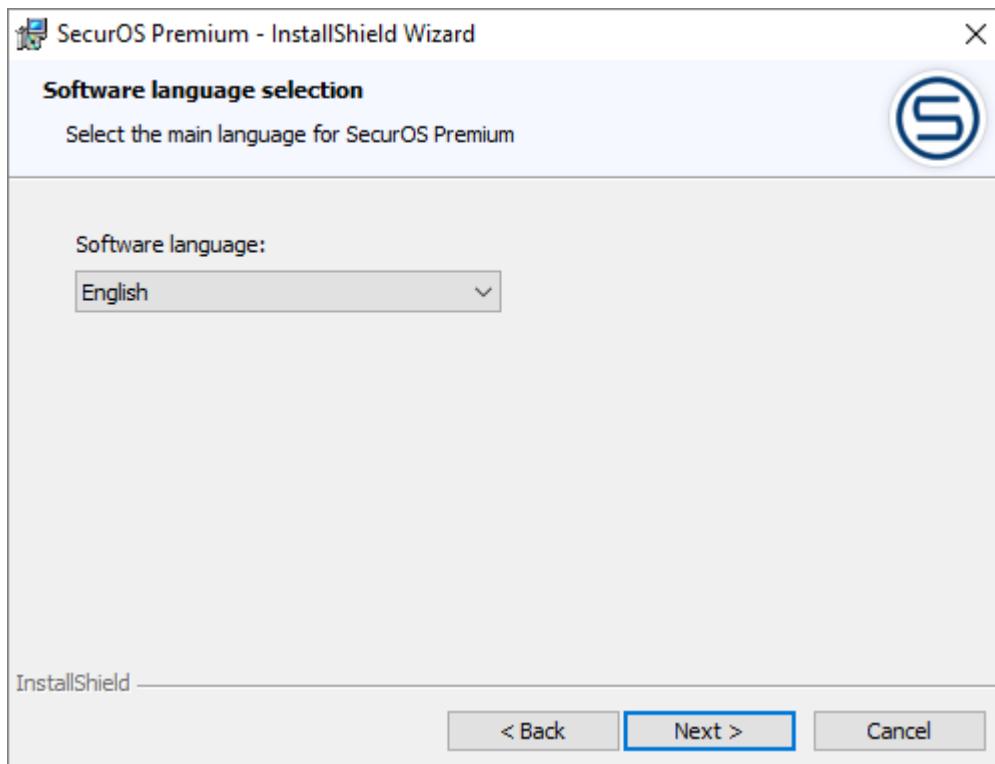


Figure 10. Software language selection window

To define SecurOS program language select the required one from the drop-down list.

Warning! You should specify only the language, which is permitted by your license key file. For more information about license key see [License Key](#) section.

Click the **Next** button.

8. The **Device driver selection** window will appear (see figure 11).

The item is excluded from the installation procedure in the *SecurOS Lite* edition.

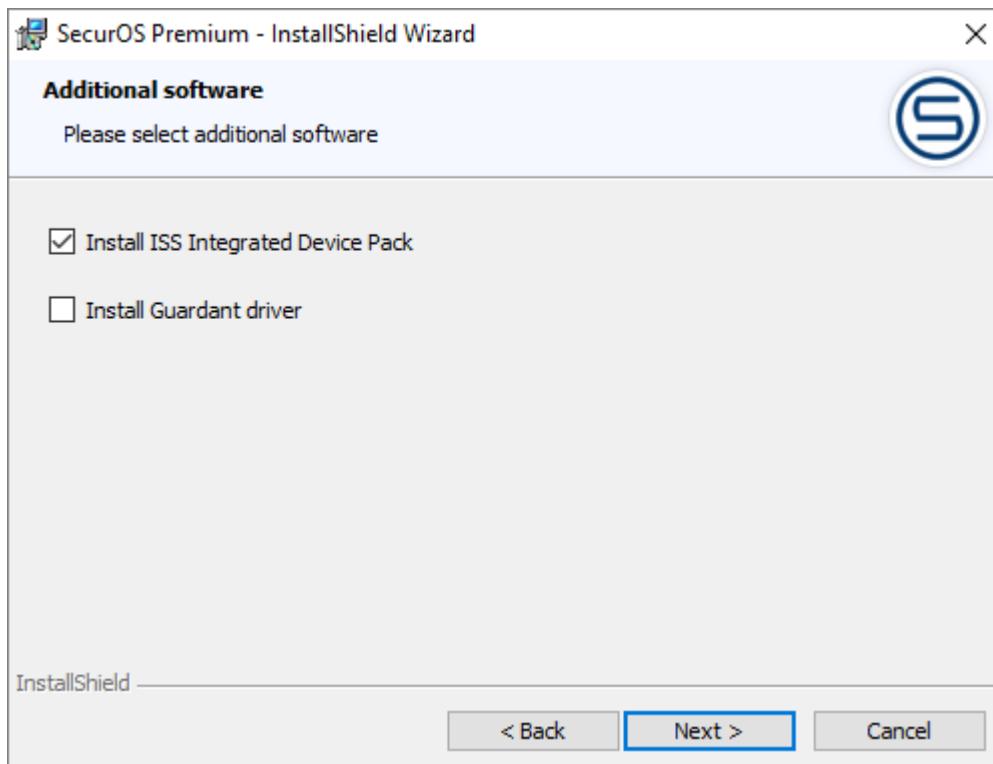


Figure 11. Device driver selection window

Leave the **Install ISS Integrated Devices Pack** checkbox selected if you suppose to connect an additional hardware: for example, cameras. Tick the **Install Guardant driver** checkbox if Guardant USB-key is used. Click the **Next** button to continue.

9. The Ready to Install SecurOS window will appear (see figure 12).

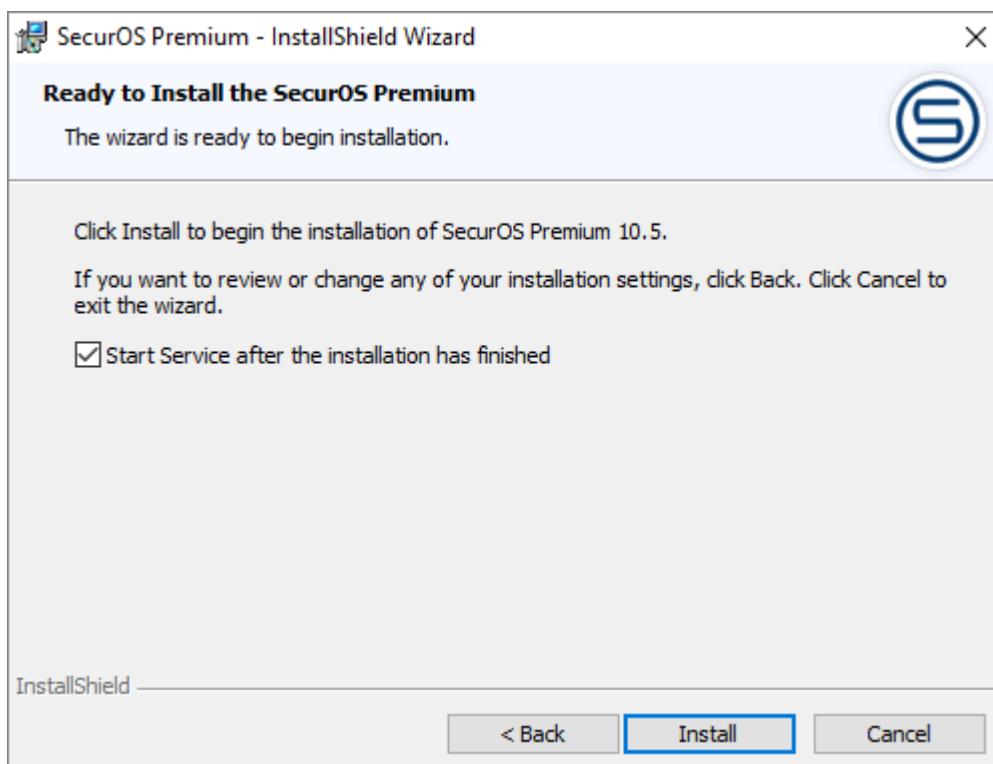


Figure 12. Ready to Install SecurOS window

If it is not necessary to start SecurOS Control Service immediately after installation has finished deselect the **Start Service after installation has finished** checkbox selected by default. To start the installation procedure click the **Install** button. The system will unpack required archives and then will begin the installation and will display **SecurOS Installation** window, in which the indicator of the process will be shown. After the installation process has successfully completed the **InstallShield Wizard Completed** window will appear (see figure 13).

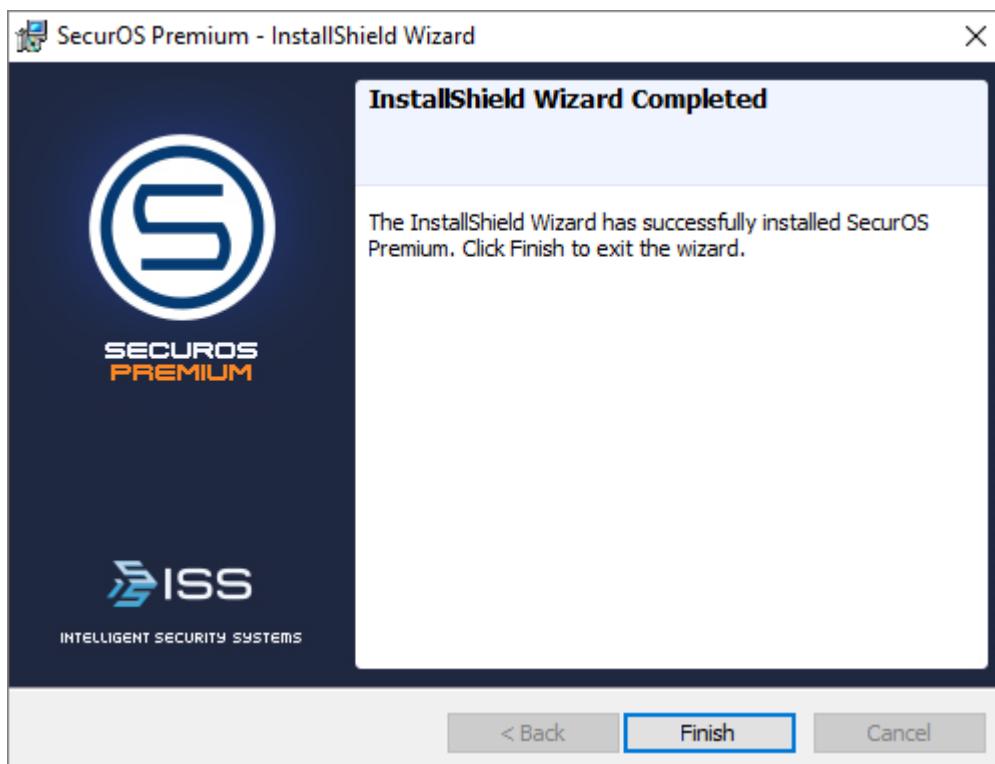


Figure 13. InstallShield Wizard Completed window

Click the **Finish** button to exit the installation program.

3.1.4 Initial Configuration

Initial SecurOS configuration is carried out on the *Configuration Server* with the help of the *System Configuration Wizard*, which offers various options of configurations. Base configuration at which the configuration data is entered by the administrator, is carried out by means of the *First Start Configuration Wizard*. Upon the configuration finish, the system will be completely ready for use.

3.1.4.1 Initial Configuration Using The System Configuration Wizard

To configure SecurOS for the first time by means of the Wizard, perform the following steps:

1. Launch SecurOS Client application by going to the Windows **Start** menu and selecting the following menu options **Programs → SecurOS → SecurOS** (see figure 14).

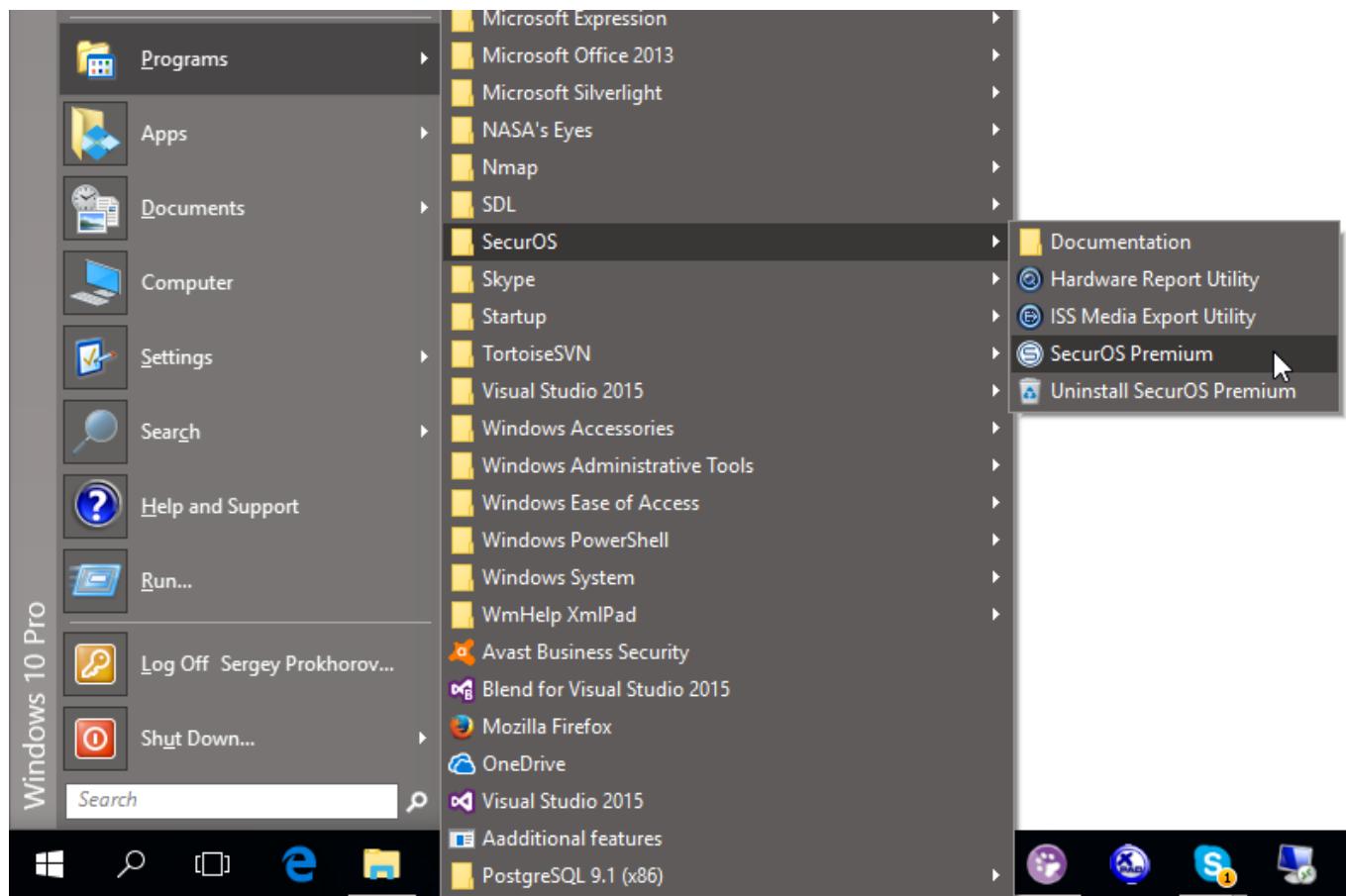


Figure 14. Start menu (All programs)

2. When *Client* starts on *Configuration Server* for the first time, system will open the *System Configuration Wizard* window which will provide options for system configuration (see figure 15). For basic configuration select the *Configure* using *Wizard* option that is active by default.

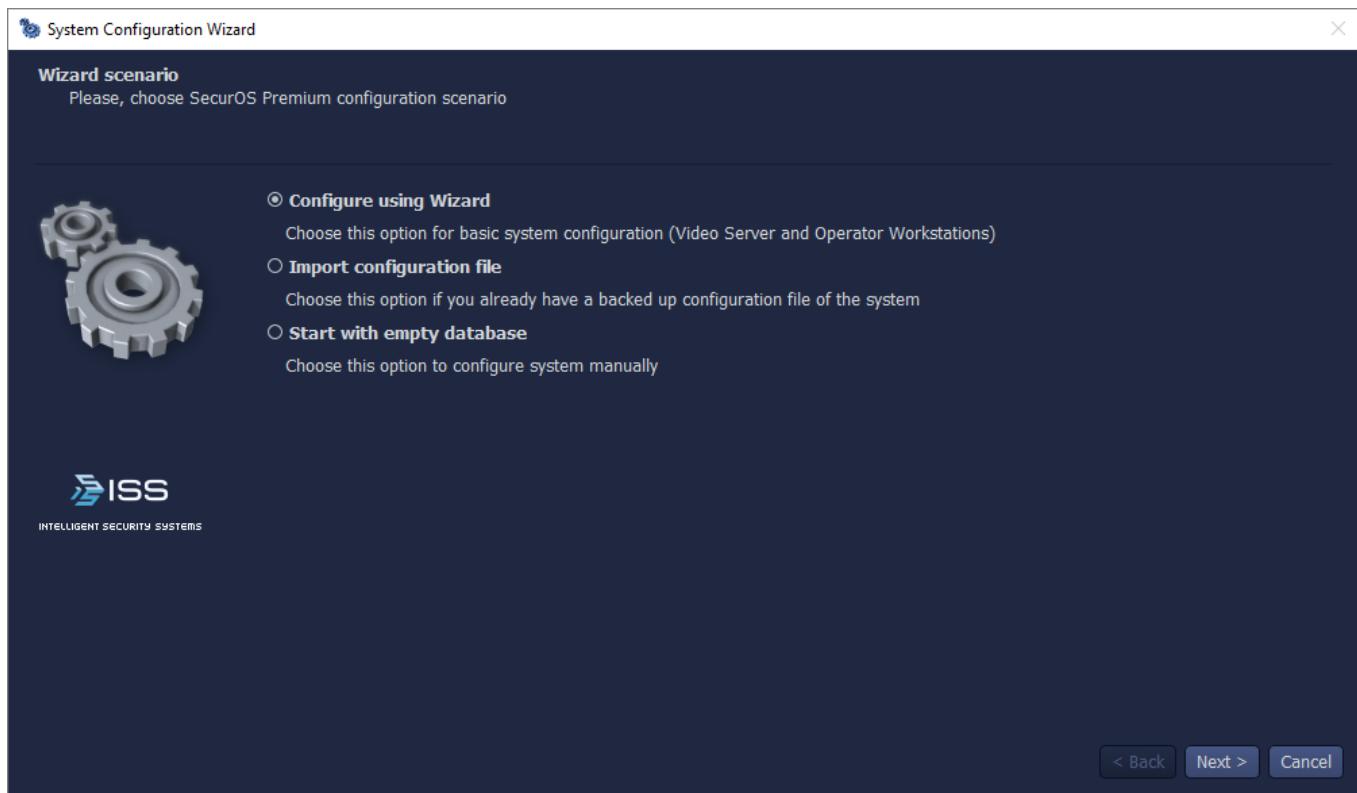


Figure 15. Wizard scenario window

Click the **Next** button.

Note. Import configuration file and Start with empty database scenarios are described below.

3. The **License view** window will appear (see figure 16).

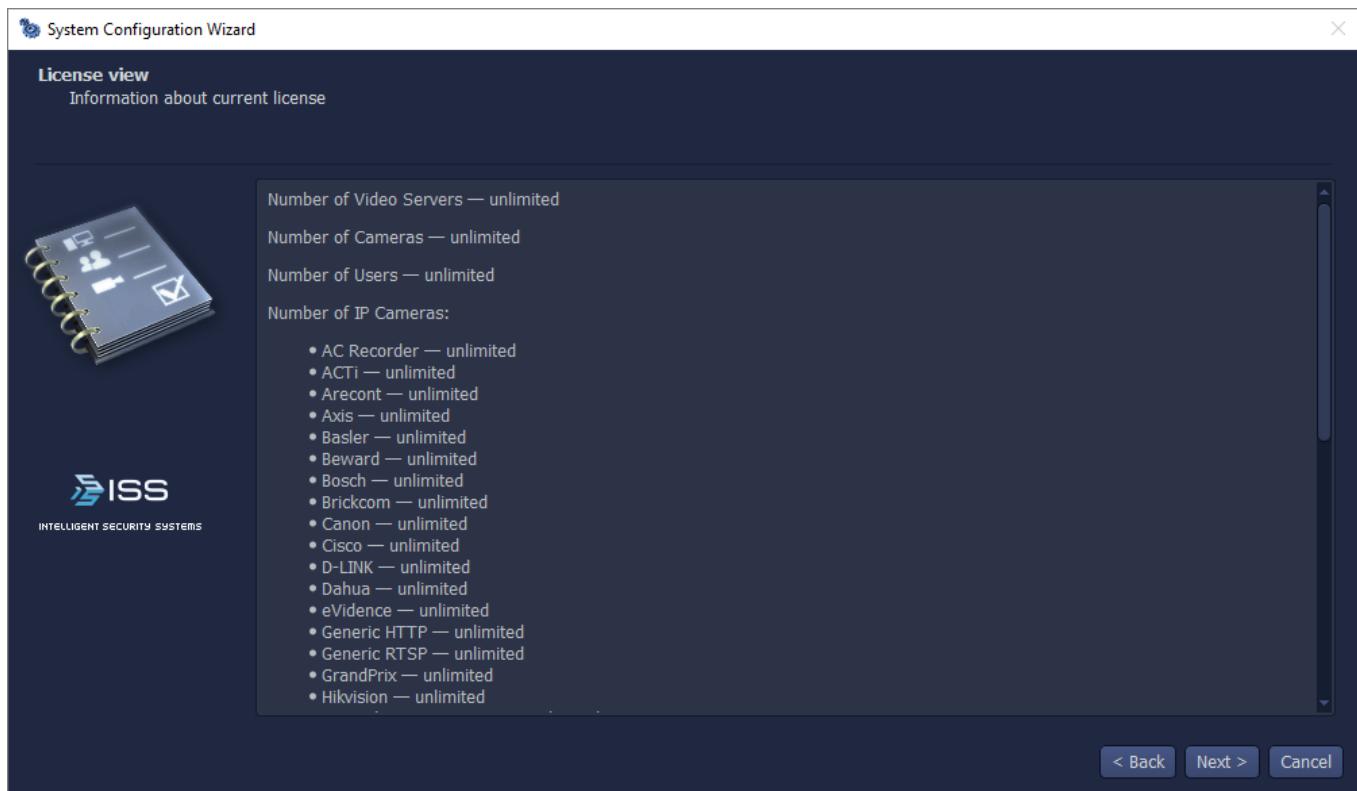


Figure 16. License view window

Window displays license restrictions for the currently installed SecurOS. Click the **Next** button to continue.

4. The **Superuser password setup** window will appear (see figure 17).

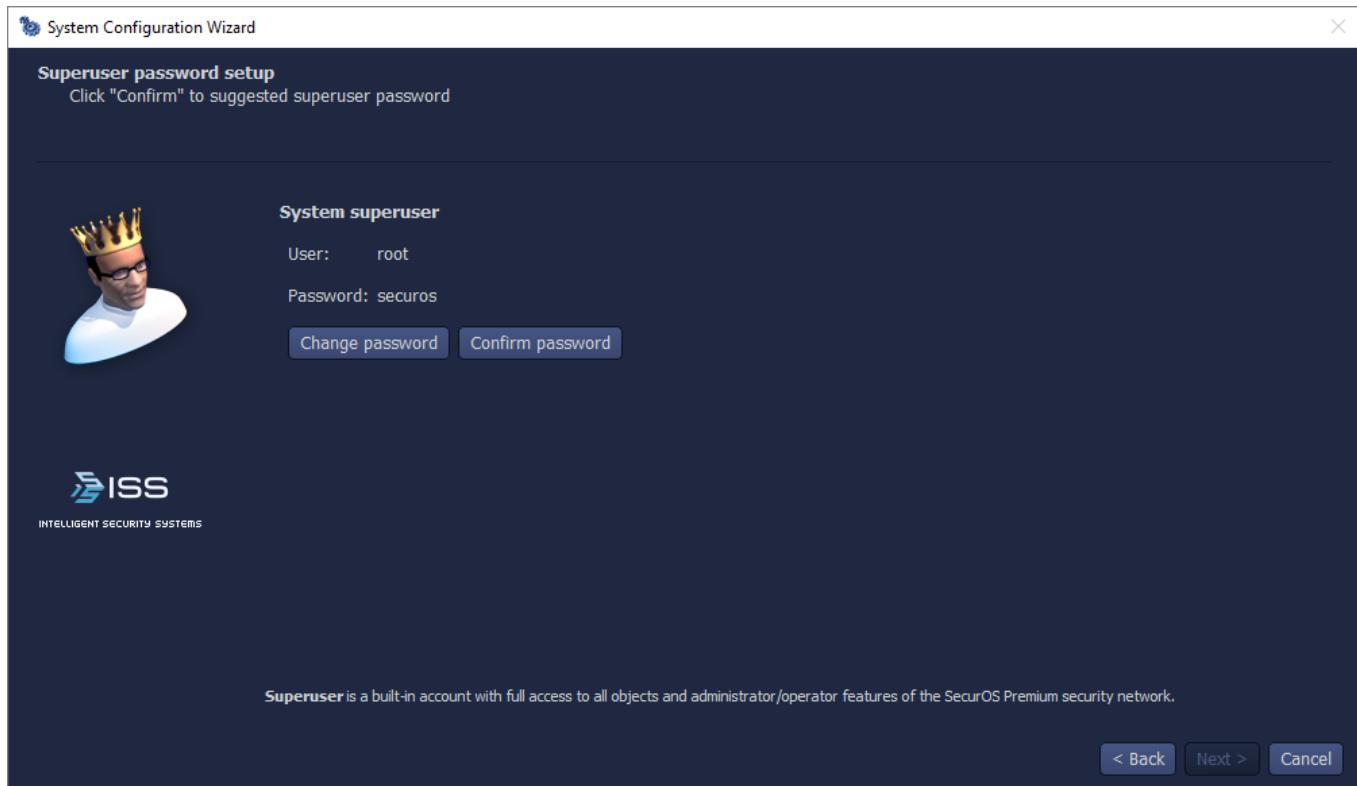


Figure 17. Superuser password setup window

To confirm default superuser password click the **Confirm password** button. To change superuser password click the **Change password** button.

The system will display window to enter new parameter values (see figure 18).

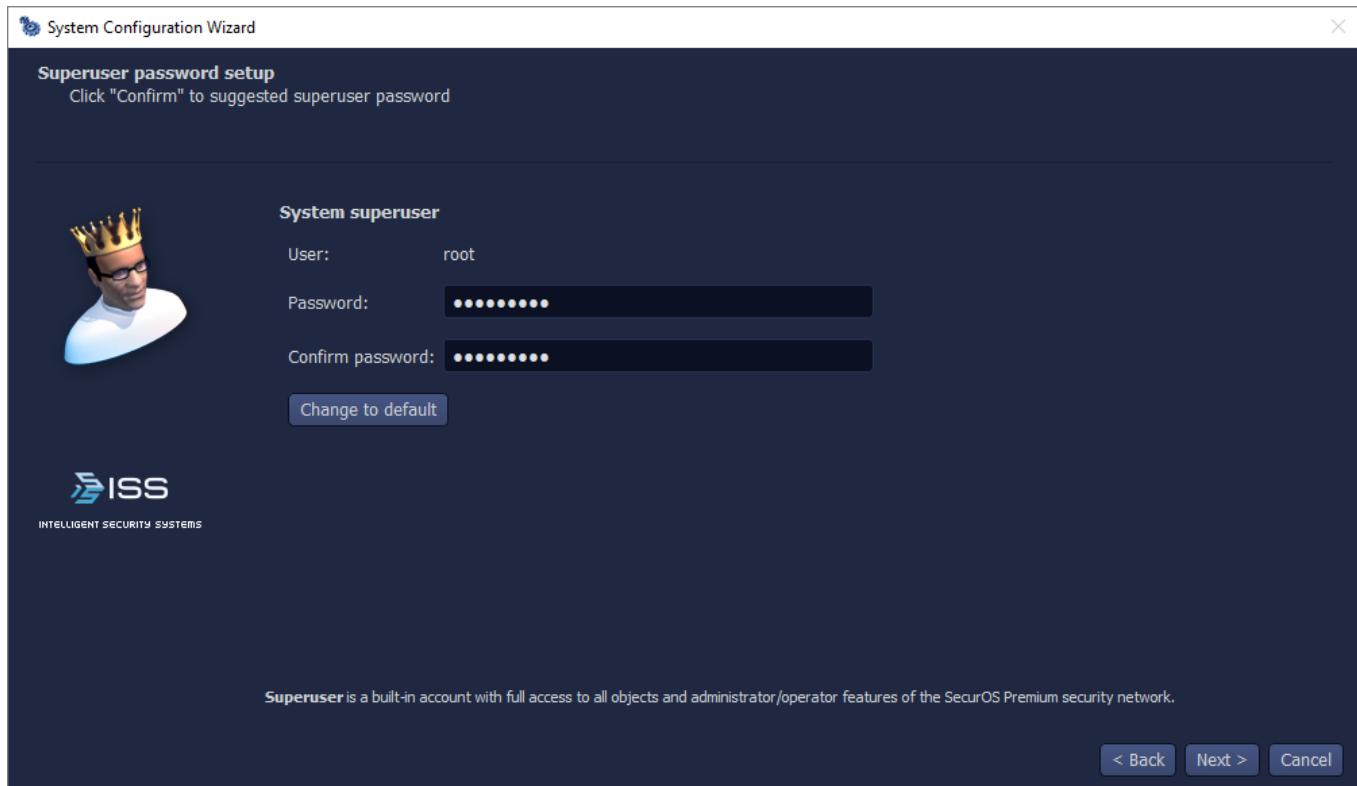


Figure 18. Change superuser password window

Set and confirm new superuser's password, or click the **Change to default** button to use default value. Click the **Next** button to continue.

5. System will display **Users setup** window (see figure 19).

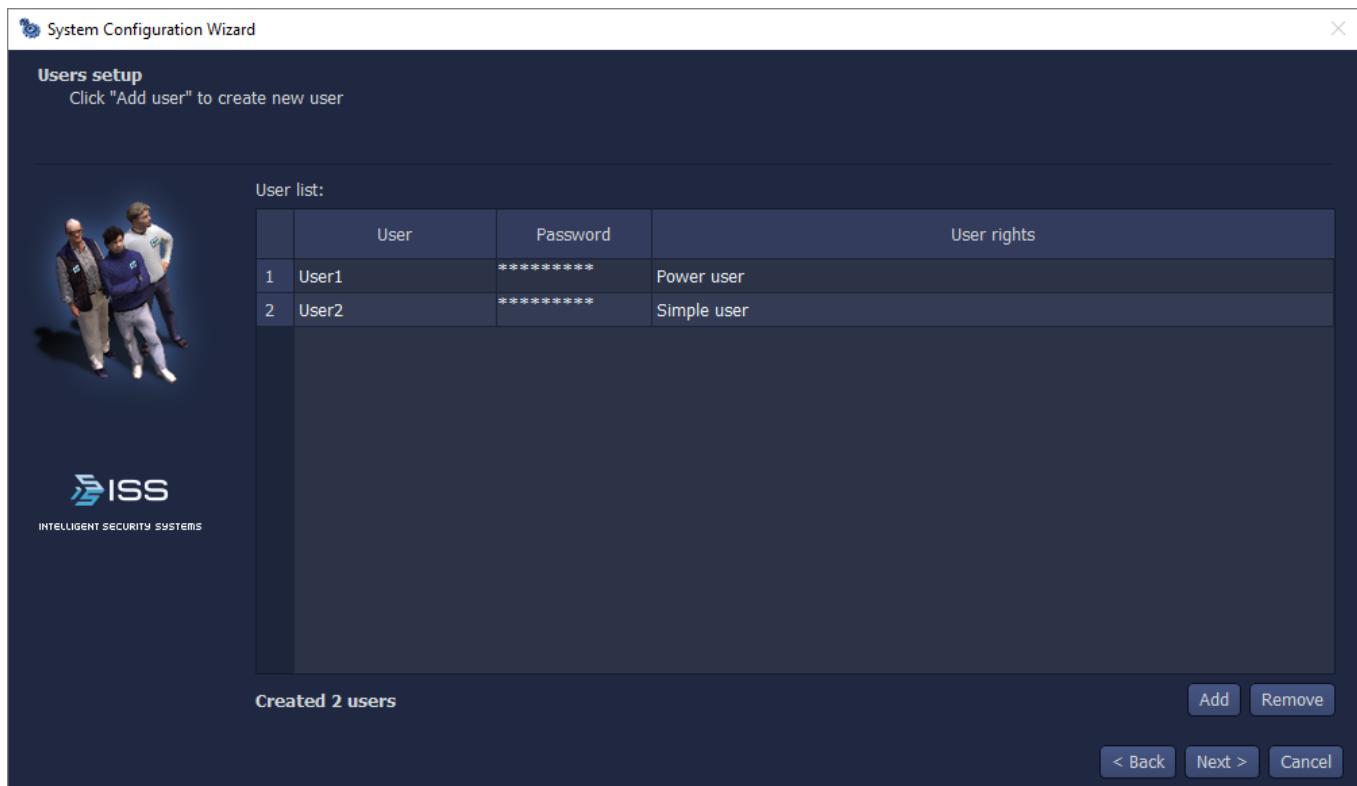


Figure 19. User setup window

To add a new users enter required values into the appropriate fields.

New users can be created with the following user account rights:

- *Power user*;
- *Simple user*.

Power user can do the following:

- View objects using the user interface;
- Control video cameras, for example, arm camera, start and stop recording;
- Control PTZ devices;
- Hide user interface;
- Log off current SecurOS user and close SecurOS *Client application*;

Simple user can do the following:

- View objects using the user interface;
- Log off current SecurOS user and close SecurOS *Client application*;

Click the **Next** button.

6. The **Video Server settings** window will appear (see figure 20).

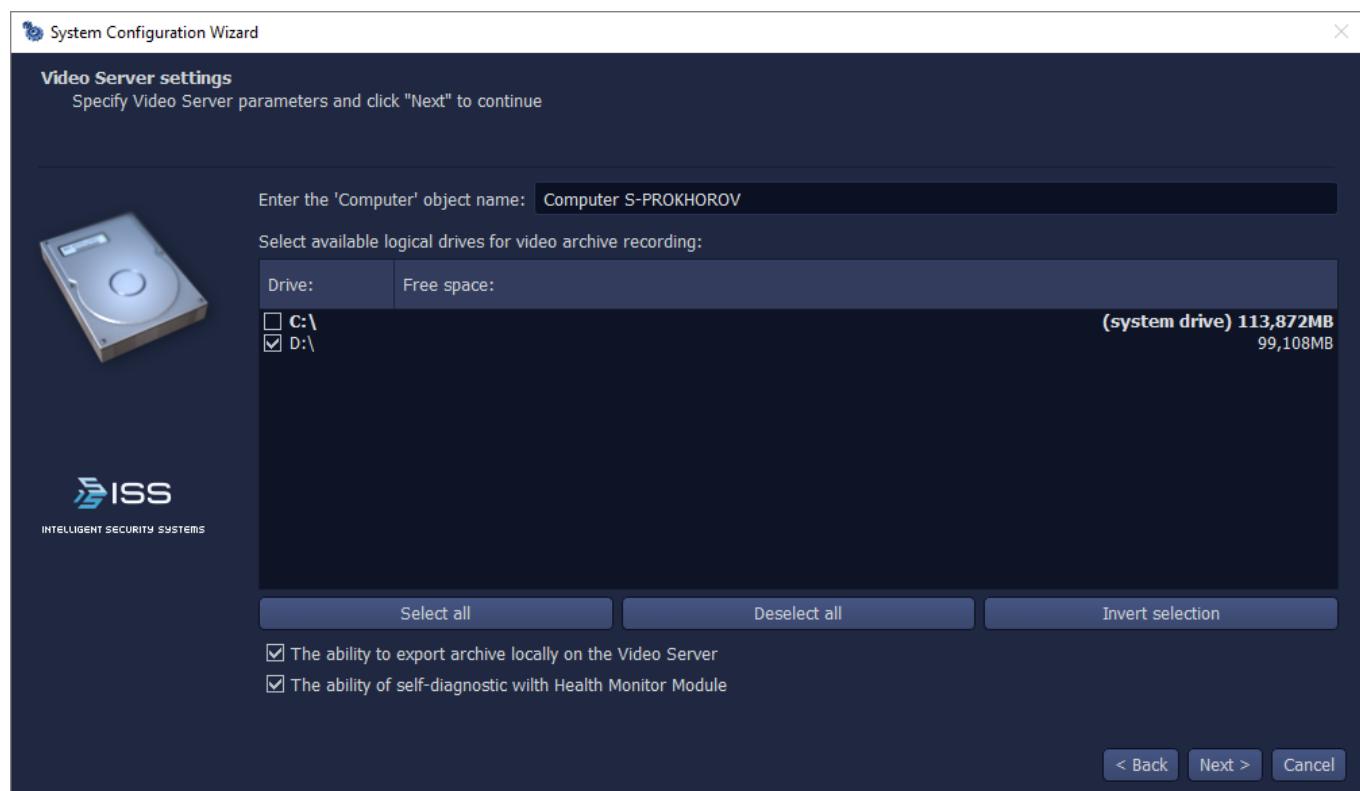


Figure 20. Computer name and video archive setup window

Do the following:

- If necessary edit the *Computer* object name in the **Enter the 'Computer' object name** field. By default the computer name is set by system in the following way: *Computer <computer_name>* (see **Computer Name Restrictions** section).
- Choose **Drives** to store recorded video by selecting the corresponding drive from the **Select available logical drivers for video archive recording** table. SecurOS will store the recorded video

on the drives specified in this window.

- If the local export of video records isn't required, clear the **The ability to export archive locally on the Video Server** check-box that was set by default.

Additional information

The given parameter regulates the possibility to create the additional objects (allowing to save video records on a hard disk of the given computer) on the *Video Server*.

- If self-diagnostic with the built-in tool on the *Video Server* is not required, clear the **The ability of self-diagnostic with Health Monitor Module** checkbox that was set by default.

Click the **Next** button.

7. System will display the **Add and configure IP devices** window (see figure 21).

If it is necessary to operate with network IP-devices (for example, IP cameras), click the **Add** button. System will add a new line in the **List of IP-devices** block. Set IP device parameters by clicking the necessary field. Repeat the operation for all required IP devices.

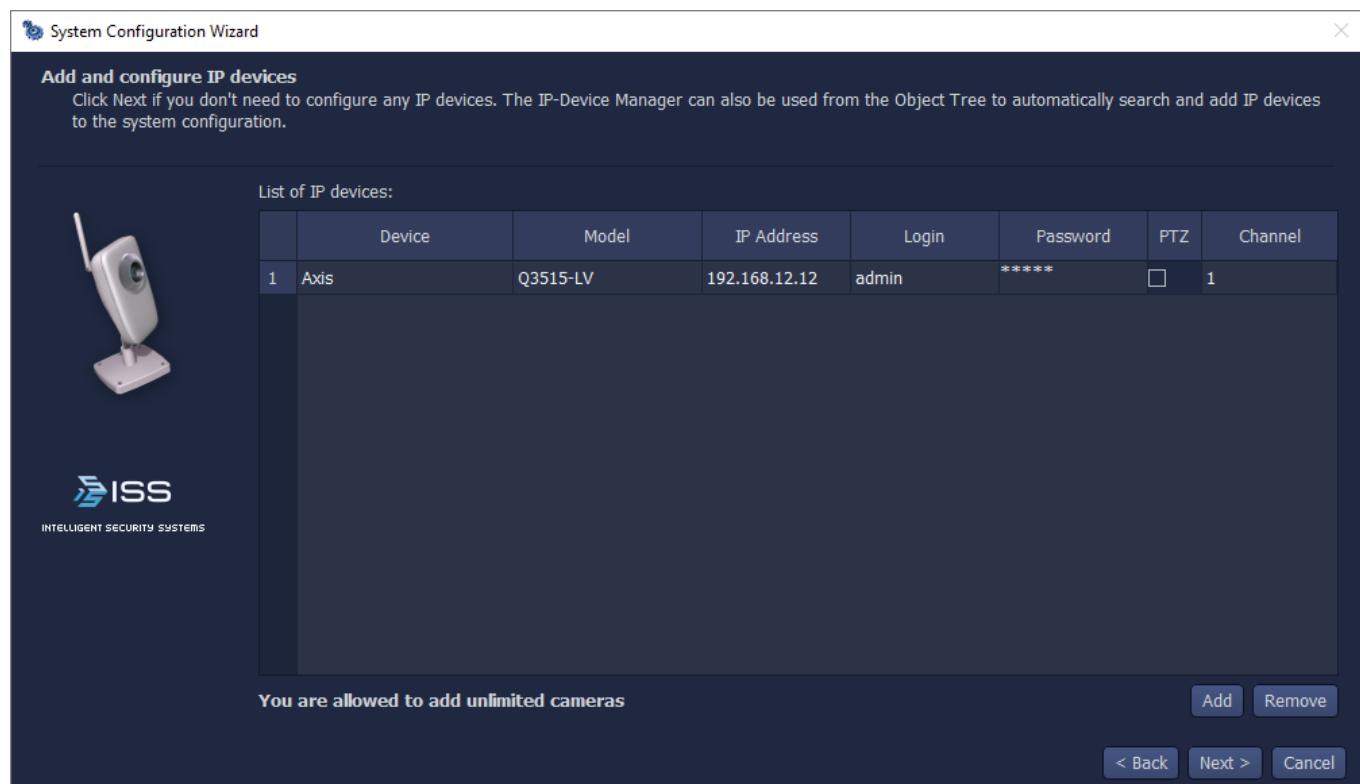


Figure 21. Add and configure IP devices window

Click the **Next** button.

Note. IP devices can be added later.

8. The **Summary information** window will appear (see figure 22).

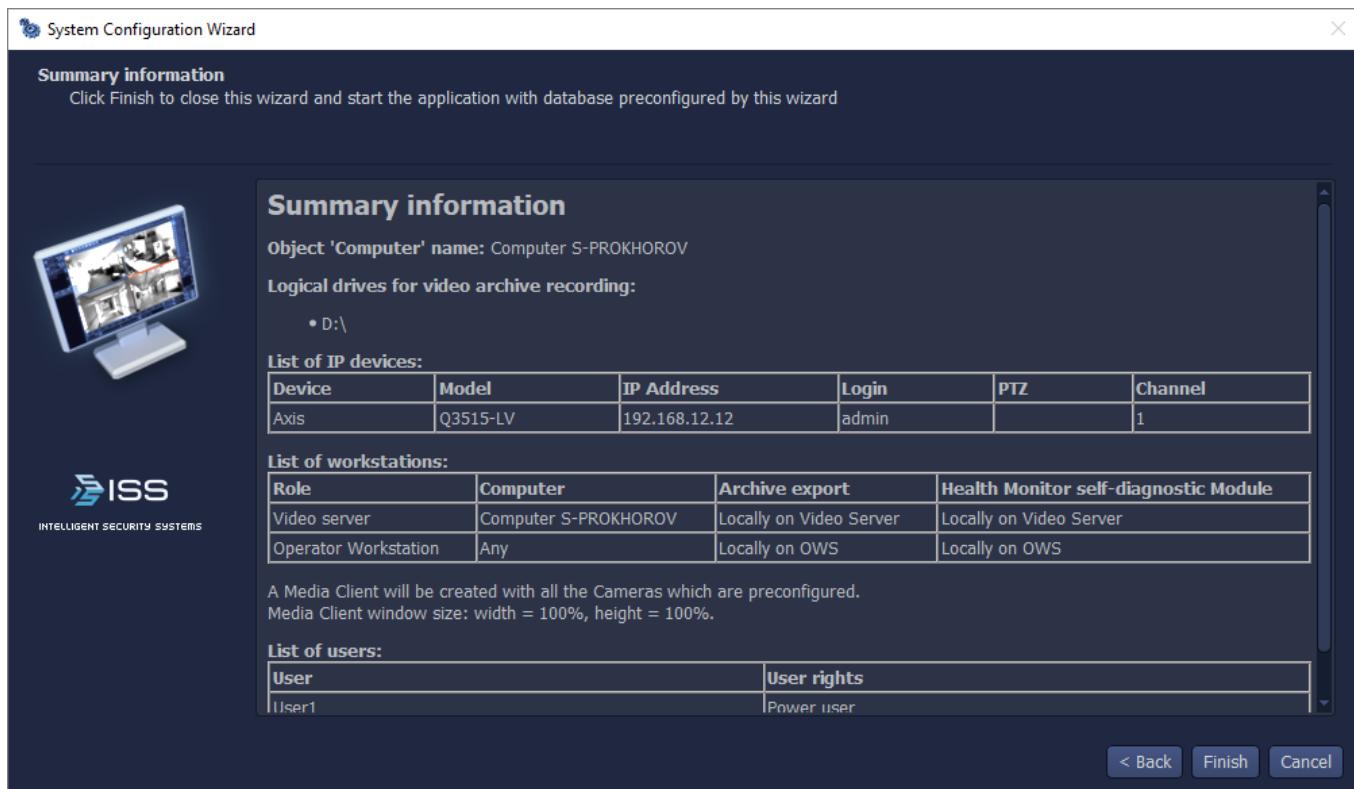


Figure 22. Summary information window

Information about server configuration parameters specified with the help of the *System Configuration Wizard* will be displayed in the table. In addition to the parameters above server will be configured so that any *Operator Workstation* located on any *Computer* within the SecurOS network can connect to it. The following operations will be available on each of these *Operator Workstations*:

- Export of the archive to the AVI and Evidence file formats;
- Self-diagnostic of the system with the help of the *Health Monitor* module (see [Health Monitor self-diagnostic Module](#)).

Review the selected system parameters. If it is necessary to change anything click the **Back** button. Set a new value. Click the **Next** button to return to the **Summary information** window. To create and save the configuration click the **Finish** button.

After the procedure of data creation and saving has completed successfully the corresponding message will be displayed (see figure 23).

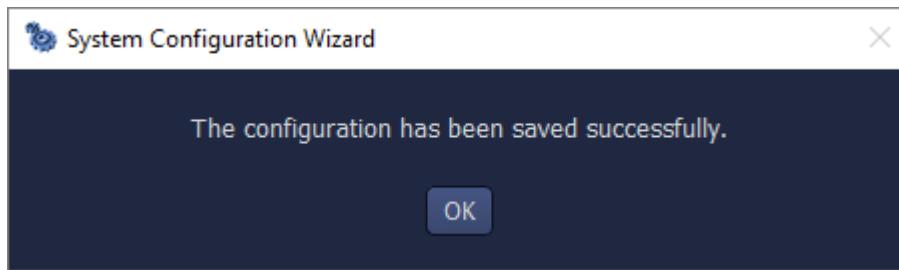


Figure 23. Successful configuration saving message

As a result of the described actions the system will be ready for operation.

3.1.4.2 Restoring Configuration

The backup copy allows to quickly and easily restore system configuration.

Warning!

1. Version of the backup copy should comply with the version of the currently installed SecurOS, otherwise it is not applicable. Backup copy creation procedure is described in the [System](#) section.
2. Restoring configuration is feasible only on the *Configuration Server* (see [Managing Network Configuration by Configuration Server](#)).

To restore system configuration from backup select **Import configuration file** scenario in the **Wizard scenario window** (see figure 24).

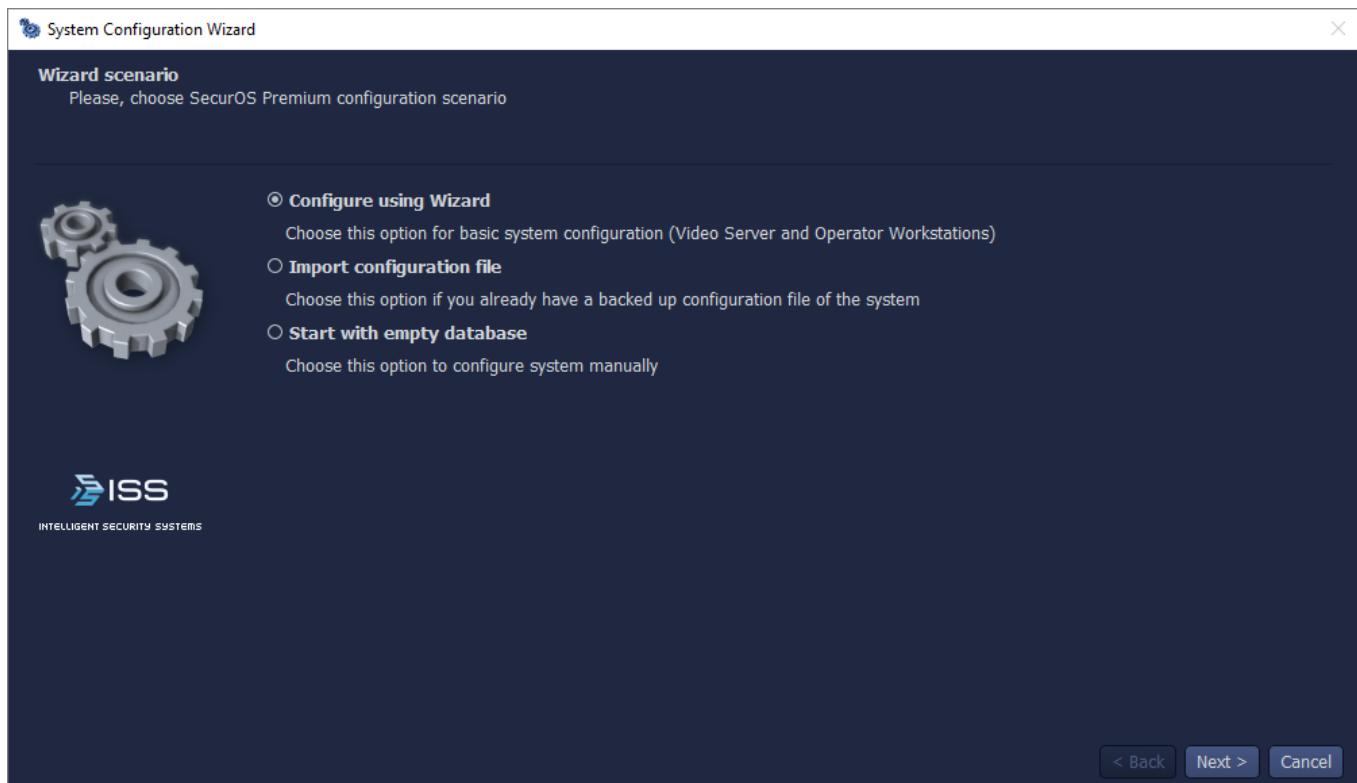


Figure 24. Wizard scenario Window

Click the **Next** button to continue and follow the Wizard.

3.1.4.3 Start with Empty Database

To start system with empty database select appropriate scenario in the **Wizard scenario** window (see figure 24). If this scenario is used the system start with minimal configuration containing one of each following types: *Security zone*, *Computer* and *Desktop*. Further system configuration is performed in manual mode.

3.1.5 Launching SecurOS On The Configuration Server

By default, the *Server part* of the SecurOS is launched automatically on the *Configuration Server* after SecurOS installation is finished and each time when OS starts.

To launch SecurOS client application on *Video Server* do the following:

1. In the **Start** Windows menu consistently choose the following menu options: **Programs** → **SecurOS** → **SecurOS** (see Figure 25).

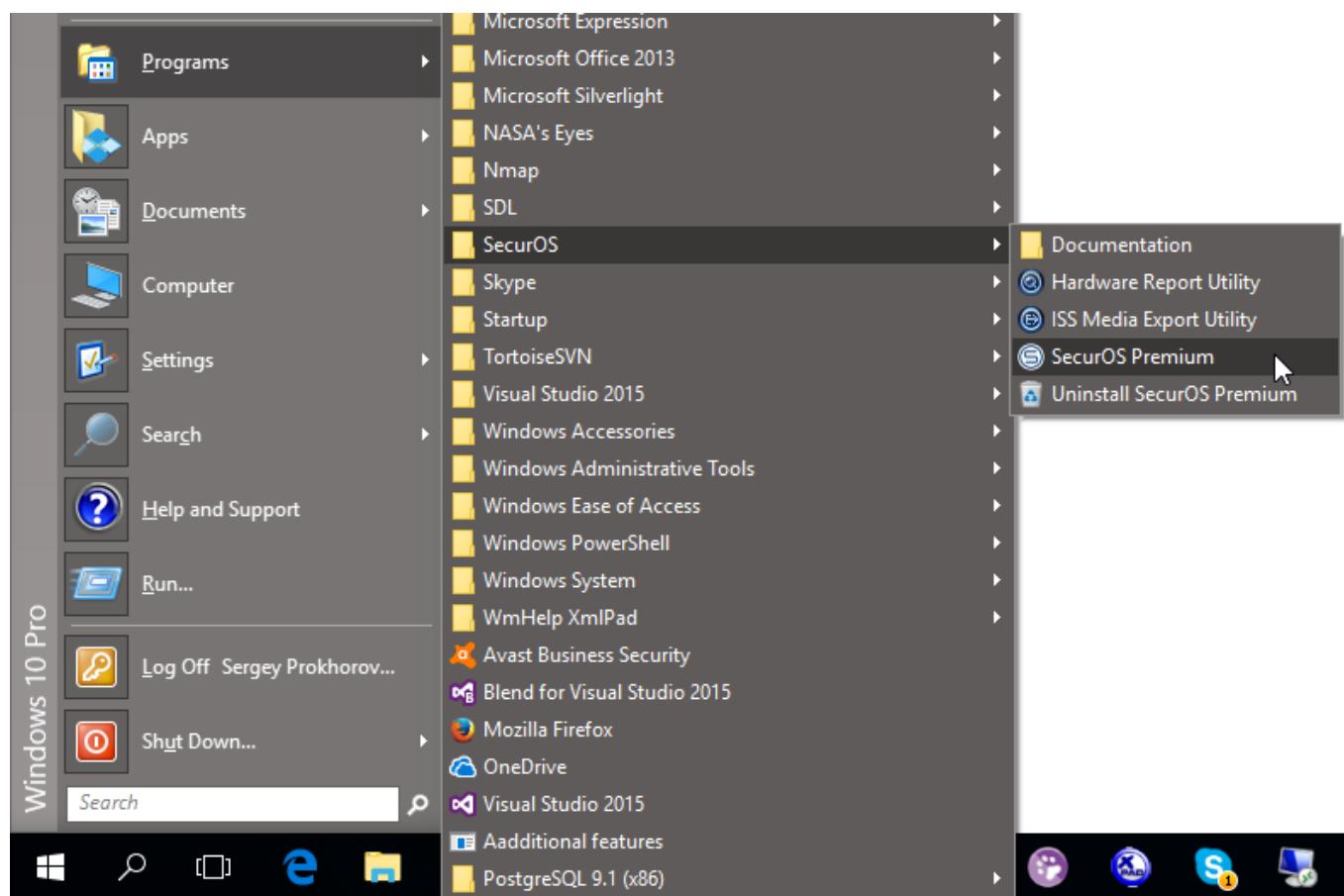


Figure 25. Start menu (All programs)

Additional Information

Client can also be launched with the help of the **Server Control Agent** utility, by means of the SecurOS shortcuts in the Start menu, on the Desktop or in the Windows taskbar.

The **Authorization** window is used to log in. It is displayed after the system has successfully started and loaded all configurations (see Figure 26).

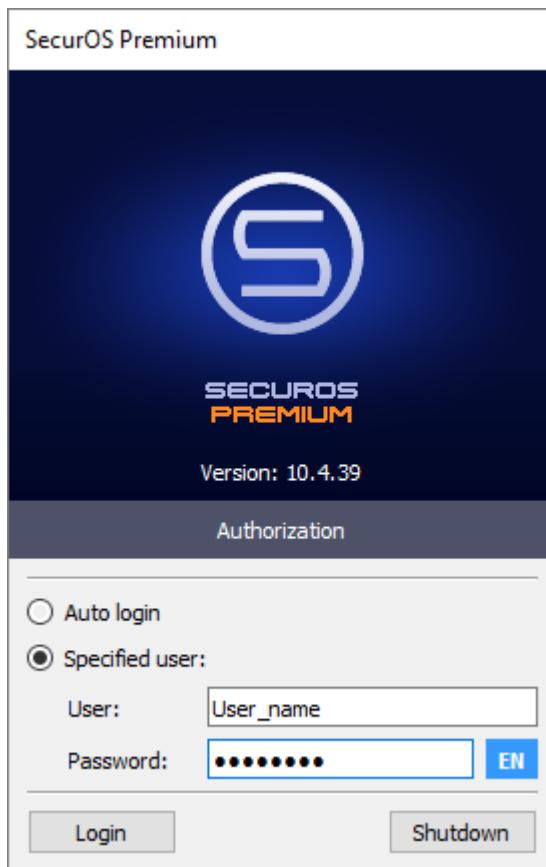


Figure 26. Authorization window

2. Select an appropriate option:

- **Auto login** – when selecting this option the credentials of the user specified by administrator in the system settings (see [Auto login](#)) will be used automatically. When system is started for the first time this option is selected by default.

Warning! Auto login is possible if this procedure is configured by the administrator.

- **Specified user** – when selecting this option specify **User** and **Password**, corresponding to the personal credentials of the SecurOS User.

Warning! At the first start select this option and use credentials of the superuser (see [SecurOS Users](#)) or other users, if they have been created with the help of the System Configuration Wizard.

3. Click the **Login** button.

3.2 Installing, Configuring And Launching Peripheral Servers

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*.

To add other *Video Servers* to the network it is necessary to do the following:

1. Add computers to the network for that create and configure the corresponding objects in the *Object*

Tree of the certain *Security Zone* object on the *Configuration Server*.

2. On the added computers install the SecurOS software, that corresponds to the *Peripheral server* role (see [Types Of Servers And Workstations](#) section).
3. Launch SecurOS and configure the system with the Wizard.

Warning! The possibility to add the given amount of the certain typed computers to the network is regulated by the license restrictions.

3.2.1 Adding To The Network And Configuring Peripheral Servers

To add a computer to the *Object Tree* do the following:

1. Enter the Administration Mode on the *Configuration Server* (see [SecurOS Administration Overview](#)).
2. In the *Object Tree* select the *Servers & Workstations* group, create a *Computer* child object and specify for it the *Video Server* role.
3. In the **Parameters of created object** window set the required values:
 - In the **ID** field set the computer name (see [Computer Name Restrictions](#)). It should correspond to the value defined in the OS settings (see [My Computer → Properties → Computer Name](#)).
 - In the **Name** field define the *Computer* object name as it will be displayed in the SecurOS *Object Tree*.
4. In the object settings window (see Figure 27) set the following obligatory parameters:

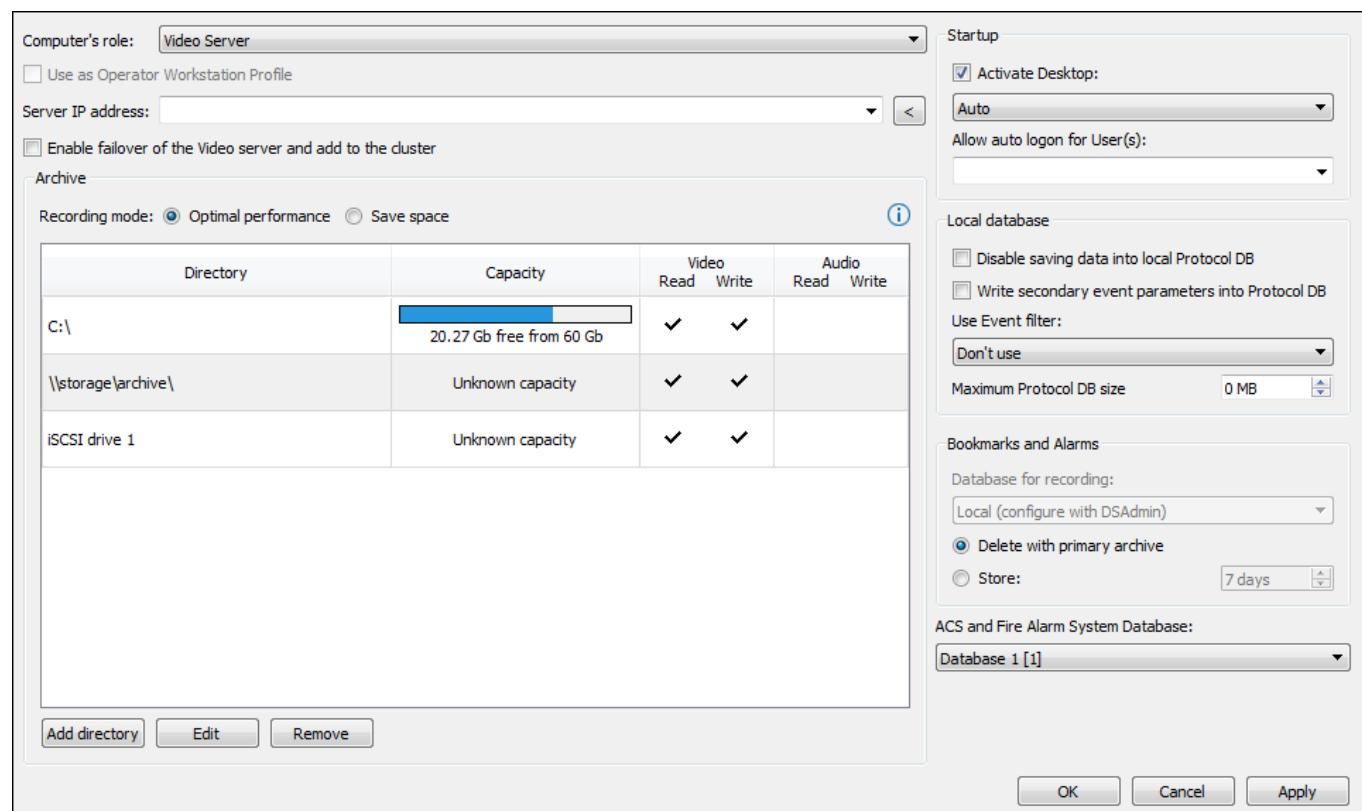


Figure 27. Computer object settings window

- *Server IP address* – the network address of the adding *Computer* object.

Note. Parameter is a mandatory one only if the network computers are registered in the different subnetworks.

- **Disk** – drives to save video and audio records.

Note. Without the parameter definition the video records saving will be impossible.

5. If needed set the other parameters. Apply new settings.
6. For the added *Computer* object create the own *Object Tree*. The type and content of the *Object Tree* is defined by a computer role in a network.
7. Repeat the steps for all added to the network computers.

3.2.2 SecurOS Installation On Peripheral Servers

To install SecurOS software on peripheral servers (other *Video servers* that are not *Configuration Server*) do the following:

1. To start SecurOS software installation on additional servers setting launch the product installation file on the corresponding computer.
2. Up to the server type selection step in the **Server type** window steps of the procedure are similar to software setting on the *Configuration server* (see [Software Installation](#) section).
3. In the **Server type** window (see figure 28) set the *Peripheral Server*.

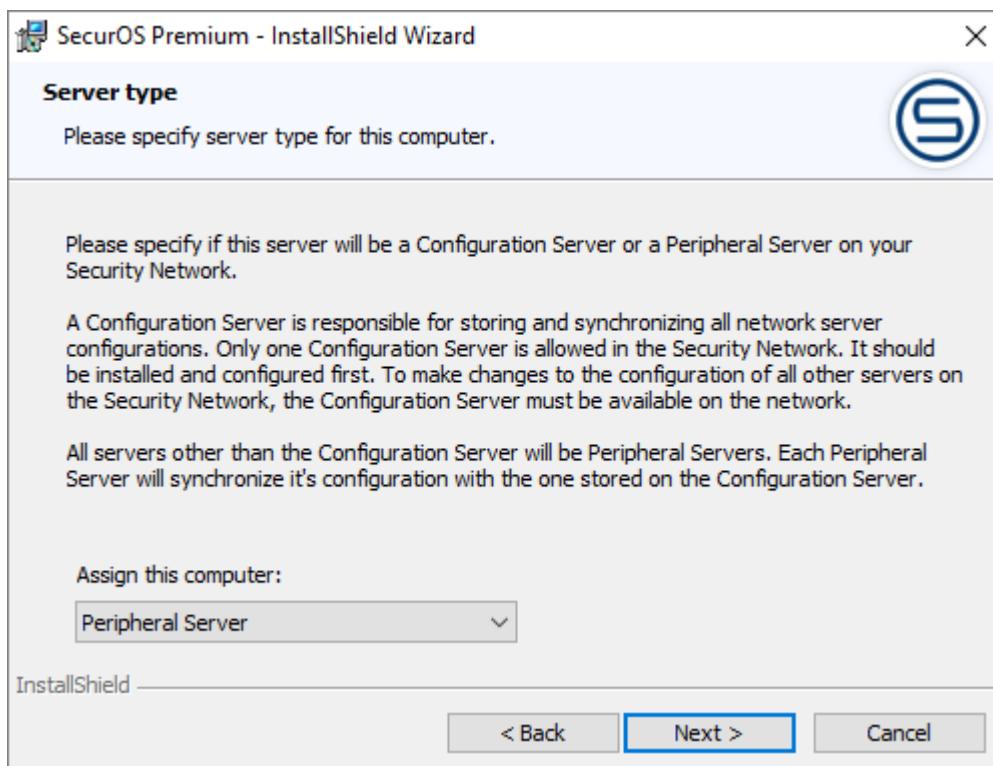


Figure 28. Server Type window

4. The further steps are similar to the software installation on the *Configuration Server* (see [Software Installation On The Configuration Server](#) section). When setting parameters It is recommended to use default values.

3.2.3 Launching And Configuring SecurOS On Peripheral Servers

By default, the *Server part* of the SecurOS is launched automatically on the *Peripheral Server* after SecurOS installation is finished and each time when OS starts.

Initial configuration of the SecurOS on *Peripheral Server* is performed with the help of *System Configuration Wizard*. To configure SecurOS for the first time by means of the Wizard, perform the following steps:

1. Start SecurOS *Client application* by selecting **Programs → SecurOS → SecurOS** from **Start Windows menu**. When *Client* is started for the first time, then *System Configuration Wizard* will appear.

Note. Client can also be launched with the help of **Server Control Agent** utility.

2. In the **Join existing security network** window (see figure 29) do one of the following to choose the *Configuration Server* with the current network configuration:

- Set *Configuration Server* name or IP address in the **Configuration server name or IP address** field.
- For automatic search for Video Server in the network click **Find servers in the local network** button. The searching procedure will be started and *Configuration Server* will be displayed in the **Servers found** box. Click found *Configuration Server* to select it.

Warning!

1. During the configuration procedure the *Configuration Server* must be active and the SecurOS should be launched on it.
2. To provide execution of the SecurOS servers search function in the local network it is necessary do the following:
 - launch the **Computer browser** system service on the DC;
 - launch the **Server** system service on the server;
 - turn on the **SMB** protocol on the server (**Turn Windows features on → SMB 1.0/CIFS File Sharing Support**).

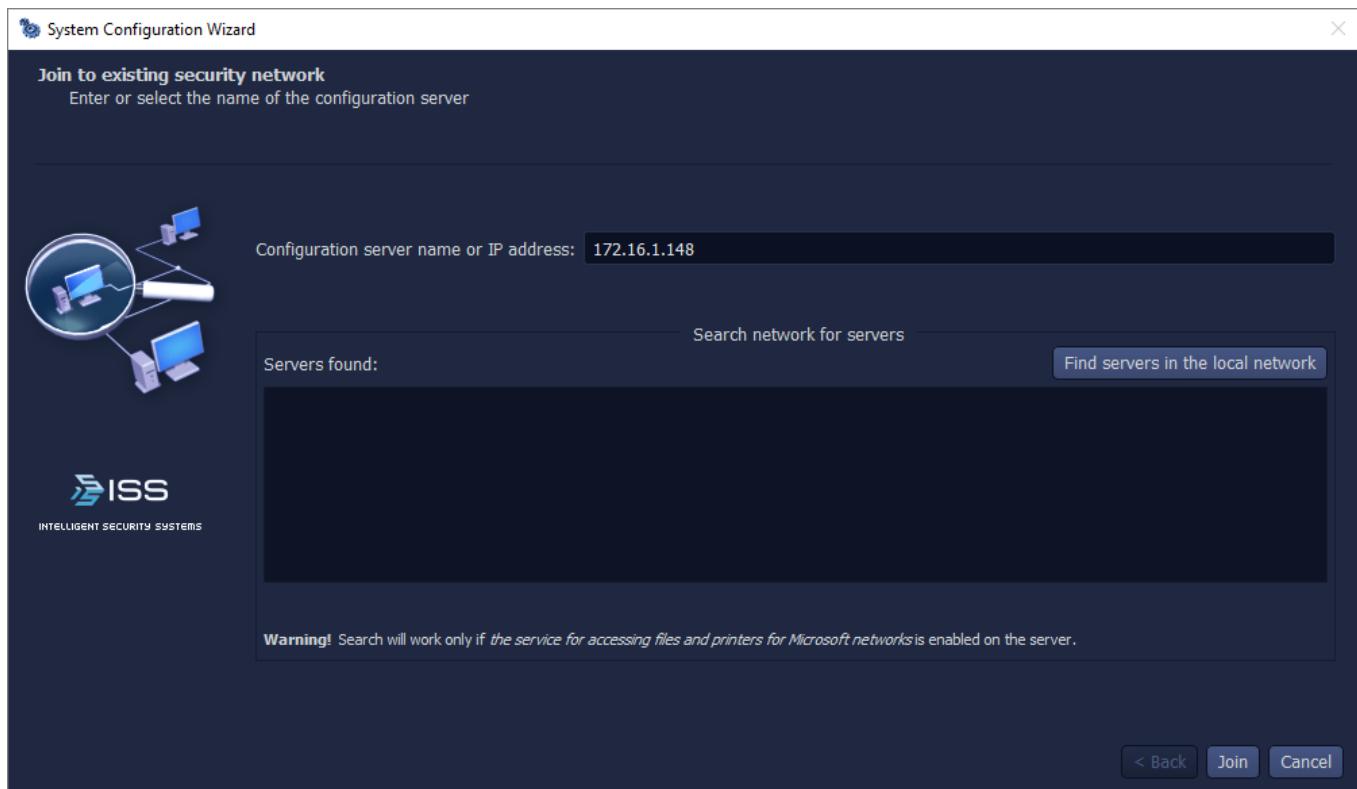


Figure 29. Join existing security network window

Click the **Join** button. The **Loading configuration** window will appear that indicates the loading process.

3. After the configuration loading finished successfully the corresponding system message will be displayed. Click on **OK** button. In the **Loading configuration** window click the **Finish** button.

3.3 Installing, Configuring and Launching Operator Workstations

To prepare *Operator Workstation* it is enough to install SecurOS software on the computer. Installation procedure is described in the [SecurOS Installation On Operator Workstation](#).

Launching operator interface on the *Operator Workstation* is possible immediately after installation (see [Launching SecurOS On Operator Workstation](#)). To connect to the *Video Server* it is enough to know its IP address or DNS/WINS name. When system starts for the first time operator can operate only with such SecurOS administrative tools, as *Control Panel* and *Object Tree*.

Note. Administrative tools are available only if SecurOS user has a rights to configure the system (see [User Rights](#)).

For further work it is necessary to create *Operator Workspace*, which is a collection of interface elements for monitoring and other features.

There are two types of the *Operator Workspace*:

- **Profile Workspace.** Such *Operator Workspace* corresponds to *Operator Workstation Profile* configuration (see [Operator Workstation Profiles](#)). It can be used on any number of computers.
- **Local Workspace.** Such *Operator Workspace* corresponds to the configuration of the *Computer* object, ID of which matches the DNS/WINS name of the computer, used by operator. It can be used on this computers. Use of local workspace allows to perform some operations only on certain computers. *Operator Workstations* that use local workspaces are called **Fixed**. Procedure for adding Fixed *Operator Workstation* to the network is described in [Fixed Operator Workstations](#).

Notes:

1. *Operator Workstation Profiles* can be used even on the Fixed *Operator Workstations*.
 2. By default, local workspace is available on those *Video Servers* where operator interface is being launched.
-

3.3.1 SecurOS Installation On Operator Workstation

To install SecurOS software on the *Operator Workstation* do the following:

1. To start SecurOS software installation on operator workstation launch the product installation file on the computer.
2. Up to the setting type selection step in the **Install type** window the steps of the procedure are similar to software setting on the video server (see [Software Installation](#) section).
3. In the **Install type** window select the **Advanced configuration options** type.
4. In the **Setup type** window (see figure 30) select the **Operator Workstation** installation type.

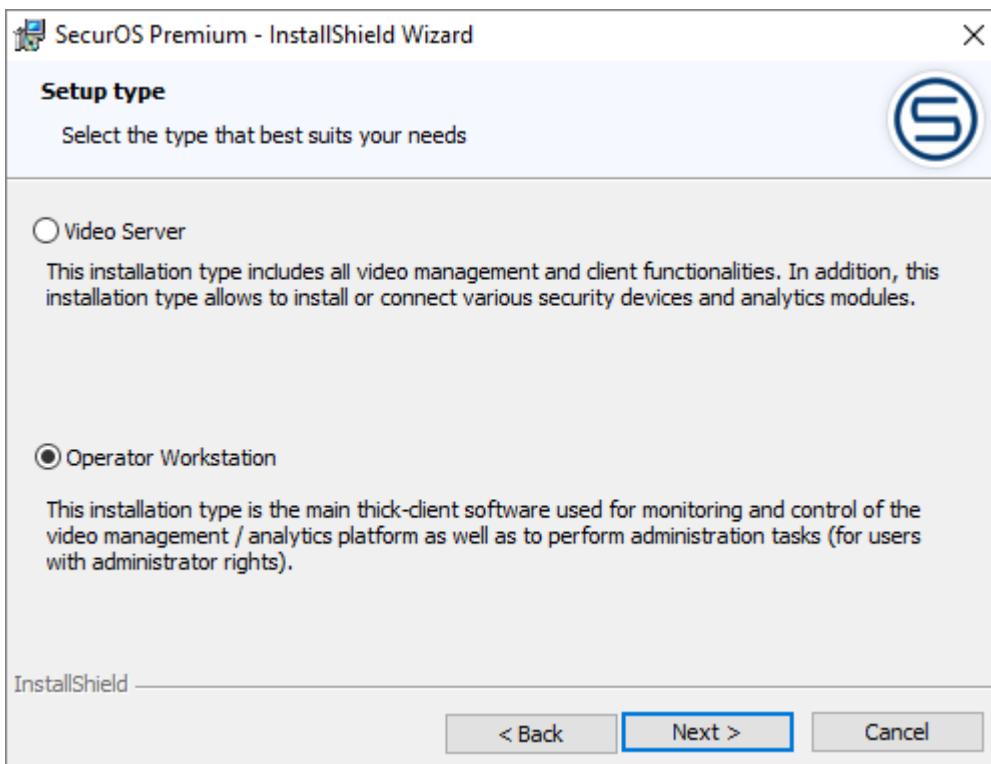


Figure 30. Setup type window

5. Follow the further InstallShield Wizard instructions.

3.3.2 Operator Workstation Profiles

Operator Workstation Profiles specify appearance of the operator interface and list of available modules. Each Profile can be used by unlimited number of *Operator Workstations*. This ensures unification of user interface and simplifies applying of changes. Any change of Profile will automatically applied for all *Operator Workstations* that use this Profile.

To use profile it is necessary to create and configure it first (see [Creating Operator Workstation Profile](#)), and then select it on the *Operator Workstation* as *Operator Workspace* (see [Changing Operator Workspace](#)).

Note. Availability of the *Operator Workspace* to specific operator is defined by system settings. User access to the profiles can be restricted via [User Rights](#). Profile is accessible, if operator has the  (View) access right to this Profile or above.

3.3.2.1 Use Restrictions

The following objects and Modules are not supported when using *Operator Workspace* (exclude *Local Environment*) on the *Operator Workstation*:

- [AC Recorder](#).

When using *Operator Workspace* the limitations for work with VB/JScript programs (scripts) and SecurOS messages are applied:

- To execute the *VB/JScript program* on the *Operator Workstation* it is necessary to create it as a child object to the same *Computer*, profile of which is used by the *Operator Workstation* as *Operator Workspace*. If the *Operator Workstation* uses *Local Environment* then the *VB/JScript program* must be created as a child object to the current *Computer*.
- SecurOS messages (events and reacts) received by the *Operator Workstation* that uses *Operator Workspace*, are not further transferred to the SecurOS network.

3.3.2.2 Creating Operator Workstation Profile

Operator Workstation Profile is represented in SecurOS configuration by the *Computer* object and its children objects. To create a profile do the following:

1. Enter the Administration Mode (see [SecurOS Administration Overview](#)).
2. In the *Object Tree* select the *Servers & Workstations* group, create a *Computer* child object.
3. In the **Parameters of created object** window set the required values:
 - In the **ID** field specify any value, that matches the requirements (see [Computer Name Restrictions](#)). For Profiles, the identifier does not have to match the DNS \ WINS name of the computer.
 - In the **Name** field specify name, that corresponds to *Profile* purpose (for example, **Building protection**). This name will be displayed in the list of *Operator Workspaces*, available to operator.
 - In the **Computer's role** drop-down list choose the *Operator Workstation*.

4. In the computer parameter settings window (see Figure 31) tick the **Use as Operator Workstation Profile** checkbox.

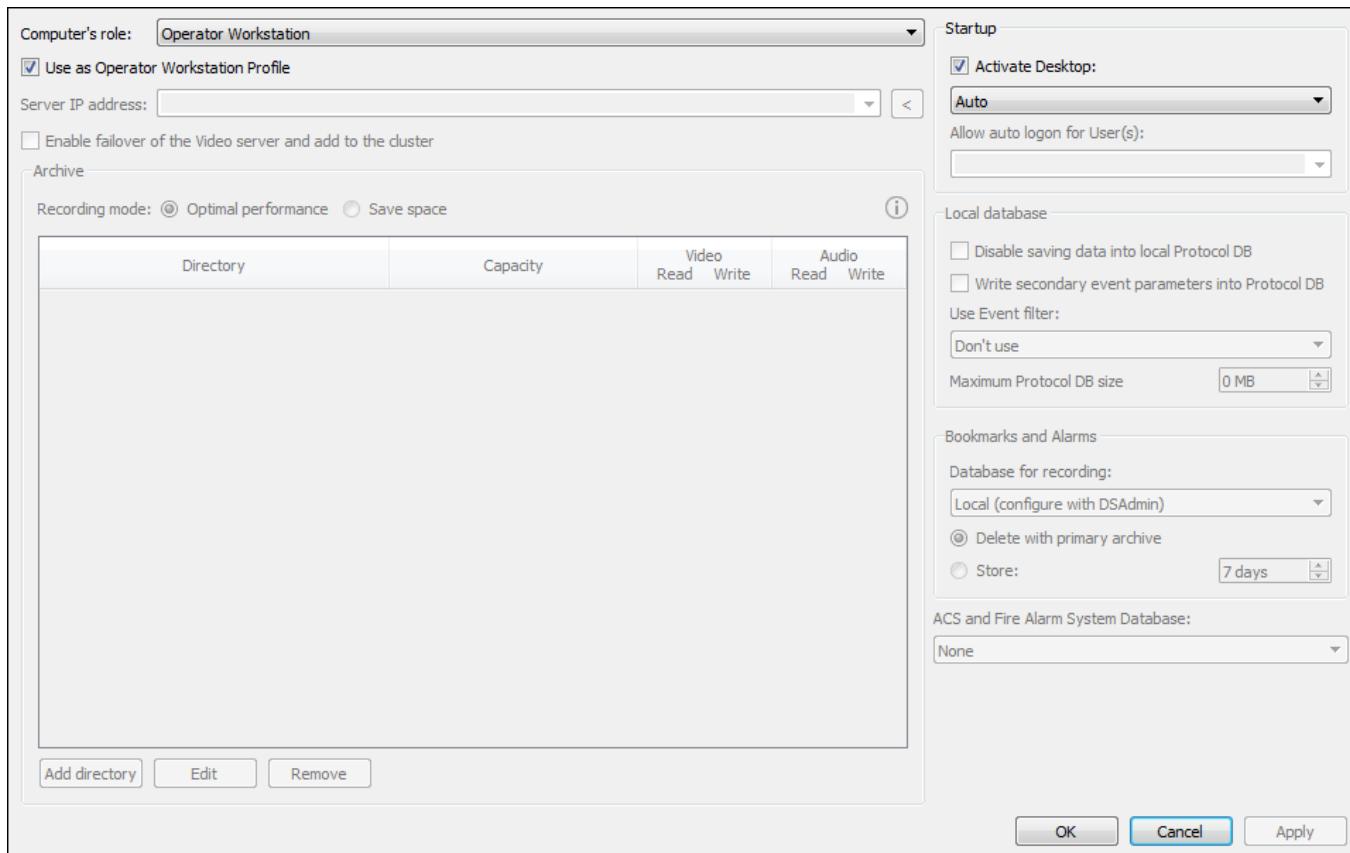


Figure 31. Computer object settings window

5. For given *Computer* create all children interface objects, required for the operator (for example, *Media Client*, *Event Viewer*). Configure these interface objects in accordance with your requirements to this Profile (for example, specify *Media Client* window size and working modes, specify list of available *Cameras*).

After that Profile can be used by operator as *Operator Workspace* (see [Changing Operator Workspace](#)).

3.3.3 Fixed Operator Workstations

In some cases, it may be necessary for a certain features to be available to operators only on specific computers. To solve this task one can use the Fixed *Operator Workstations*.

For such Fixed *Operator Workstations* the **Local Workspace** is used as *Operator Workspace*.

3.3.3.1 Adding To The Network And Configuring Fixed Operator Workstations

Fixed *Operator Workstations* are represented in SecurOS configuration by the *Computer* objects. To add a computer to the network do the following:

1. Enter the Administration Mode (see [SecurOS Administration Overview](#)).
2. In the *Object Tree* select the *Servers & Workstations* group, create a *Computer* child object.
3. In the **Parameters of created object** window set the required values:

- In the **ID** field set the computer name (see [Computer Name Restrictions](#)). It should correspond to the value defined in the OS settings (see [My Computer → Properties → Computer Name](#)).
- In the **Name** field define the *Computer* object name as it will be displayed in the SecurOS *Object Tree*.
- In the **Computer's role** drop-down list choose the *Operator Workstation*.

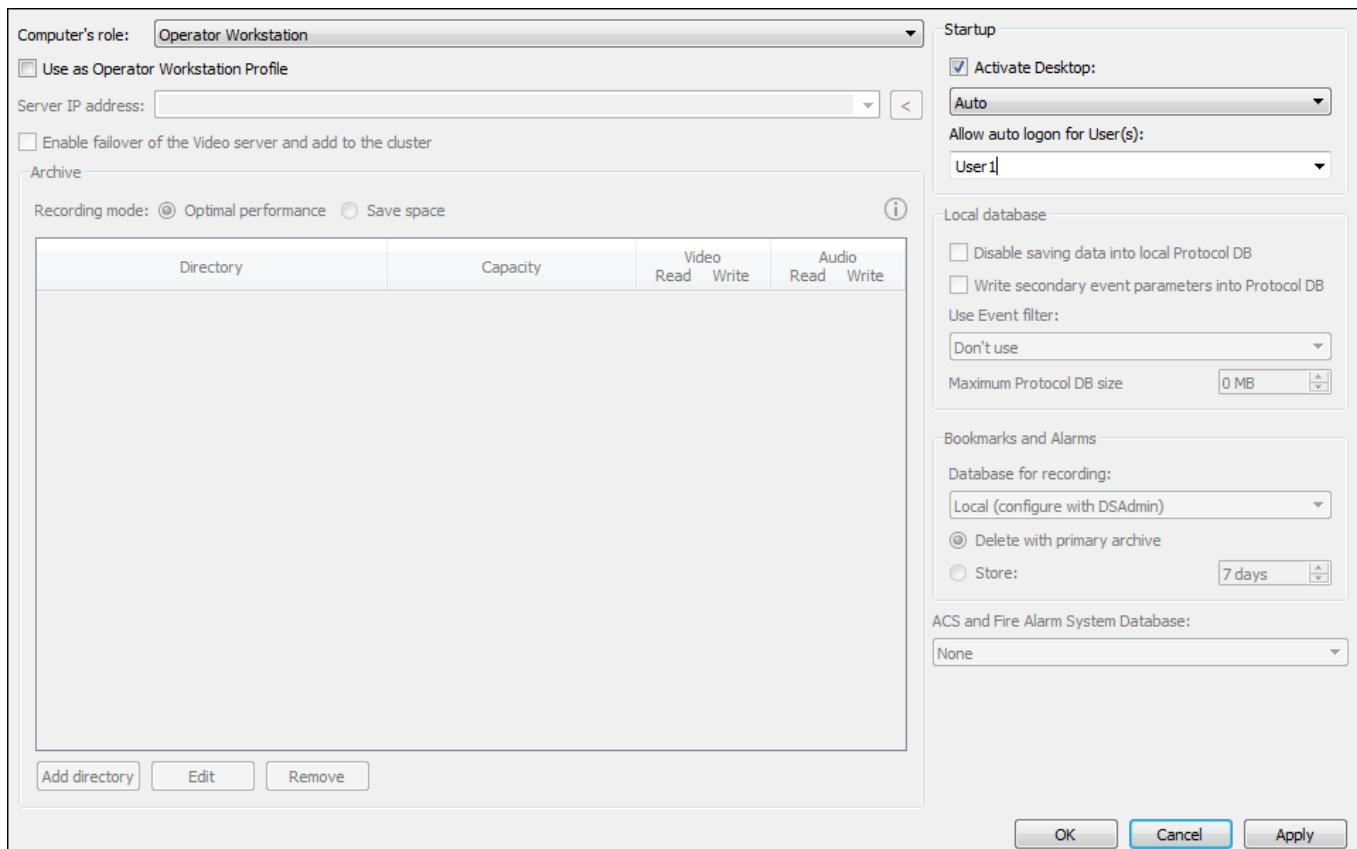


Figure 32. Computer object settings window

4. If necessary, specify other parameters (see Figure 32). Apply new settings.
5. For the created *Computer* create all necessary children objects. Set of such children object is defined by tasks, that will be performed on this *Operator Workstation*.
6. Repeat the steps for all *Operator Workstations* added to the network.

3.3.4 Launching SecurOS On Operator Workstation

To launch SecurOS *Client application* on *Operator Workstation* do the following:

1. In the **Start** Windows menu consistently choose the following menu options: **Programs → SecurOS → SecurOS**.
2. In the **Authorization** window (see Figure 33) in the **Connect to** field specify IP address of the *Video Server* to connect.
3. Select an appropriate option:
 - **Auto login** – when selecting this option the credentials of the user specified by administrator in the system settings will be used automatically. When system is started for the first time this option is selected by default.

Warning! Auto login is possible if this procedure is configured by the administrator (see [Auto login](#)).

- **Specified user** – when selecting this option specify **User** and **Password** that match credentials of the *User* earlier created by administrator or use superuser account credentials (see [SecurOS Users](#)).

4. Click the **Login** button.

For more information about the authorization see [SecurOS Quick User Guide](#).

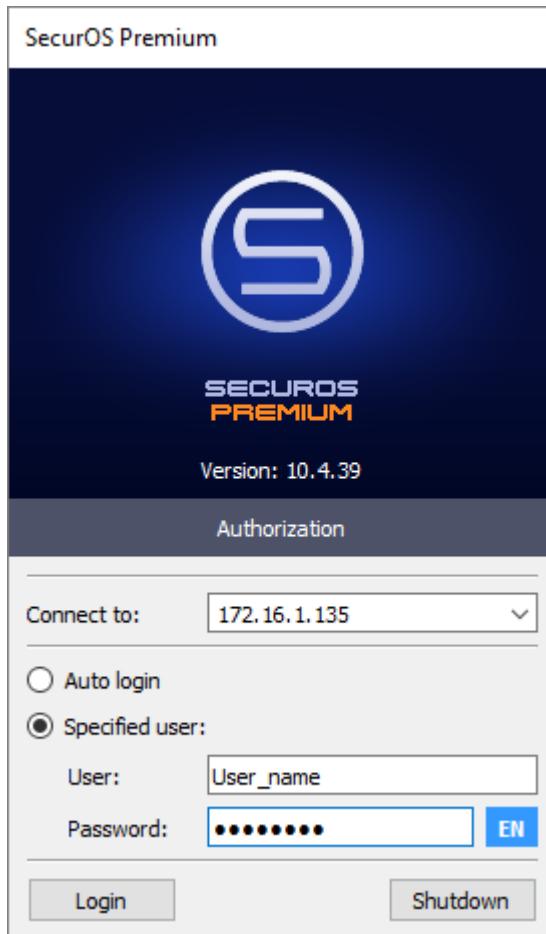


Figure 33. Authorization window

5. After successful authorization, the operator interface will be displayed on the screen. When connecting for the first time *Operator Workspace* will be selected automatically. If there is a local workspace for this computer, then it will be used. Otherwise one of the available profile workspaces will be used randomly. Later operator can change *Operator Workspace* (see [Changing Operator Workspace](#)).

Notes:

1. Possibility to connect to the server is controlled by the *Security Zone* object settings (see [Security Zone](#)) and *User Rights* (see [User Rights](#)). List of available *Operator Workspaces* is also defined by *User Rights*.
 2. For the Fixed *Operator Workstations* automatic authorization is possible for the user for which such possibility is specified by the administrator. To apply automatic authorization choose the **Auto login** option. Details of the automatic authorization procedure are described below (see [Computer](#) parameters description and [Auto login](#) section).
-

3.4 Installing Additional Multimedia Components

If *Video Servers* and *Operator Workstations* are running under MS Windows Server 2008 R2 it is necessary to install additional multimedia components required for proper operation of SecurOS (see [Installing Multimedia Components and Services under MS Windows Server 2008 R2](#) section for detailed description).

3.5 SecurOS Update Order

Correct SecurOS work is guaranteed in case the versions of the SecurOS software, installed on each computer of the system, coincide.

Usually, updates are applied to all computers of any system at the same time. If it is not possible to stop SecurOS on all computers within network at the same time, software upgrade procedure must be performed in the following order:

1. Stop, update and start SecurOS on *Configuration Server*.
2. Sequentially stop, update and start SecurOS on *Peripheral Servers*.
3. Sequentially stop, update and start SecurOS on *Operator Workstations*.

Update should be carried out with the following restrictions:

- During the upgrade, it is strongly recommended not to change the system configuration. Otherwise, those *Peripheral Servers*, software on which is not updated, will not be able to receive modified configuration from updated *Configuration Server*.
- Software update on the *Peripheral Server* should be carried out only if the *Configuration Server* is enabled and available on the network from the computer, on which the update is performed.

When upgrading one must also consider the features specific to some SecurOS versions (see [SecurOS Version Upgrade Features](#) in the Appendix A).

Software updating procedure on separate computer is described in Appendix A (see [Upgrading Software](#)).

4 SecurOS Administration Overview

Administration mode is used to configure security network and its components. One can run this mode on any *Video Server* and *Operator Workstation*, if operator has appropriate privileges to configure system (see [User Rights](#)). All security system components remain completely functional when entering administration mode (without any restrictions).

Warning! After SecurOS and PostgreSQL software installation Windows OS creates the `postgres` account. To configure SecurOS system use an Windows administrator account but not the `postgres` one.

4.1 Working With Control Panel

The control panel is intended for opening *Administration Center*, *Desktop* and user session management, and also configuring the panel itself. In addition, the control panel can be used to open help documentation and to launch special system control commands (see [Macro](#) section). The control panel is represented in figure 34.



Figure 34. SecurOS Control Panel

Active *Desktops* and *Macros* control buttons (see [Disabling/Enabling Objects](#)) are placed in the panel. Number of these buttons is specified by system settings. If this number is exceeded, extra buttons are minimized and the corresponding menu for calling these objects is displayed on the panel:

- – for *Desktops*;
- – for *Macros*.

An active *Desktop* button is displayed in light blue (see Figure 34). If *Administration Center* is opened, then the **Configure the system** button is displayed in the same color.

See also:

- [Control Panel Activation, Configuring and Hiding](#);
- [Opening and Closing Administration Center](#);
- [Changing Operator Workspace](#);
- [User Session Administration and Client Shutdown](#);
- [Getting Help](#);

- [System Shutdown](#).

4.1.1 Control Panel Activation, Configuring and Hiding

This section describes typical operations with the *Control Panel*:

- [Control Panel Activation](#);
- [Configuring Control Panel](#);
- [Hide Control Panel](#).

Control Panel Activation

By default, after logging on the system, *Control Panel* is displayed on the Windows desktop. If there are several physical monitors connected to the operator's computer, panel is displayed on the first of them.

If *Control Panel* is not displayed on the Windows desktop, press and hold the **Ctrl** key, then move mouse pointer so it touches the top of the screen.

Note. Depending on operation mode, you can use different methods to activate the *Control Panel* (see [SecurOS Quick User Guide](#)).

Additional Information

The *Control Panel* also can be activated by clicking on the application icon in the Windows taskbar (system tray), or using the **Show Control Panel** command in the application icon context menu.

Configuring Control Panel

To set *Control Panel* call/hide method click on the  (Change user/Shutdown system) button, then select the **Configure Control Panel** command. In the **Control Panel settings** window (see figure 35) set the required parameters.

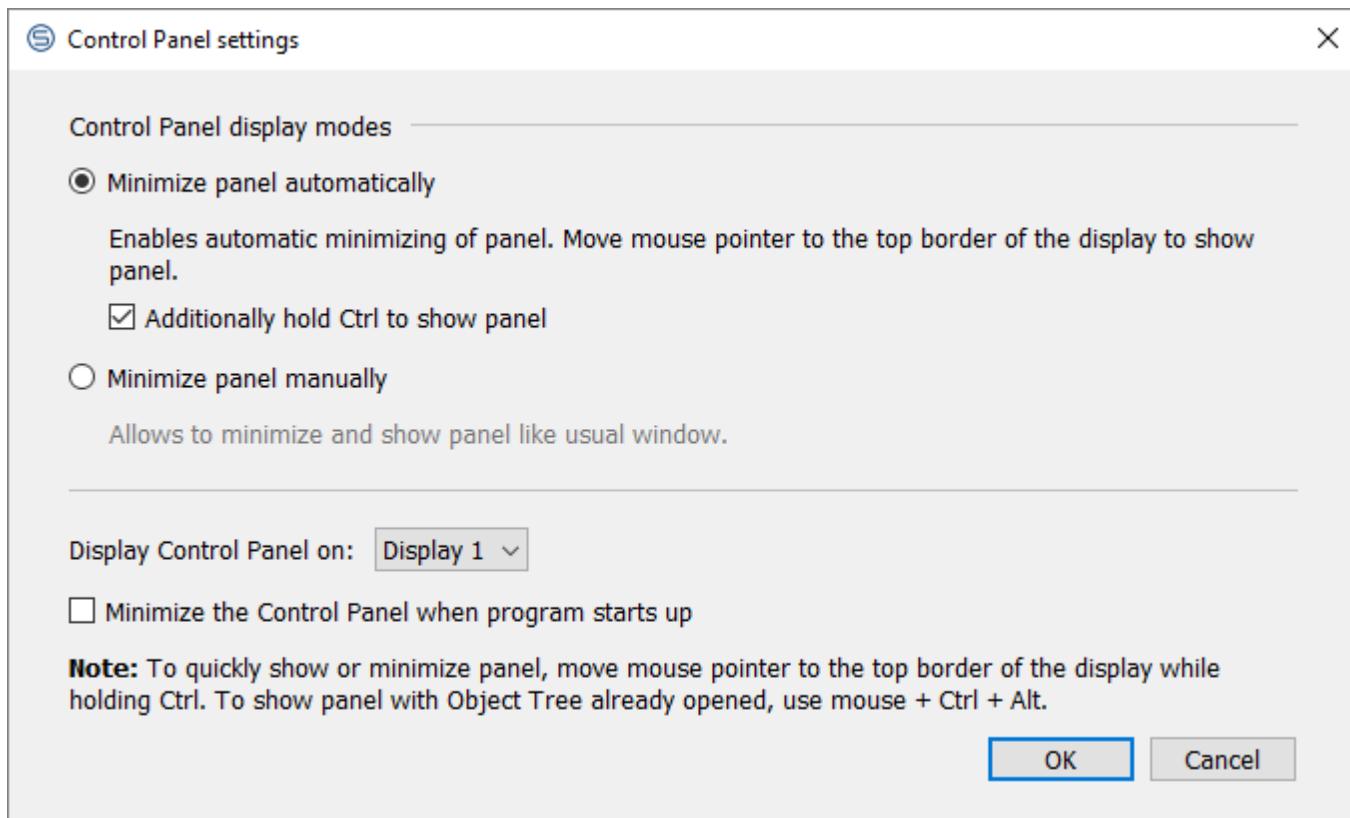


Figure 35. Control Panel settings window

Hide Control Panel

Method to hide the *Control Panel* depends on its current settings (see [Configuring Control Panel](#)):

- In the **Minimize panel automatically** mode panel is hiding itself, if the mouse pointer is no longer above the panel.

Note. Automatic hide of *Control Panel* is impossible if [Administration Center](#) is opened.

- To hide panel in the **Minimize panel manually** mode, click on the  (Minimize the Control Panel) button.

Note. The *Control Panel* can also be minimized by clicking its icon in the Windows Taskbar notification area (system tray), on the Windows Taskbar or with the help of application icon context menu in the system tray.

4.1.2 Opening and Closing Administration Center



To open *Administration Center* click on the ([Configure the system](#)) button in the [Control Panel](#).

Main window of the *Administration Center* will appear (see Figure 36).

SecurOS Administration Overview

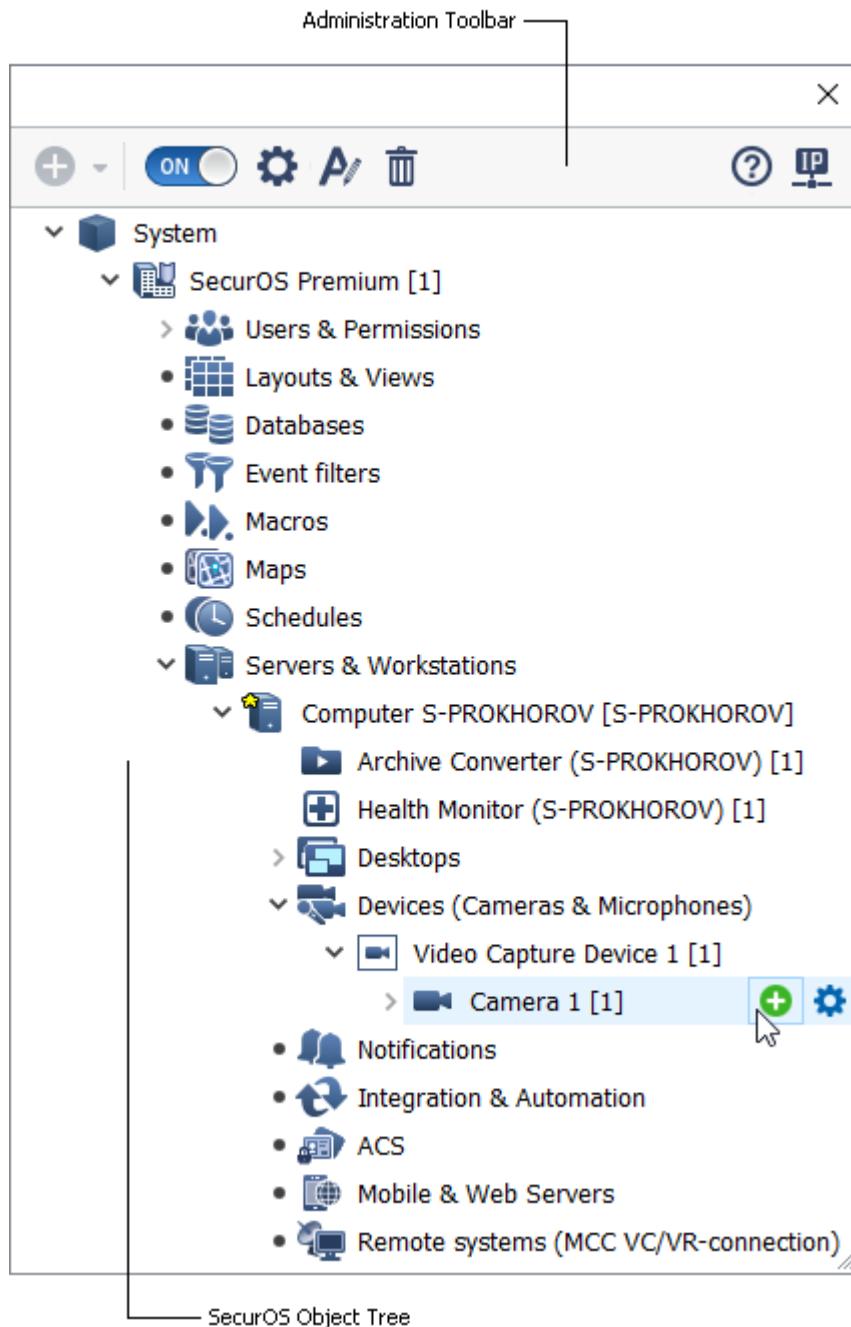


Figure 36. Administration Center



To close *Administration Center*, click on the button again.

See also:

[Administration Center](#).

4.1.3 Changing Operator Workspace

Created *Operator Workstation Profiles* (see [Operator Workstation Profiles](#)) are available for the operator as *Operator Workspaces*. *Operator Workspace* specify appearance of the operator interface and list of available modules. Each *Operator Workspace* can be used by unlimited number of *Operator Workstations*. Current *Operator Workspace* can be changed in *Control Panel*. To do this click on the **Change user**/



Shutdown system (), select **Change Operator Workspace**, then click on the required item (see Figure 37).

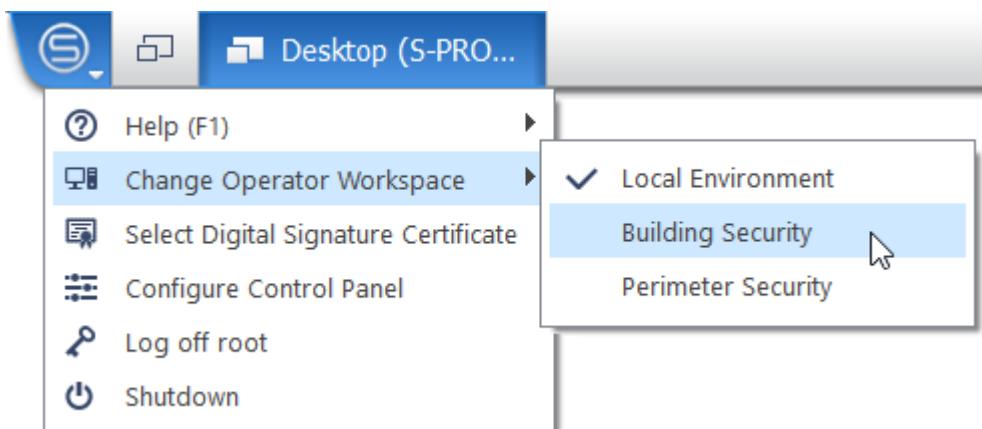


Figure 37. Change Operator Workspace

Current *Operator Workspace* will be marked with the ✓ sign. *Operator Workspace* configured on the fixed *Operator Workstation* (see [Fixed Operator Workstations](#)) is called *Local*.

Warning! Last time used *Operatator Workspace* is remembered only for Windows user.

For more information about how to use *Operator Workspace* see [SecurOS Quick User Guide](#).

4.1.4 User Session Administration and Client Shutdown

Using *Control Panel* one can change user or close *Client*. Click the **Change user/Shutdown system**



button () and from the drop-down list select a necessary command (see figure 38).

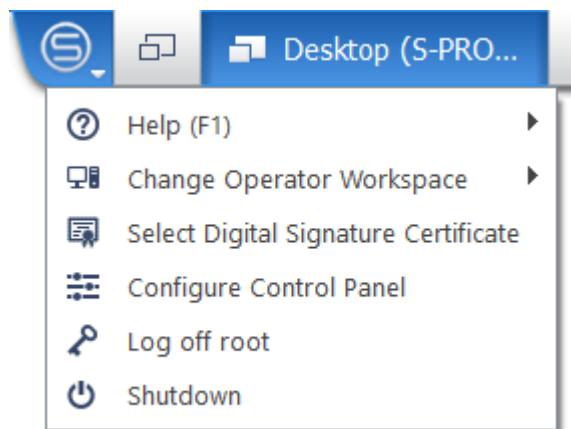


Figure 38. Change user/ Shutdown system menu options

4.1.5 System Shutdown

One can shut down the system (*Server part* of the SecurOS) using one of the following ways:

- Stop the *Server part* of the SecurOS with the help of the **Server Control Agent** utility.
- Stop the SecurOS Control Service. When stopping the service, the *Server part* of the SecurOS will be stopped automatically. The service also can be stopped with the help of the **Server Control Agent** utility or, when running Windows OS, with the help of the **Computer management** console (Computer → Manage → Services and Applications → Services).

4.1.6 Getting Help

When getting help, one can open the following descriptions:

- **Full list of the Manuals and Guides;**
- **Description of the Administration Center;**
- **Description of the SecurOS object settings.**

To open list of all available SecurOS Manuals and Guides you can use one of the following ways:

1. Click on the  (Change user/System shutdown) in the SecurOS Control Panel (see Figure 39):

SecurOS Administration Overview

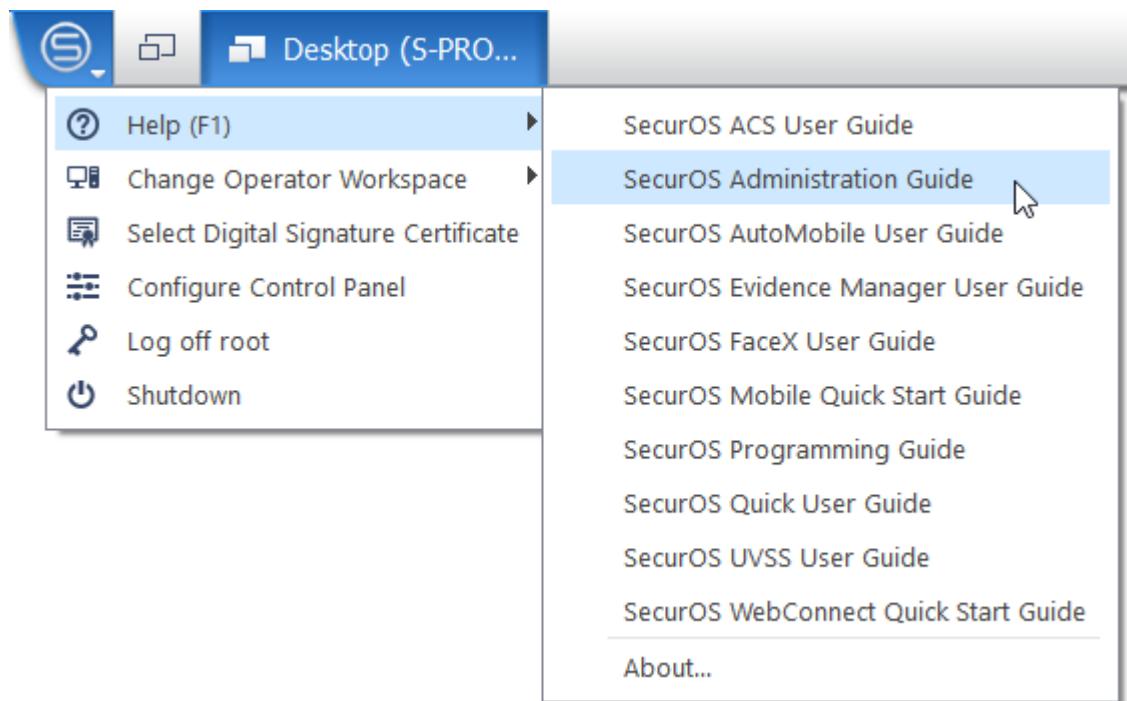


Figure 39. Getting help from the Control Panel

2. From the Windows task bar (system tray), by right clicking on the SecurOS icon (see figure 40):

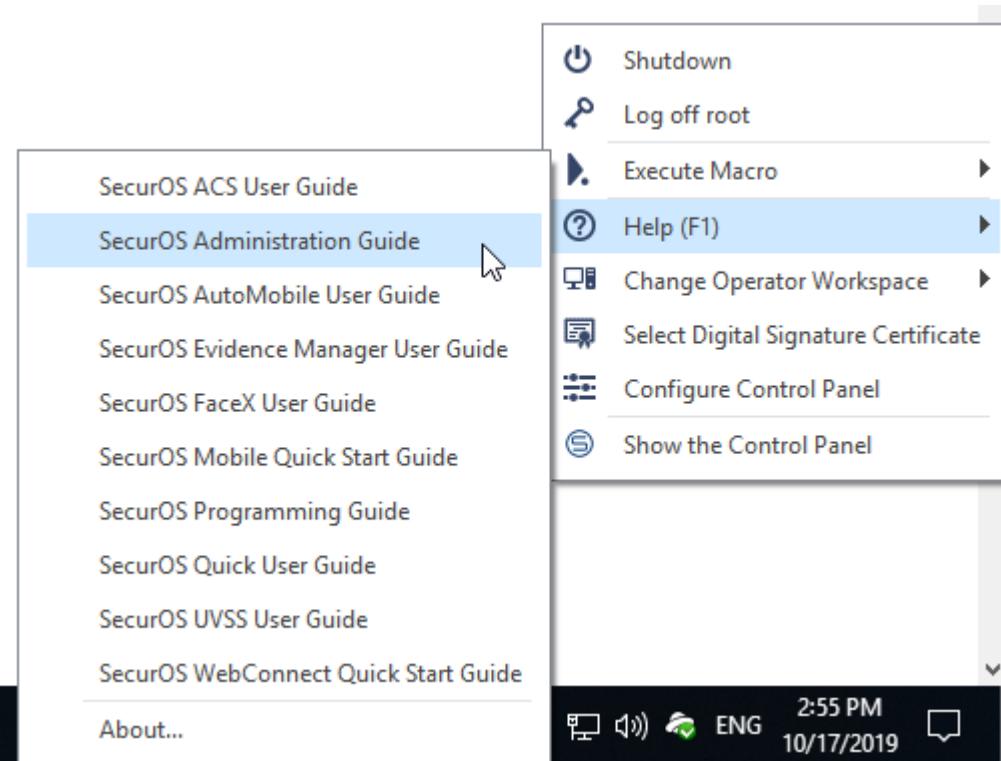


Figure 40. Getting help from the Windows system tray

3. From the Windows taskbar (**Start → All Programs → SecurOS → Documentation**).

To open description of the **Administration Center**, press the **F1** key or click on the  button in the **Administration Center**.

SecurOS Administration Overview

To open description of the object settings, open object settings window from the *Object Tree* and, further, press the **F1** key or click on the  button in the *Administration Center*.

4.2 Administration Center

To open *Administration Center* click on the  (Configure the system) button in the [Control Panel](#).

Administration Center contains [Administration Toolbar](#) and [Object Tree](#) (see Figure 41):

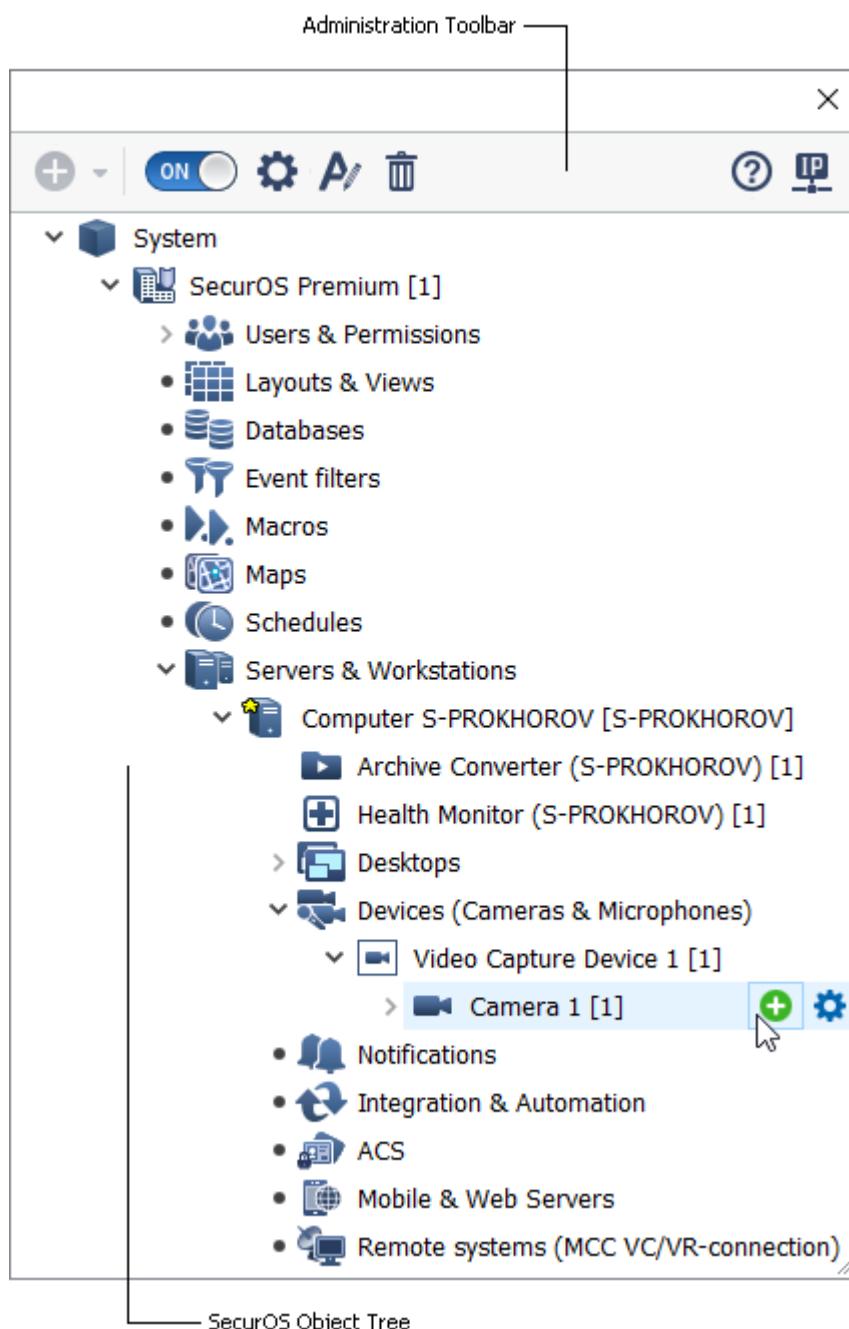


Figure 41. Administration Center

Administrator Toolbar

The Administrator Toolbar contains the controls (buttons) allowing one to make typical operations of the system administrator (see [Working with Objects](#)).

Administration operations are done with the SecurOS object selected in the *Object Tree*. The list of operations which can be done with an object (i.e. availability of each of the Toolbar buttons) depends on the selected object.

Object tree

The security system elements are displayed in the form of a object tree – the hierarchical structure reflecting correlations between them. The *System* object is the root element of the tree. All other SecurOS objects are its children.

Additional information

Objects which are one level down the hierarchy are called *child* objects to the object one level above them. The *parent* objects contain child objects.

There are two element types in the tree:

1. *Group* – this element is intended for grouping *Objects* by the functional sign. *Group* is being created automatically and can not be deleted by administrator. To the left from icon of the group there is an indicator. It can designate following group states:

- – group with no child objects ("empty" group).
- – group with some child objects.

Most group are child to *Security Zone*. Some groups are child to other SecurOS objects. For example, *Desktops* group is child to *Computer* object.

2. *Object* – the functional element of the security network. In the SecurOS tree it can be allocated only within a *Group*, if it is defined for the given type of object. An *Object* can be created, modified and deleted by administrator

There are two *object* classes in the SecurOS network: system objects and user interface objects. System objects reflect the network functionality, user interface objects are intended for security network monitoring and management.

The *Object Tree* is used to configure/manage any aspect of the system.

4.2.1 Working with Objects

Administration toolbar contains the following buttons to work with objects (see Figure 42):

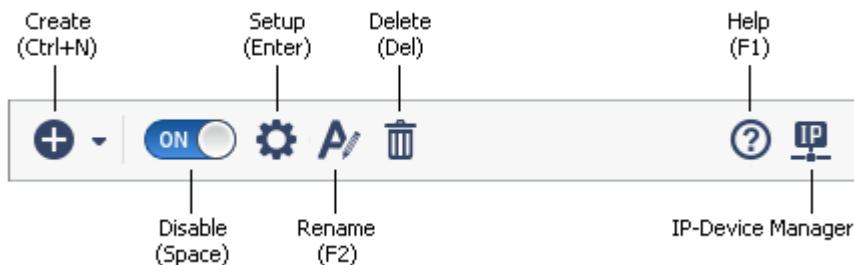


Figure 42. Administration Toolbar buttons

Note. If any operation is unavailable, the corresponding button is disabled.

- **Create** – create new object (child to selected object/group);

Warning! Object with the same hierarchy level can be created only from context menu of parent object/group.

- **Disable/Enable** – disable/enable object. When executing an operation, this button changes its appearance and reverts an action;
- **Setup** – open/close object's settings window;
- **Rename** – rename object;
- **Delete** – delete object;
- **Help** – call help (context dependent on the currently selected object in the *Object Tree*);
- **IP-Device Manager** – open the IP-Device Manager utility to search for IP devices within the SecurOS security network and add them to the system configuration.

Administration Toolbar's buttons are duplicated by commands of the object's context menu (for example, see Figure 43):

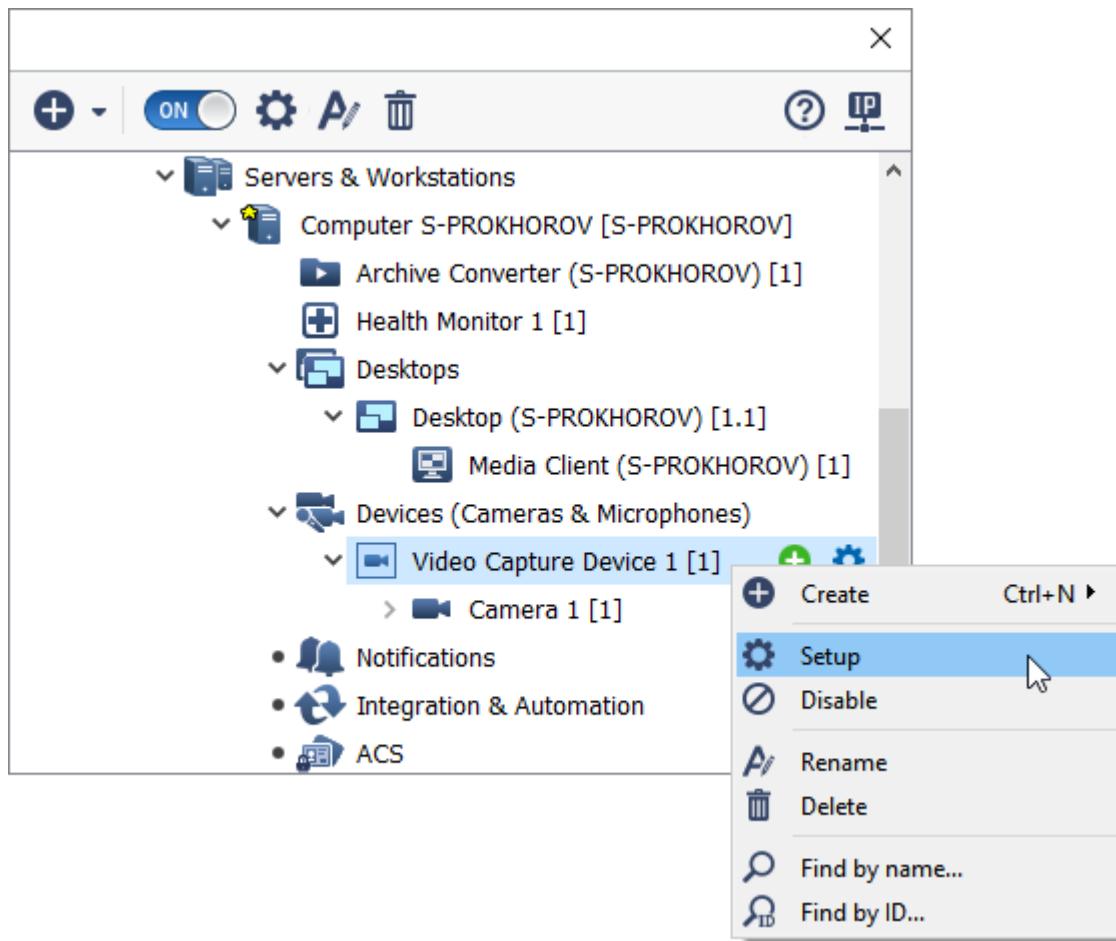


Figure 43. Object context menu

To call context menu right click on the required object. Context menu allows the following additional operations with objects: **Find by name** and **Find by ID** (see [Searching objects](#)).

4.2.1.1 Creating Objects

To create a new object:

1. Select a parent object in the *Object Tree*.



(Create) button

2. In the Administration toolbar or to the right from the object click on the (Create) button and choose the necessary object type from the drop-down list.
3. In the **Parameters of created object** window set the **ID** and **Name** of the object. Click on the **OK** button.
4. In the object's settings window specify the required values. Apply changes.

Creating Objects Limits

Limits of the system configuration (amount of objects of each type within the security network) is specified in the license key file (`key.iss`). If you have created maximum number of object of particular type, then you will not be able to add extra objects of this type into the SecurOS network. To be able to have more objects of this type, contact our Technical Support Team to get the new key (see [Updating License Key on All Servers](#)).

Warning! If maximum number of objects is exceeded when copying objects with the help of *IP-Device Manager*, the system will display the appropriate message. Only permitted number of object copies will be created.

4.2.1.2 Editing Object Settings

To edit or view an object's settings:



1. Select an object in the *Object Tree*, then click on the (Setup) button on the Administrator Toolbar or on the right of the object.
2. Change the current parameters of the object.

Notes:

1. Parameters in the object settings window are described in the section corresponding to the given object for each subsystem (see [Software Implementation. SecurOS Subsystems](#)).
2. If you selected an objects, that have no editable parameters or operation is restricted by [User Rights](#), then the **Setup** button is disabled.

-
3. Apply changes.

4.2.1.3 Deleting Objects

To delete object:



1. Select an object in the *Object Tree*, then click on the (Delete) button in the Administration Toolbar.
2. To confirm operation click on the **Yes** button.

Warning! This operation cannot be undone, so use it carefully. If you delete an object, its child objects will be deleted as well. When you delete a group object, all objects within this group are deleted.

4.2.1.4 Disabling/Enabling Objects

To temporarily exclude object from SecurOS network without deleting it and, thus, loosing its settings, just disable it.

To disable an object select it in the *Object Tree*, then click on the  (Disable) button. Disabled objects are marked with "turquoise cross" icon (see Figure 44).

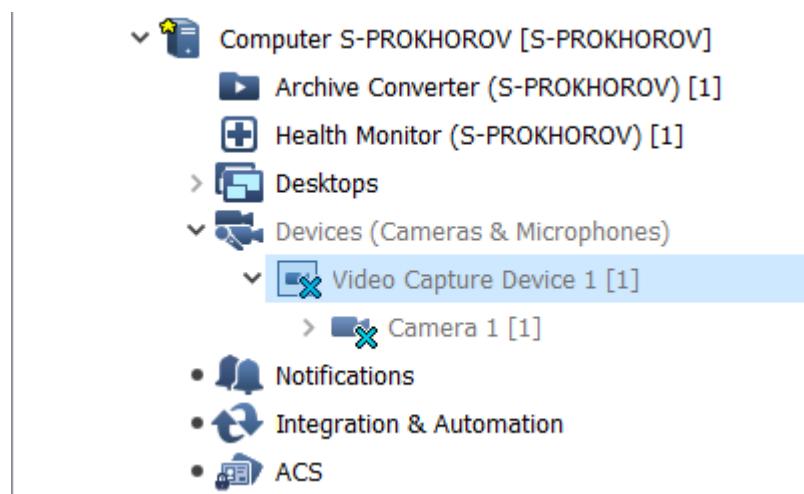


Figure 44. Disabled Object

To enable a disabled object select it in the *Object Tree*, then click on the  (Enable) button.

Additional Information

You can disable/enable all objects in the group. To do this, disable/enable *Group* or *Parent object*. When doing so name of the object\group will be marked with grey color.

4.2.1.5 Renaming Objects

It is possible to rename any object preserving all its settings.

To rename object:

1. Select an object in the *Object Tree*, then click on the  (Rename) button.
2. In the pop-up dialog window specify a new object name.
3. Click the **OK** button to save the changes.

4.2.1.6 Searching Objects

To find objects by their names or parts of names, do the following:

1. In the *Object Tree* call object/group context menu, then select **Find by name**.
2. In the search window (see Figure 45) select object type and type in the name (or part of the name) of the required object and press the **Enter** key or click on the **Search** button. If such objects exist, then the object corresponding to the search conditions will be selected in the object tree. The **Previous** and

Next buttons will become active.

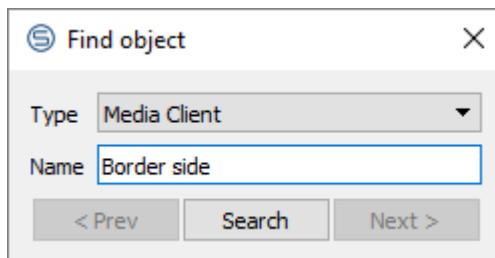


Figure 45. Searching by Name Window

3. To continue search press the **Enter** key (or the **Previous** and **Next** in the search window).

4. To stop search and close the window, press the **Esc** key.

To find objects by their IDs, do the following:

1. In the *Object Tree* call object/group context menu, then select **Find by ID**.
2. In the search window (see Figure 46) select object type and type in the name (or part of the name) of the required object and press the **Enter** key or click on the **Search** button. The focus will switch to the object that matches search ID, that will be selected in the object tree.

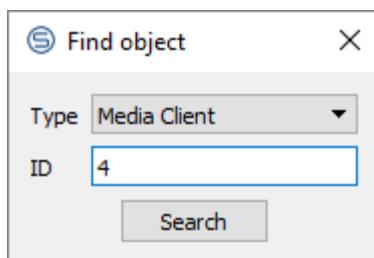


Figure 46. Searching by ID Window

3. To stop search and close the window, press the **Esc** key.

4.2.2 Working with Object Table Parameters

Object setting window can include both single parameter text boxes and tables. Example of the table parameter (**Holidays**) is shown on figure 47.

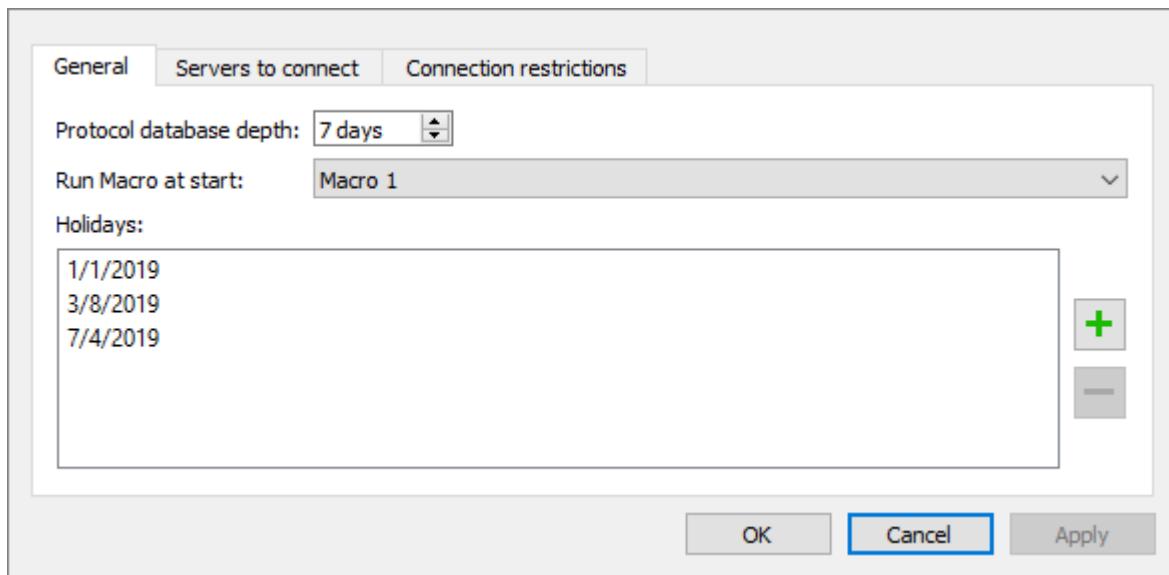


Figure 47. Example of the object table parameter

When working with table parameters the following methods are used:

- To add several entries into the table, use ↓ key on the keyboard or click mouse below the last entry in the list.
- To delete an entry from the table, select the required row and press the **Delete** keyboard key.

4.2.3 IP-Device Manager

The *IP-Device Manager* is designed to search for IP devices within the SecurOS security network and to add them to the system configuration.

The search is performed with the help of standard network technologies (see [Searching Devices in the Network](#) section) within the local network of the *Computer*, which is running the *Manager*. All found devices are assumed un-tuned; you can perform the following operations with such devices:

- [Adding IP Device](#);
- [Editing IP Device Parameters](#).

With devices that are already registered in the network (with the help of the *Manager* or by standard tools) you can perform the following operations:

- [Editing IP Device Parameters](#);
- [Deleting IP Device](#).

4.2.3.1 Specification

The main application window is shown on figure 48.

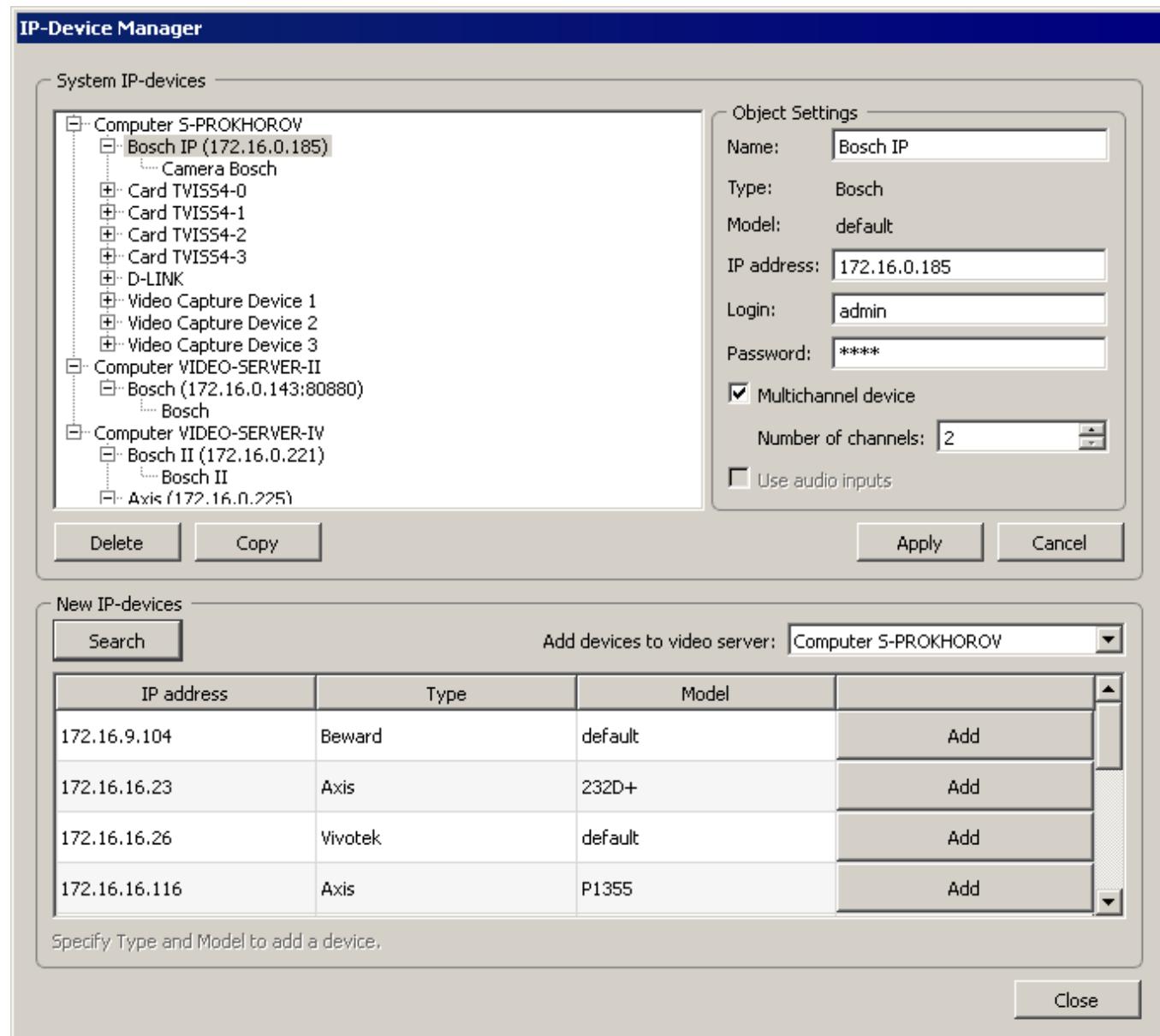


Figure 48. IP-Device Manager

The window consists of the following controls (see table 3):

Table 3. IP-Device Manager controls

Parameter	Description
System IP-devices	

Parameter	Description
Object Tree	<p>The Object Tree consists of <i>Computers</i> having the <i>Video Server</i> role that exist within the SecurOS network. When expanding the <i>Video Server</i> node all <i>Video Capture Device</i> child objects including their <i>Camera</i> child objects are displayed. If a device has integrated audio or it is configured to operate in the synchronized recording mode (see Synchronized Audio/Video Recording and Playback section), all appropriate <i>Microphone</i> objects are also displayed in the tree.</p> <hr/> <p>Notes:</p> <ol style="list-style-type: none"> 1. Objects which settings are currently being edited are displayed in the Object Tree in <i>italic</i>. 2. Objects that are disabled in SecurOS, are displayed in the Object Tree in grey (shaded out), similarly to inactive Windows objects.
Object Settings	
Name	<p>Name of the object selected in the Object Tree (see above).</p> <hr/> <p>Note. Object names are restricted with the following:</p> <ol style="list-style-type: none"> 1. Name cannot be empty. 2. Name should be unique.
Type, Model	<p>Type and model of the device, selected in the Object Tree. The Information field is not editable by the user.</p>
IP address	<p>IP address of the device.</p>
Login, Password	<p>Login/Password to access the device. By default when a device is added, the values are assigned to admin/admin.</p> <p>Warning! If login and password were assigned earlier (when device was physically added to the network) through the web-interface of the device, then enter the given values. Otherwise access to the device will be denied.</p>
Multichannel device	<p>Check the box if the added device is an IP video server/encoder with more than 1 physical video input, or an IP camera with several lenses.</p> <hr/> <p>Limitations. To use this functionality the system must meet the following conditions:</p> <ol style="list-style-type: none"> 1. The device should support several independent video streams. 2. The device integration should support multichannel systems.
Number of channels	<p>Number of used independent video channels of the multichannel device.</p> <hr/> <p>Note. Max number of video channels depends on the device Type and Model.</p>

Parameter	Description
Use audio inputs	<p>Check the box, if you want to use the device's audio inputs (or integrated microphone). Max number of audio channels depends on the device Type and Model and are defined in the device integration. In general, the number of audio channels \leq number of the video channels.</p> <hr/> <p>Limitations. To use this functionality the system must meet the following conditions:</p> <ol style="list-style-type: none"> 1. Device must be equipped with audio inputs. 2. Device integration in SecurOS should support audio.
Buttons	
Delete	Delete a <i>Video Capture Device</i> , selected in the Manager's Object Tree .
Copy	Copy a <i>Video Capture Device</i> , selected in the Manager's Object Tree (see Copying IP Device).
Apply (Cancel)	<p>Save the newly entered or edited device settings (Discard changes while saving previous settings).</p> <hr/> <p>Notes:</p> <ol style="list-style-type: none"> 1. The buttons are enabled only if settings were assigned / edited in the Settings and/or Usage tabs. 2. If the current settings were edited and the Close button was clicked before these new settings were saved or canceled, the system will display a message to save the changes.
New IP-devices	
Search	Start searching for non-configured IP devices in the local network of the SecurOS Computer, that's running the <i>IP-Device Manager</i> .
Add devices to video server	Select the <i>Video Server</i> in the Object Tree for which a new <i>Video Capture Device</i> , associated with the network IP device selected below (see Table of IP-devices below) will be created and where the video archive of this device will be created and stored. The <i>Computer</i> that's running the <i>IP-Device Manager</i> is selected by default.
Table of IP-devices	<p>The table contains found non-configured IP devices.</p> <hr/> <p>Note. An IP device is assumed non-configured, if there is no parent <i>Video Capture Device</i> in the SecurOS network, that has an IP address specified in the IP address field (see below).</p> <hr/> <ul style="list-style-type: none"> • IP address – IP address of the found device. <hr/> <p>Note. If a port number was defined for the device at the initial IP address assignment process, it is displayed in this field in standard format (for example, 192.16.0.185:8080).</p>

Parameter	Description
	<ul style="list-style-type: none">• Type – type of the IP device. Filled in automatically based on the discovery results.• Model – model of the IP device. Filled in automatically based on the discovery results.• Add – add the selected network IP device to the specified <i>Video Server</i>.

Once all required tasks are completed, the **IP-Device Manager** window can be closed by clicking the **Close** button.

4.2.3.2 Basic Operations

This section describes the following operations performed with the help of the *IP-Device Manager*:

- [Searching Devices in the Network](#);
- [Adding IP Device](#);
- [Editing IP Device Parameters](#);
- [Copying IP Device](#);
- [Deleting IP Device](#).

Warning! If the connection with the **Configuration Server** is lost, all operations are blocked until the connection is restored.

4.2.3.2.1 Launching IP-Device Manager

To launch the *IP-Device Manager* do the following:

1. Open [Administration Center](#).
2. On the *Administrator Toolbar* (see Figure 49) click on the  (**IP-Device Manager**) button.

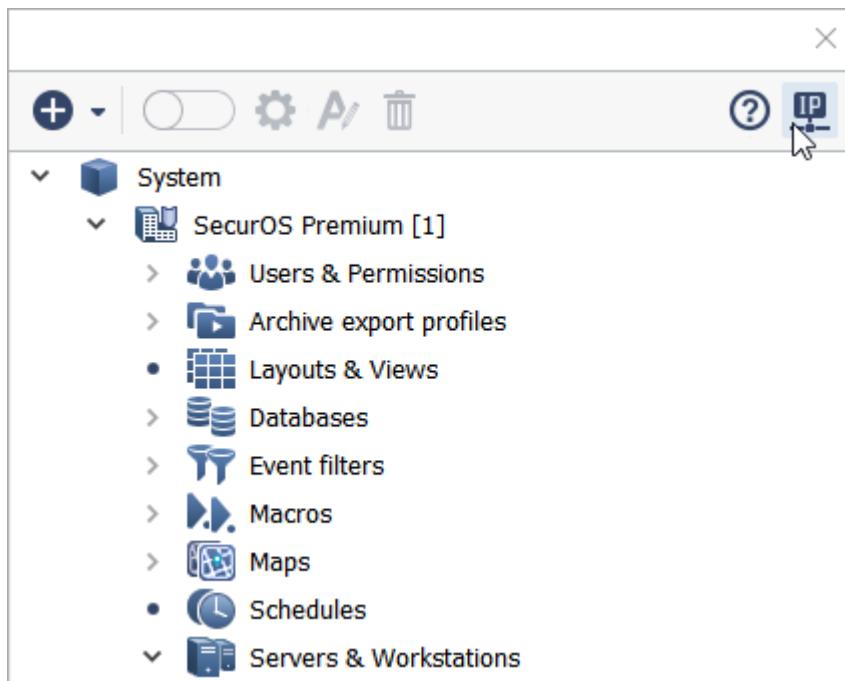


Figure 49. Launching IP-Device Manager

Notes: **IP-Device Manager** button is disabled in the following cases:

1. Setting window of any SecurOS object is opened.
2. Connection with the *Configuration Server* is lost.

3. System will display the **IP-Device Manager** window (see [Specification](#)).

Warning! When the **IP-Device Manager** window is active, the SecurOS object settings mode is blocked (i.e. it is impossible to open a object settings window from the SecurOS Object Tree).

4.2.3.2.2 Searching Devices in the Network

To search devices in the network the Universal Plug & Play technology is used. Search parameters are completely defined by the UPnP internal mechanism with no restrictions (for example, by search duration) on the SecurOS side.

To search IP devices in the SecurOS network do the following:

1. Enter the Administration Mode and launch the *IP-Device Manager*.
2. In the **New IP-devices** block click the **Search** button. The system will perform the search and display all found devices in the **Table of IP-devices** (see Figure 50).

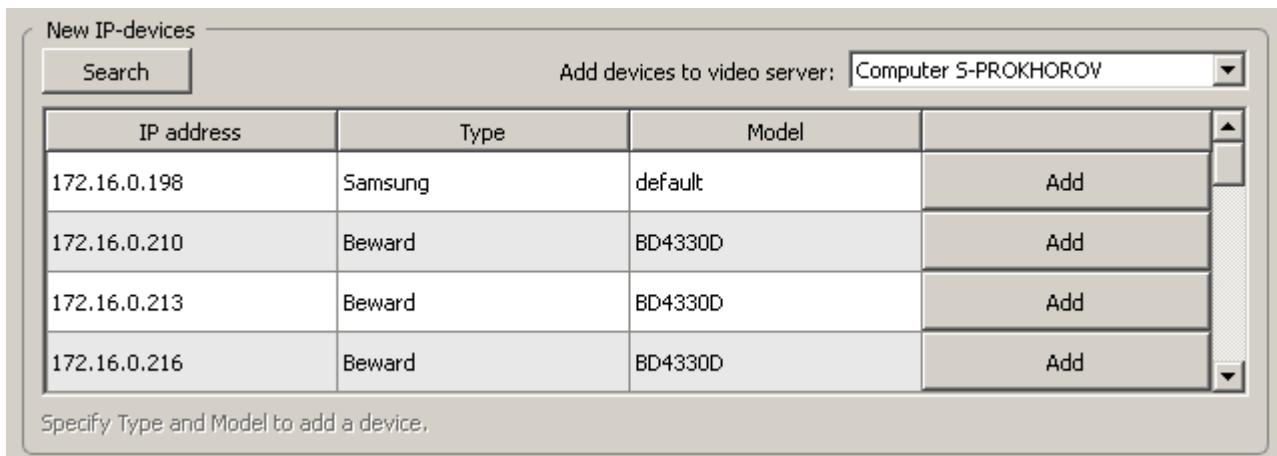


Figure 50. Device search results

Additional Information

When placing the mouse cursor over the **IP address** field an informational message containing the device info will be displayed. Typically, the message's string consists of three fields in the following format: <Device Manufacturer> <Device Model> (<Device Name>). For example, Beward BD2570 (H.264 5M box camera).

Warning! The **Table of IP-devices** displays all found network devices, including printers, scanners, etc.

4.2.3.2.3 Adding IP Device

To add an IP device do the following:

1. Enter the Administration Mode and launch the *IP-Device Manager*.
2. In the **New IP-devices** block of the *Manager* window click the **Search** button. After the query is finished, the *Manager* displays the list of un-tuned devices in the **Table of IP-devices**.
3. In the **Add devices to video server** field, select the *Computer* of the SecurOS network, where the device should be added.
4. In the **Table of IP-devices**, select the device which should be added to the network, then do the following:
 - For an unrecognized device (only **IP address** is determined):
 - In the selected device row click the **Type** cell, and in the drop-down list select device type (see Figure 51).

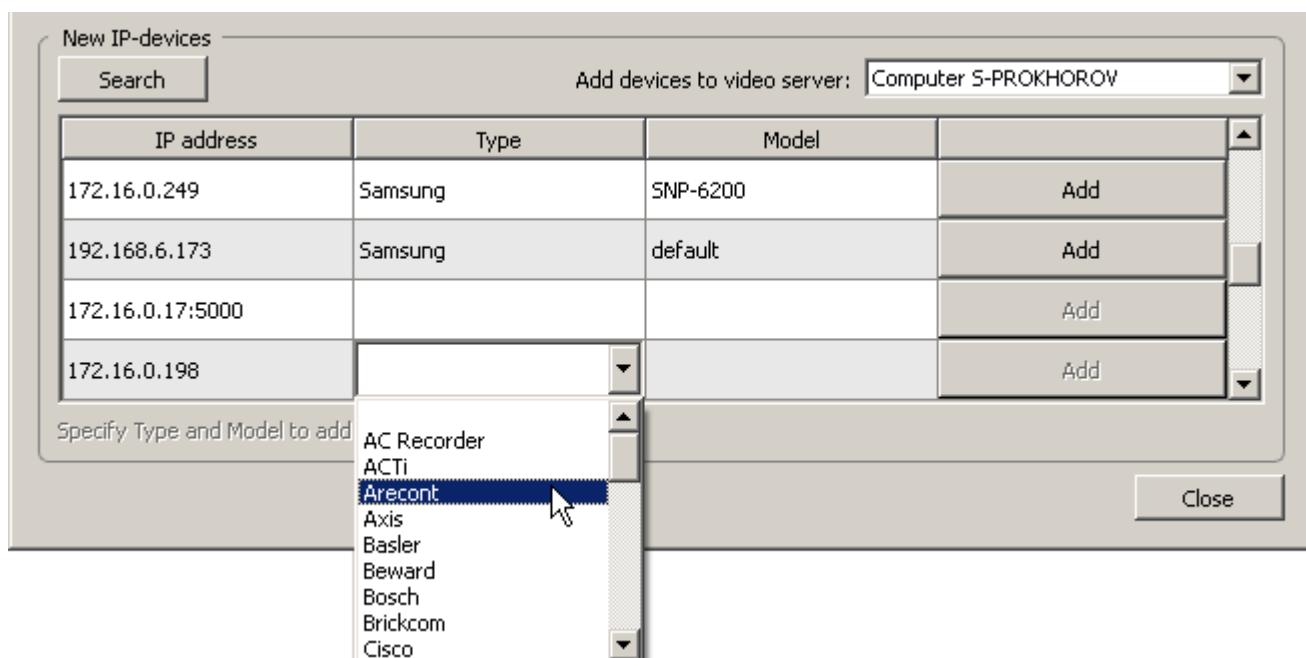


Figure 51. Select the Type of device

- Click the **Model** cell, and in the drop-down list select the model of the device. Select **default** if there is no required model in the list. System will activate the **Add** button.
 - For a recognized device (**IP address**, **Type** and **Model** parameters are determined):
 - Select the device from the **Table of IP-devices**.
 - For the arbitrary device (there is no device information in the table):
 - Click the **Type** cell in the last (empty) table row, and in the drop-down list select the device type.
 - Click the **Model** cell, and in the drop-down list select the model of the device.
5. Click the **Add** button.

Note. If the device can't be added due to license restrictions or if the connection with the *Configuration Server* is lost, the system will display a corresponding informational message.

The system will create a new *Video Capture Device* with specified parameters and add it to the *Manager's Object Tree* to the selected *Computer*, the added device will be currently selected in the device tree. A *Camera* child object will be created for the added *Video Capture Device* automatically. You can edit its parameters in the Administration Mode from the SecurOS *Object Tree*.

Note. The default name for each added device is *Video Capture Device N*, where *N* – next sequential digital identifier of the given type of object.

6. Further execute the **Editing IP Device Parameters** operation.

4.2.3.2.4 Editing IP Device Parameters

To specify/edit device settings do the following:

1. In the *Manager's Object Tree* select the device whose settings you wish to specify/edit.
2. Edit device settings in the **Object Settings** block (see Figure 52):

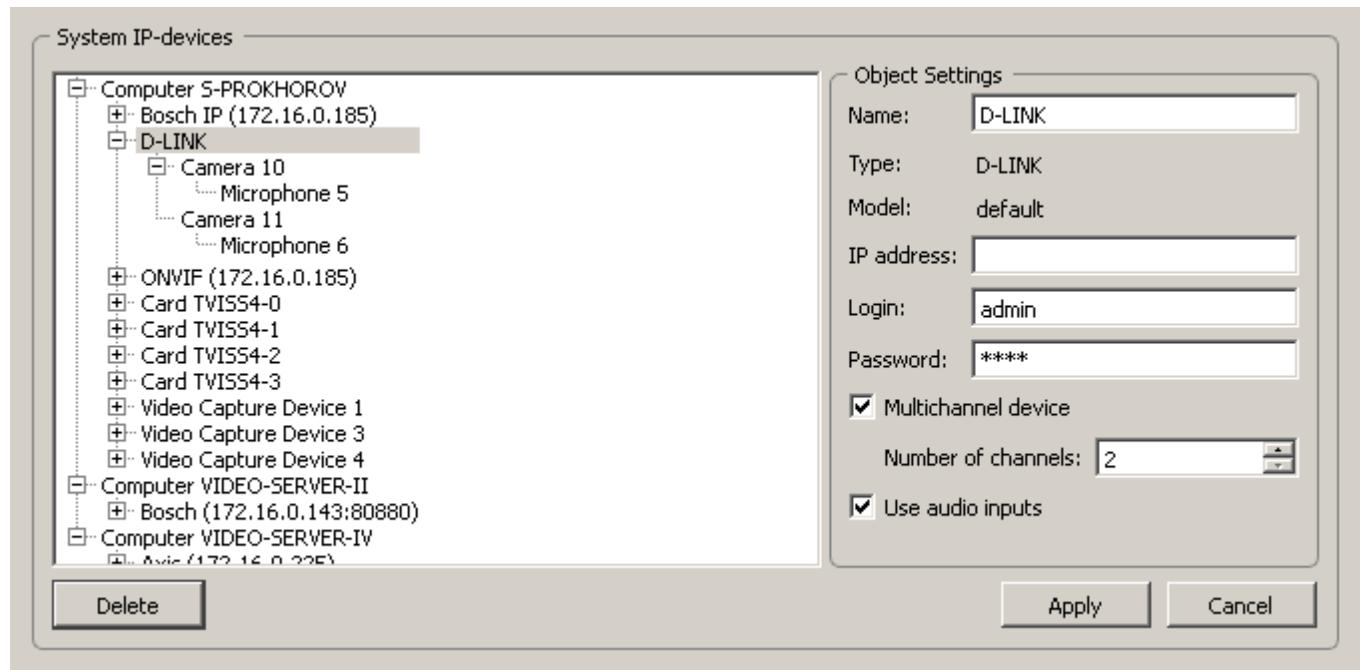


Figure 52. Setting up audio inputs

- If necessary, change device name in the **Name** field.
- If necessary, specify or edit **IP address**.
- If necessary, change default **Login/Password** to access the *Video Capture Device* (admin/admin).
- In case of a multichannel device, activate the **Multichannel device** checkbox and specify the required number of channels. Depending on the specified value, the appropriate number of *Camera* objects will be created. The created objects will be child objects of the given *Video Capture Device* in the SecurOS *Object Tree*, which will also be displayed in the *Manager's Object Tree*. The *Camera* with the minimal identifier will be assigned to a **Channel number** equal to 1, additional channels are numbered with increments of 1.
- If the added device supports audio, activate the **Use audio inputs** checkbox. An *Audio Capture Device* with one or more (for multichannel device) *Microphone* child object(s) will be automatically created in the SecurOS *Object Tree*. In the *Manager's Object Tree* such microphones will be linked with the appropriate number of device's cameras (see Figure 52), and in the SecurOS *Object Tree* will be specified in the settings of the appropriate *Cameras*.

3. Click **Apply** button.

4.2.3.2.5 Copying IP Device

Operation allows to create up to 99 copies of the configured *Video Capture Device* that exists within SecurOS.

The following main parameters and child objects of the selected source object will remain intact for each copy:

1. device **Type**;
2. device **Model**;
3. other parameters, that are specified by device **Type** and **Model**;
4. child *Cameras*. Number of the child *Cameras* of the each copy will correspond to the number of *Cameras* child to the source device.

The following associated objects and parameters are not copied:

1. *Audio Capture Devices*.
2. *Microphones*.
3. The following parameters of the *Camera*:

- **Microphone**;
- **Presets**;
- **Tours**;
- **Wiper**;
- **Washing Kit**;
- **Zones**. The one Zone is created by default (**Main**).

To copy *Video Capture Device* do the following:

1. In **System IP-devices** block (see [Specification](#)) select an object, that you want to copy.

Warning! You cannot copy device, which settings are not saved with the *IP-Device Manager*.

2. Click the **Copy** button. Depending of the type of the selected *Video Capture Device* system will display one of the following **Copying** window (see Figure 53).

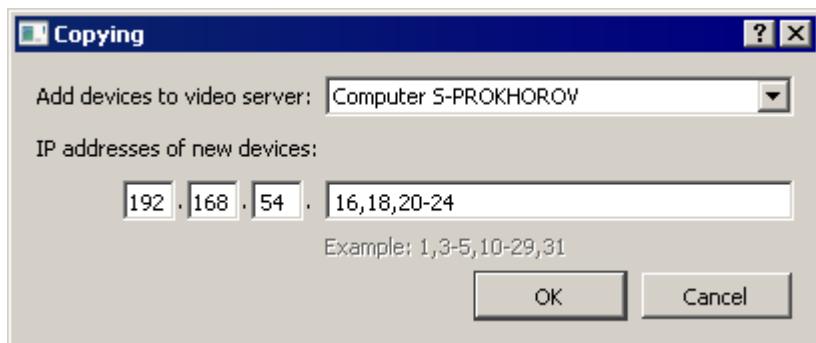


Figure 53. Copying window for the IP Cameras

3. Select a **Video Server**, where new devices will be added to, specify a **Number of copies** or range of **IP addresses**, that will be assigned to the created devices. Click the **OK** button.

Note. If a **Port** was specified in the **IP address** parameter of the device is being copied, then this port will be set for each device copy with no changes.

4. System will create required number of copies of the initial device on the specified *Video Server*.

5. If necessary, configure each created device copy on the **Settings** tab. Click the **Apply** button.

4.2.3.2.6 Deleting IP Device

To delete an IP device do the following:

1. Enter the Administration Mode and launch the *IP-Device Manager*.
2. In the *Manager's Object Tree* select the device you want to delete.
3. In the **System IP-devices** block click the **Delete** button. The selected device will be deleted from all **Video Servers** along with all child or linked objects.

4.3 Users and Rights

Restriction of the access to the SecurOS objects and operations with them is based on the access rights assigned to each user. Users and their access rights can be specified both at the initial system configuration (see [Initial Configuration Using The System Configuration Wizard](#)) and at the further system operation (see [User Registration and Configuring User Rights](#)).

The following SecurOS objects are used to control users and their rights:

- **Department** – is used to group *Users*, for example, depending on user's role within the system.
- **User Account** – serves for the creation of the SecurOS's user personal account (contains login and password that are used for authorization in the system).
- **Active Directory / LDAP** – this object provides authorization in SecurOS for the Windows/Linux users registered in the Windows Active Directory domain.
- **User Rights** – is used to assign users (both native SecurOS *Users* and OS users) *Access rights* to SecurOS objects and operations with them. For the details see [User Registration and Configuring User Rights](#).

Detailed information about users, their rights, SecurOS objects used for configuration is given in the following sections:

- [SecurOS Users](#);
- [User Registration and Configuring User Rights](#);
- [Configuration of Network Domain User Rights](#).

4.3.1 SecurOS Users

The following users can log in and work with SecurOS:

- [SecurOS Superuser](#);
- [Typical user of the SecurOS](#);
- [OS user registered in domain](#).

SecurOS Superuser

Superuser account is created during initial system configuration via System Configuration Wizard and has the `root` (user name) and password specified by the administrator (`securos` by default) credentials. The set of the rights of such account gives user the full access to all system objects and the right to execute any actions in the network. Objects of the superuser account aren't displayed in the SecurOS Object Tree; to change the name and the set of the superuser rights is impossible.

Warning! Superuser password can be changed with the help of Wizard (see [4](#) in the [Initial Configuration Using The System Configuration Wizard](#)) or further at system operation (see [Changing Superuser Password](#)).

Typical user of the SecurOS

Typical SecurOS user account can be created both via System Configuration Wizard and further system operation. The operations for creating a typical user account and setting up its rights are described in the [User Registration and Configuring User Rights](#).

OS user registered in domain

In addition to the pointed above users, any user of Windows/Linux operating systems registered in the Windows Active Directory domain can work with SecurOS. The operations of registering such user in SecurOS and configuring his rights are described in the following sections:

- [User Registration and Configuring User Rights](#);
- [Configuration of Network Domain User Rights](#).

4.3.1.1 Changing Superuser Password

To change superuser password:

1. Log on the system using superuser credentials ([SecurOS Users](#)).
2. Open settings window for the root *System* object (see Figure [54](#)).

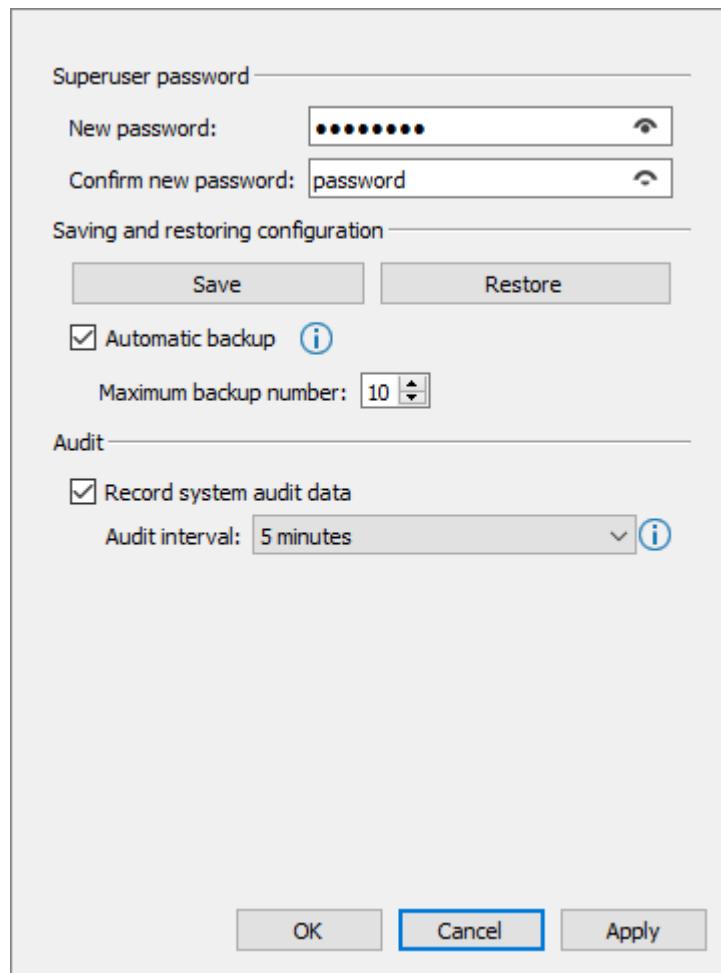


Figure 54. System object settings window

3. Use text boxes of the **Superuser password** block to type and confirm new password. Click **OK** button to save the changes.

Warning! Minimum superuser password length is 7 characters. After changing the password, keep it a secret.

4.3.2 User Registration and Configuring User Rights

Warning! If there are no other *Users* in the system except the *Superuser* (see [SecurOS Users](#), access to the system will be granted without taking into account the user name and password).

To create and configure new user accounts the following system objects are used:

- *Department* object (**Security Zone** → **Users & Permissions group** → **Department**) – contains a list of the *User* object. The name of each *User* object is used at authorization as the **User** parameter. User's **Password** is specified in the appropriate **User Account** object settings. New users can be registered both in the given *Department* object, and in any other *Department* object created by the system administrator.

Note. *Department* object is created in the object tree only if *Power user* or *Simple user* were added during system configuration with the help of System Configuration Wizard.

- *Users & Permissions* group (**Security Zone** → **Users & Permissions group**) – contains the *User*

Rights objects. Each of the existing *User Rights* objects can be used repeatedly (i. e. can be assigned to any user). This group contains two predefined set of user rights (*Rights for Power User* and *Rights for Simple User*) which differ in the level of access to objects and operations with them.

User registration and user rights configuration procedures are described in the following sections below:

- [New user registration](#);
- [Assigning rights to a user/user group](#);
- [Checking the possibility of authorization of the specified user of the OS network domain](#).

New user registration

Note. The procedure for registering in SecurOS an OS user registered in an Active Directory domain is described in the [Configuration of Network Domain User Rights](#).

To register in SecurOS a new SecurOS user do the following:

Warning! If system contains more than one *Security Zone* it is necessary to define user and his rights for each of these zones. Users registered in the separate *Security Zone* can log on only the *Computers* that are children to the given *Security Zone*. Superuser (see [SecurOS Users](#)) can log on any computer that belongs to any *Security Zone*.

1. In the *Users and Permission* group create a new *Department* object or use existent.
2. Create an *User* object children to the selected *Department*.
3. In the **Parameters of created object** window in the **Name** field specify user name that will be used for the authorization (see Figure 55).

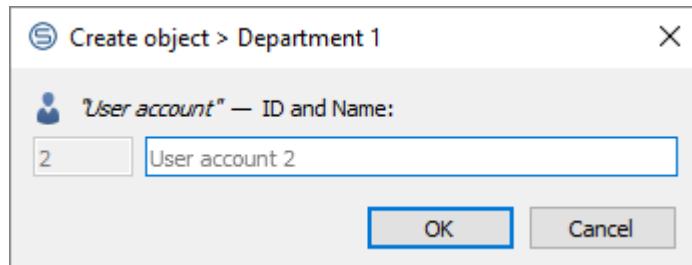


Figure 55. Parameters of created object

4. In the object settings window (see Figure 56) specify required **Password** that will be used for the authorization. Specify other parameters, if necessary (for the details see [User Account](#)).

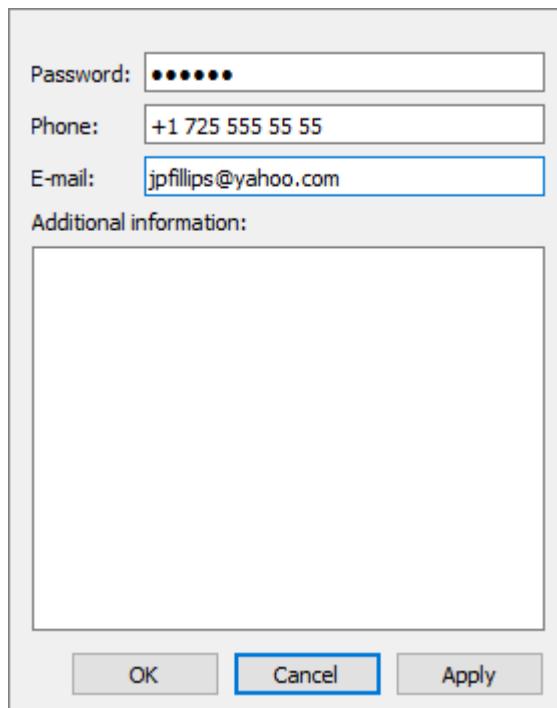


Figure 56. User Account object settings window

5. Save changes.

Assigning rights to a user/user group

To implement the security scheme with user access restrictions:

1. Plan how many different levels of access your *Security Zone* should have, and what users will have each of these levels of access.
2. Create required number of the **User Account** objects (see [New user registration](#)).
3. In the *Users and Permissions* group create **User Rights** object or use one of the predefined set of the user rights (**Rights for Power User/Rights for Simple User**).
4. In the **User Rights** object settings window (see Figure 57):
 - For each SecurOS object in the object tree (is placed at the top of the window) specify access level by clicking its icon. Specified access level will be assigned to each user defined in the **Users and Groups** list.

Note. Detailed information about access levels and its corresponding icons is available in the [User Rights](#) section.

- Select required checkboxes.
- In the **Providers** list select provider database of which stores user accounts.
- In the **Users and Groups** box of the created object settings window specify a list of users, who should have the rights defined for this group. Depending on selected **Provider** the list of users to whom the custom rights will be assigned is formed differently:
 - **for the user of SecurOS** – in the users list click an area below the last entry than in the drop down list select a user that must be added to the list.

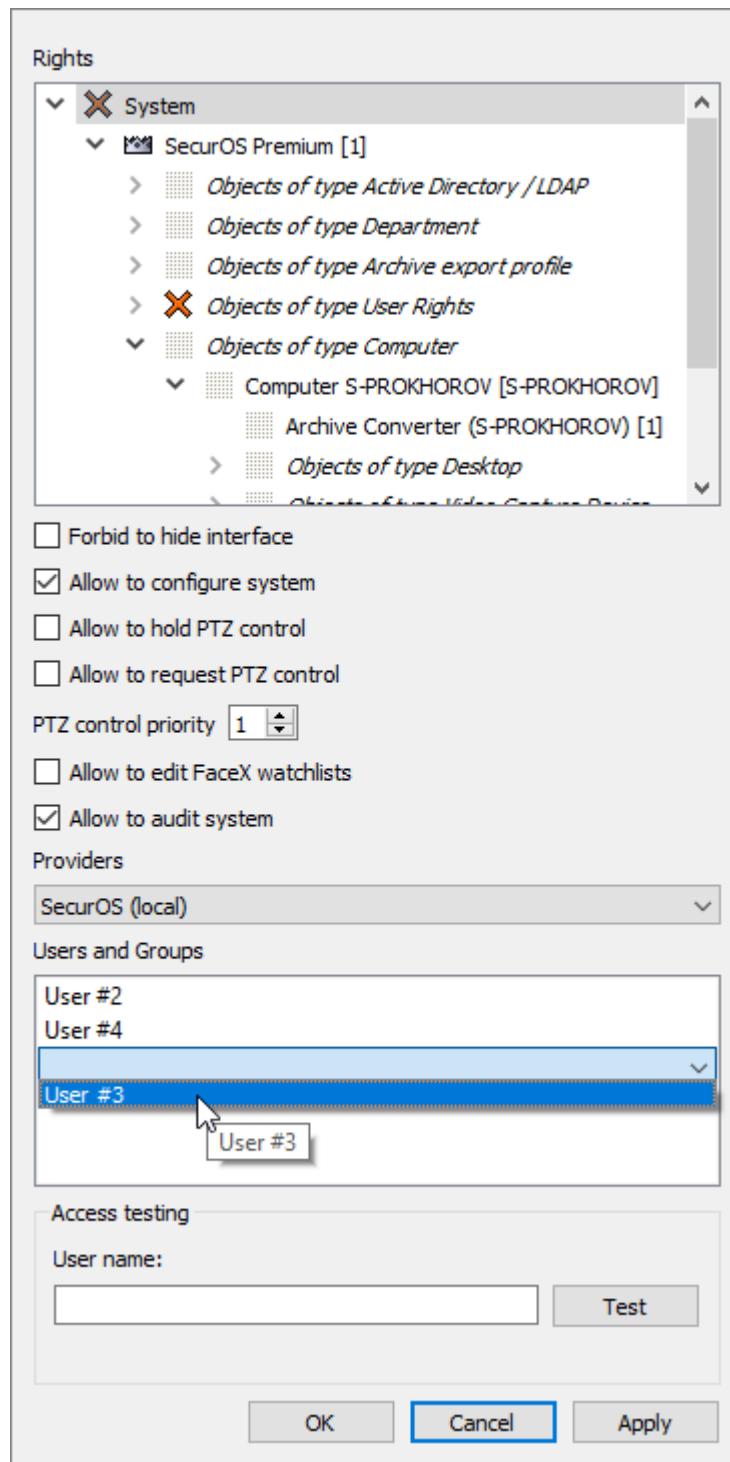


Figure 57. The User Rights object properties window

- for the Windows/Linux users registered in the Active Directory network domain – configuring rights for the OS user group are described in the [Configuration of Network Domain User Rights](#).
5. Repeat steps 2 - 4 for each *Security Zone* within your network. For each *Security Zone* SecurOS Object Tree will contain elements shown in figure 58.

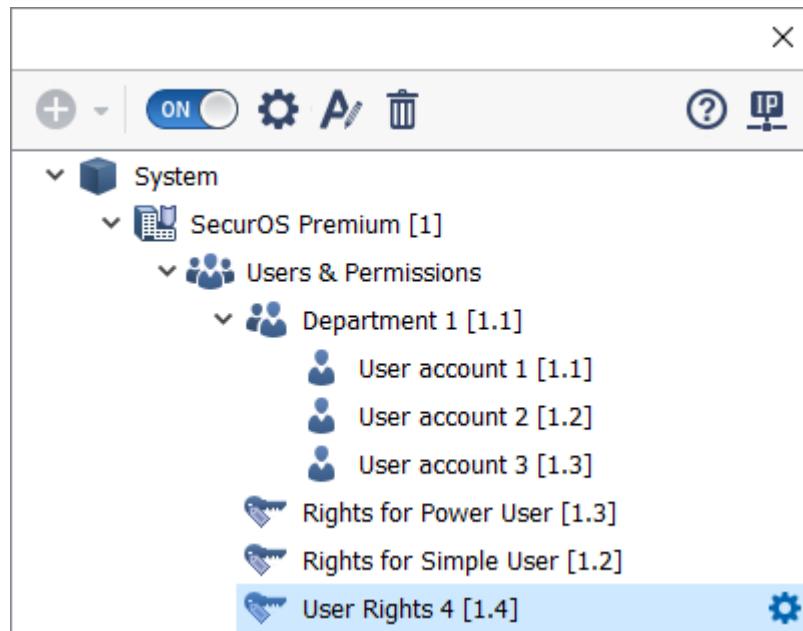


Figure 58. Objects Tree with Department, User Accounts and User Rights objects

Checking the possibility of authorization of the specified user of the OS network domain

One can test the possibility of the authorization of the specified user of the OS network domain in the **User Rights** object settings window. To perform the test do the following:

1. Configure the OS user rights (see [Configuration of Network Domain User Rights](#)).
2. In the **Access testing** block (see Figure 59):

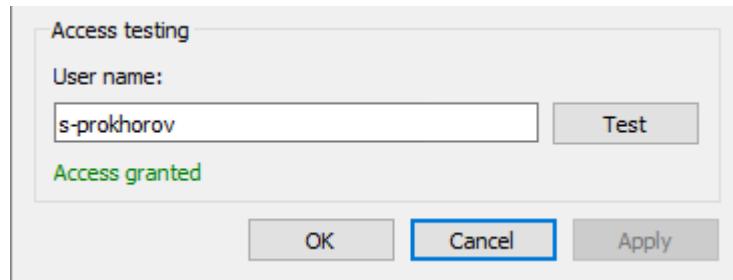


Figure 59. Access testing block

- Enter the **User name** of the OS user for which it is necessary to check the possibility of the authorization in SecurOS;
- Click the **Test** button.

The following is analyzed when testing is performed:

- correctness of the selected provider settings (see [Active Directory / LDAP](#));
- correctness of the specified LDAP filter to define user/user group (when using LDAP provider);
- presence of the specified user/user group's account in AD.

3. Testing may complete with the following outcomes:

- Access granted – settings are correct. This OS user will be able to authorize in SecurOS;

Warning! Access level to the *Computer* object specified in the configured *User Rights* is not taken into account when checking.

- Access denied – settings are incorrect or specified user is not registered in OS domain;
- Check failed – domain controller request timeout exceeded.

The ability to authorize the specified native SecurOS user can be checked in a similar way.

4.3.3 Configuration of Network Domain User Rights

In this section the *Active Directory / LDAP* (see [Active Directory / LDAP](#)) and *User Rights* object configuration procedure is described for the domain provider (Windows NT or LDAP) that receives the SecurOS user authorization request. Contains the following parts:

- [Settings for Windows NT Provider](#);
- [Settings for LDAP Provider](#).

4.3.3.1 Settings for Windows NT Provider

To set domain parameters for Windows NT provider:

1. In *Active Directory / LDAP* (see [Active Directory / LDAP](#)) object settings window choose Windows NT (local or domain) value from the **Provider** drop-down list.
2. Select **Use primary domain controller** checkbox to use primary domain controller where the computer is registered, or fill the **Server** field with IP address of domain controller server. You do not need to fill the **Port** field (port for Windows NT provider).
3. Select **Use credentials provided at system login** checkbox to connect domain controller using current MS Windows login and password, or fill in the **User name** and **Password** fields (specified user must be defined for domain controller, see item 2).
4. If the **User name** and **Password** fields are filled, select the **Use secure authentication** checkbox.

To set user rights for a single user, specify the user system name (for example, j-smith) in the the **Users and Groups** field of the *User Rights* object settings window (see [User Rights](#) section).

To set user rights for a user group, fill the **Users and Groups** field in the *User Rights* object settings window with a network domain users group login and ,group postfix without spaces (e. g. Users,group). The ,group postfix is required.

4.3.3.2 Settings for LDAP Provider

To set domain parameters for LDAP provider:

1. In *Active Directory / LDAP* (see [Active Directory / LDAP](#)) object settings window choose LDAP (domain) value from the **Provider** drop-down list.
2. Select **Use primary domain controller** checkbox to use primary domain controller where the computer is registered, or fill in the **Server** field with IP address of domain controller server.
3. Select **Use credentials provided at system login** checkbox to connect domain controller using current MS Windows login and password, or fill in the **User name** and **Password** fields (specified user must be defined for domain controller, see item 2).
4. If the **User name** and **Password** fields are filled, select the **Use secure authentication** checkbox.

To set user rights for a single user, fill the **Users and Groups** field in the *User Rights* object settings window (see [User Rights](#)) with the following string: &(objectClass=user) (sAMAccountName=j-smith), where the user name (for example, j-smith) is specified.

To set user rights for a user group, fill the **Users and Groups** field in the *User Rights* object settings window with the following string:

```
&(objectClass=user) (memberOf=cn=Users,cn=Builtin,dc=test-dev,dc=test)
```

where **Builtin** – system folder where the **Users** group is located.

4.4 SecurOS Logging

In operation, SecurOS provides continuous system logging. Data recording is done separately by each of the servers in their own, local database. By default, each server stores information about all the events occurring within the system. Database retention period, that is common for all servers within the system, is specified in the [Security Zone](#) object settings.

Additionally, specific rules of data recording and storage can be specified for each of the system servers in the **Local database** parameter block of the [Computer](#) object settings:

- **List of events allowed to be recorded into the database** – only events specified in the [Event Filter](#) object settings will be recorded into the local database. Use **Event filter** parameter is used to specify if event filter should be applied while recording;
- **Database size** – restriction on the local database size. Is specified in the **Maximum Protocol DB size** parameter. If specified value is reached then information is re-recorded in ring mode – the oldest protocol records are deleted first. If maximum is not reached, then common for all system servers database retention period value is considered;
- **Disable recording into the database** – if this mode is on, then no information is recorded into the local protocol database. Is specified in the **Disable saving data into local Protocol DB** parameter.

To view protocol database records the [Event Viewer](#) interface object is used. *Event Viewer* interface object window displays information from database of the server to which you are connected. For the *Video Server* this is its own, local protocol database of the corresponding computer, and for the *Operator Workstation* – database of that *Video Server*, to which operator's computer is connected. Thus if *Operator Workstation* is connected to the servers where different rules of the database information recording and storage are specified, then different information can be displayed in the *Event Viewer* interface object window.

Database access control is ensured by the PostgreSQL DBMS access control system, eliminating the possibility of unauthorized modification or deletion of records by a simple user. *Event Viewer* interface object cannot be used for unauthorized data modification or deletion.

4.5 Updating License Key on All Servers

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*, *SecurOS Xpress*.

To update license key on all servers:

1. Copy the latest version of the `key.iss` to the SecurOS program directory on the *Configuration Server*.

2. System will automatically update the license key on any of the *Peripheral Server* when given server will connect to the *Configuration Server* for the next time.

Additional information

Outdated license key is stored in the SecurOS installation root directory in the `key.iss.bak` file.

Warning! After license key was updated on the *Peripheral Server* SecurOS program may automatically reboot.

4.5.1 License Expiration Reminder

All workstations can be configured to notify simultaneously about license key file expiration date.

If less than certain days remain before license expiration then an information window will appear on each workstation during operator working (see figure 60). Operator may close the window and continue working.

Notification window appears with a certain periodicity (e.g. three times a day, with three hours between messages).

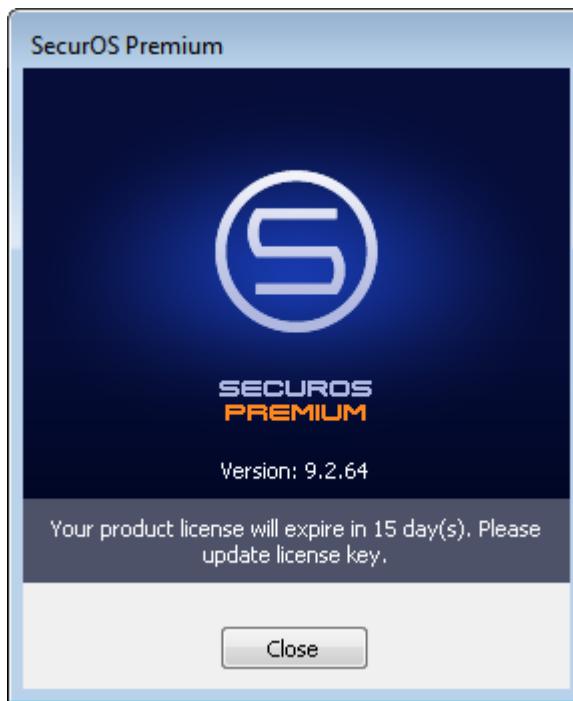


Figure 60. License expiration information window

To setup notification parameters, do these steps on each computer where reminder window should appear:

1. Open `client_config.xml` file located in the SecurOS root directory.
2. Insert the following parameters into the `<Main>` section:
 - `DaysForRemaining` – specify a number of days before license expiration date to begin operator notification;
 - `RemaindersPerDay` – specify a number of notifications per day;

Warning! Zero value of this parameter results in that the reminder window will be never displayed!

- MinRemaindPeriod – specify a minimal time interval (in minutes) between two notifications (must be no less than 30).

3. Save the changes and close the file.

Listing 1. client_config.xml example

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<client>
    <params name="Common">
        <param name="CoreAddress" value="localhost"/>
    </params>
    <params name="Main">
        <param name="AutoLogin" value="false"/>
        <param name="CoreRestartTimeout" value="30000"/>
        <param name="CurDayRemaindCount" value="0"/>
        <param name="DaysForRemaining" value="15"/>
        <param name="KeepCoreAlive" value="true"/>
        <param name="KeepProcessesAlive" value="true"/>
        <param name="LastRemaind" value="2013-03-22 13:58:39"/>
        <param name="LastUser" value="root"/>
        <param name="MinRemaindPeriod" value="180"/>
        <param name="ProcessWaitTimeout" value="30000"/>
        <param name="RemaindersPerDay" value="10"/>
    </params>
    <params name="ServersList">
        <param name="0" value="192.168.3.35"/>
    </params>
    <params name="UserServersList">
        <param name="0" value="192.168.3.35"/>
        <param name="1" value="192.168.0.51"/>
        <param name="2" value="s-zhulev"/>
    </params>
</client>
```

4.6 Health Monitor self-diagnostic Module

The *Health Monitor* self-diagnostic Module is designed for system monitoring to identify different issues.

Working procedures are described in the following subsections:

- [Configuring and Launching](#).
- [Operation Modes](#).
- [Health Monitor Window](#).
- [Diagnosed issues](#).

Configuring and Launching

Parent object – [Computer](#).

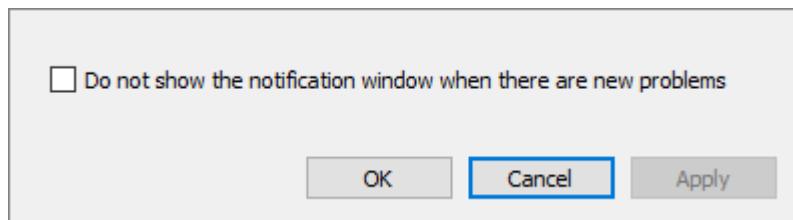


Figure 61. Health monitor object settings window

Table 4. Health monitor object settings

Parameter	Description
Do not show the notification window when there are new problems	Use this checkbox to select new problem notification mode: <ul style="list-style-type: none"> • checkbox is not selected (default value) – Autoinforming mode – a pop-up window is used to inform operator about new issues. • checkbox is selected – Silent informing mode – an application icon in system tray is used to inform operator about new issues.

The *Health Monitor* can be located on any *Computer* within the network (*Video Server* or *Operator Workstation*) and, regardless of location, allows you to monitor the state of the whole system.

After application is started its icon is displayed in system tray. Icon appearance indicates current system state:

- – there are no issues;
- – there are issues;
- – a new issues were discovered (is used only for *Silent informing mode*). Displays the total number of problems that occurred after the previous **Health Monitor** window session was closed.

Operation Modes

Depending on object settings (see [Configuring and Launching](#)) one of two modes is used to notify operator about new issues:

- **Autoinforming mode (pop-up informer window is used for informing)** – when a new problem occurs, the informer window that contains the list of problem objects and a brief description of the problem is automatically displayed (see Figure 62). If there are no new problems, the informer window will automatically hidden in 10 seconds. If informer window is hidden, one can call it by clicking application icon in system tray;
- **Silent informing mode (application icon in system tray is used for informing)** – when total number of problems changes, the system automatically updates the problem counter () on the application icon (see Figure 63). To view list of current issues call informer window by clicking application icon.

SecurOS Administration Overview

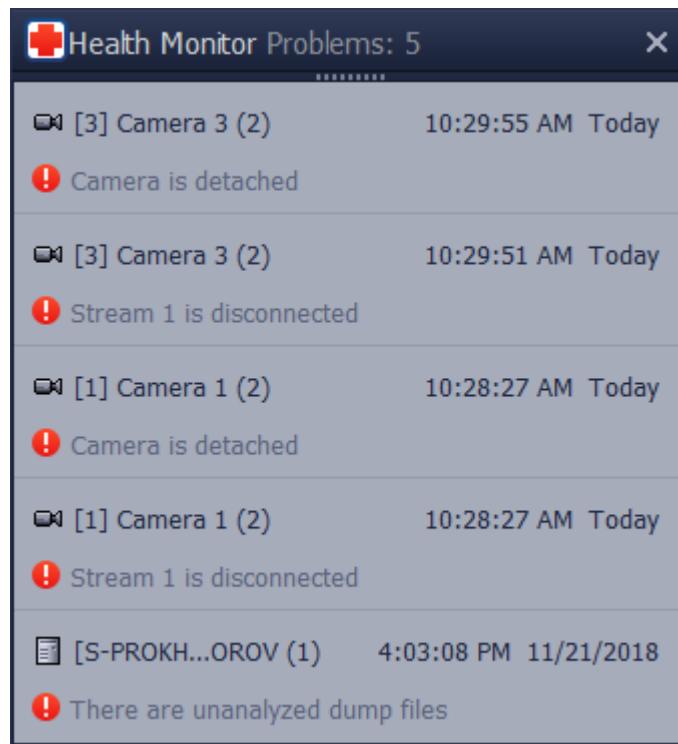


Figure 62. New issues informer window



Figure 63. Informing with the help of application icon

To view issue details description call **Health Monitor** window by clicking required one in the informer window list. Informer window can also be called from the context menu of SecurOS icon in system tray (see Figure 64).

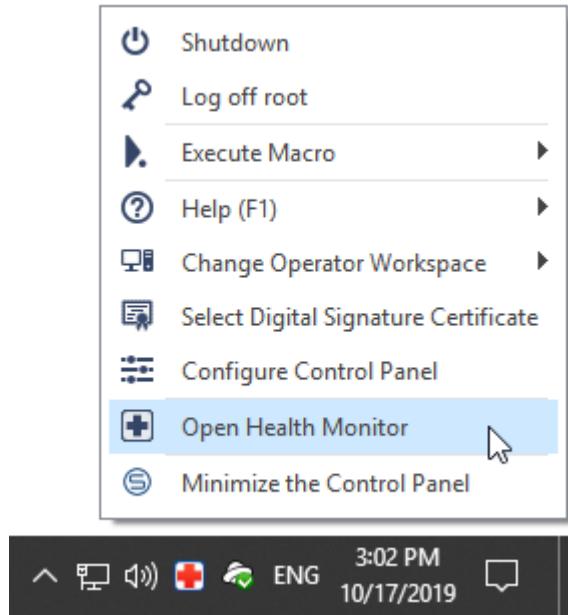


Figure 64. Open Health Monitor Window

Health Monitor Window

This window displays detailed information about problem objects. Appearance of the window is represented in Figure 65.

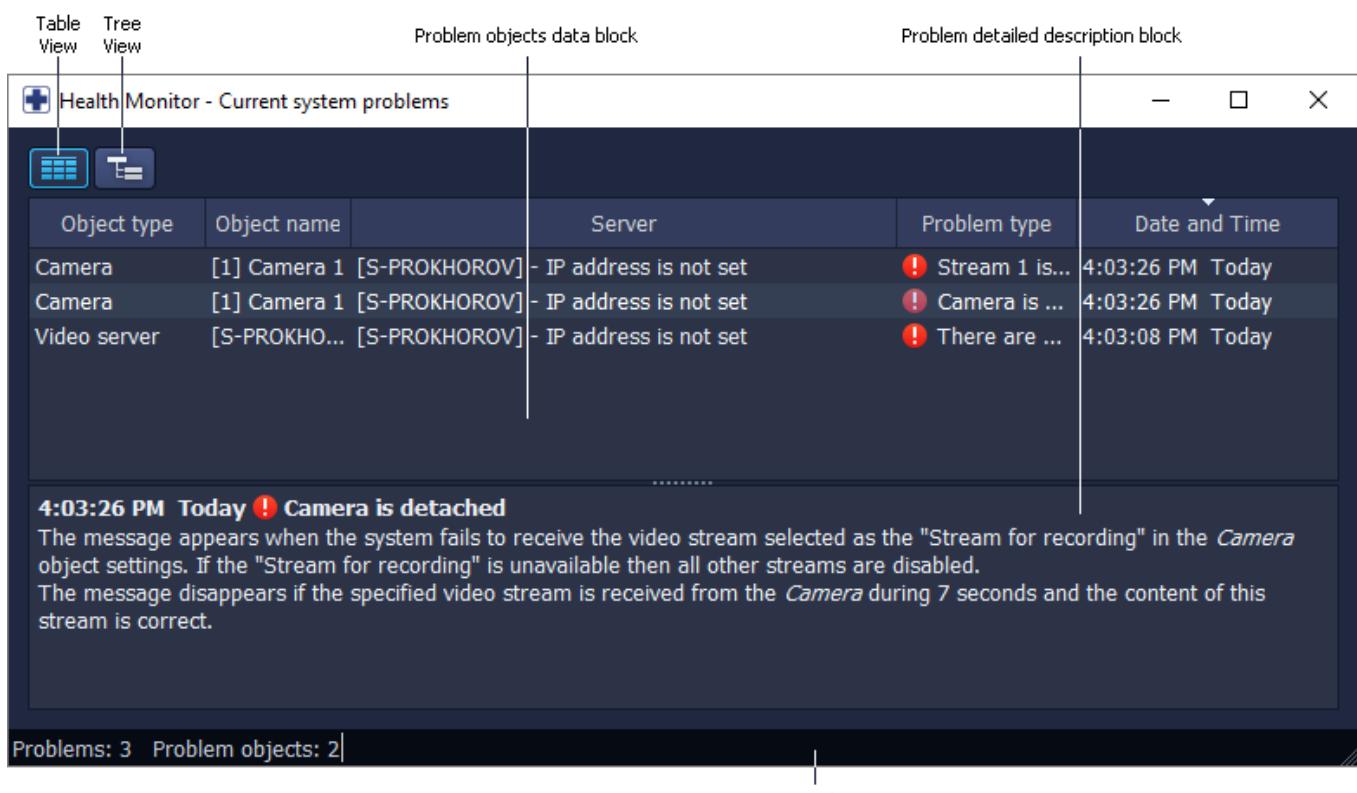


Figure 65. Health Monitor Window. Table view

Note. When window is opened for the first time, then *Table* view is used.

Window contains the following components and controls:

- **Problem objects data block** – contains data about problem objects within the system. In this block information can be displayed in **Table** or **Tree** view;
- **Problem detailed description block** – contains details about problem appearance and disappearance conditions. This detailed information is displayed after issue is selected in **Problem objects data block** or informer window problems list;
- **Status bar** – contains total number of issues and problem objects within the system;
- **(Table) button** – use **Table** view for data presentation;
- **(Tree) button** – use **Tree** view for data presentation.

Note. Current view of data representation is indicated by a turquoise button.

Table view

Appearance of the **Health Monitor** window when table view for data representation is used is shown in Figure 65. Data is located in the following columns:

- **Object type** – type of the problem object;
- **Object name** – id and name of the problem object;
- **Server** – id and IP address of the *Video Server* where problem appears. If IP address is not specified in the **Computer** object settings, then the "IP address is not set" string is displayed in the

cell;

- **Problem type** – name of the problem that occurred on the specified object;
- **Date and Time** – problem date and time in OS format. Problems of the current day is marked with the "Today" word.

One can change table columns width. To do this place mouse pointer over columns separator. Pointer will be changed as it represented in Figure 66.

Object type	Object name	Server	Problem type	Date and Time
Camera	[1] Camera 1 [S-PROKHOROV] - IP address is not set		! Stream ...	4:03:26 PM Today
Camera	[1] Camera 1 [S-PROKHOROV] - IP address is not set		! Camera i...	4:03:26 PM Today
Video server	[S-PROKHOR...]	[S-PROKHOROV] - IP address is not set	! There ar...	4:03:08 PM Today

Figure 66. Changing table column width

Press the mouse button, and while holding it down, move the cursor in the required direction.

Note. Width of the last column in the table can not be changed.

Table data can be sorted by ascending/descending by column value. To sort table entries by any field, click required column in the table head, then click the "up arrow/down arrow" icon (see Figure 67). Table entries will be sorted by ascending/descending order in selected column.

Object type	Object name	Server	Problem type	Date and Time
Camera	[1] Camera 1 [S-PROKHOROV] - IP address is not set		! 4:03:26 PM Today	
Camera	[1] Camera 1 [S-PROKHOROV] - IP address is not set		! 4:03:26 PM Today	
Video server	[S-PROKHOROV] Compute...	[S-PROKHOROV] - IP address is not set	! 4:03:08 PM Today	

Figure 67. Sorting list

Tree view

Appearance of the **Health Monitor** window when tree view for data representation is used is shown in Figure 68.

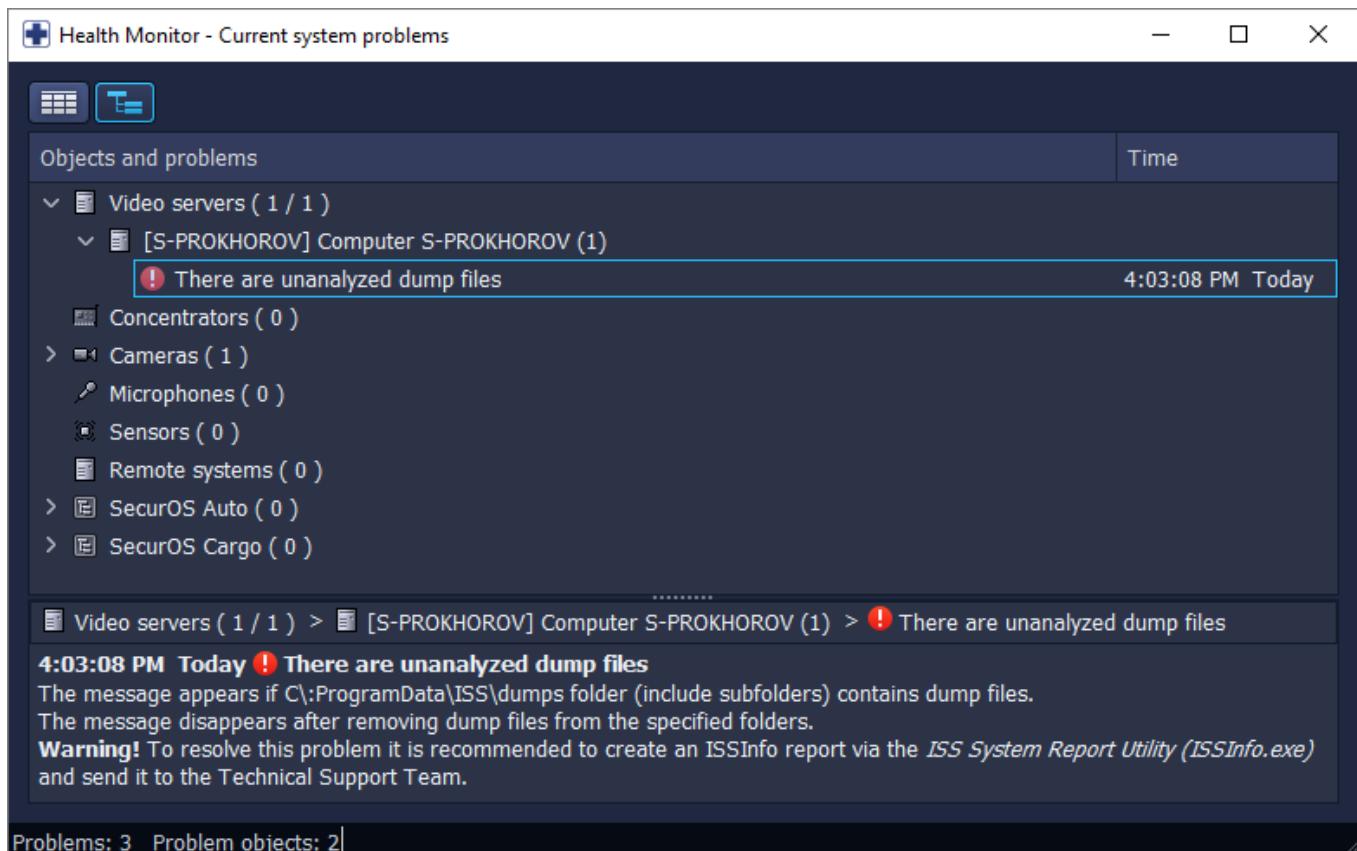


Figure 68. Health Monitor Window. Tree view

SecurOS objects with current problems are represented as a tree and grouped in eight main nodes, representing the object type or SecurOS Intelligent Module: *Video Servers*, *Concentrators*, *Cameras*, *Microphones*, *Sensors*, *Remote systems*, *SecurOS Auto* and *SecurOS Cargo*. The number of objects of the given type is displayed to the right of the node name. The total amount of objects of the given type within the SecurOS network is additionally displayed for the *Video Servers* node. Within the node problem objects are grouped by video server name. The total number of problem objects of given type is displayed to the right of the video server name.

One can use address bar of the **Problem detailed description block** to quickly navigate through the branches of the **Problem objects tree**. To jump to the required level, simply click it (see Figure 69).

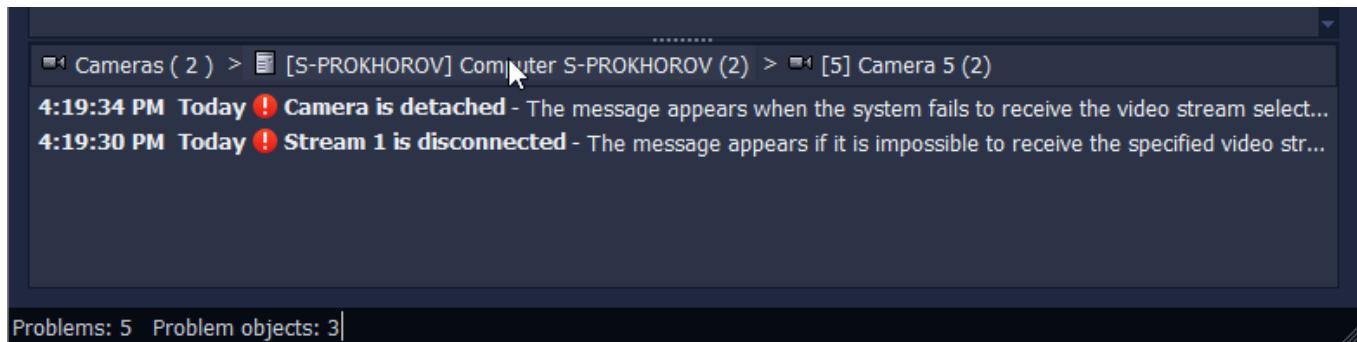


Figure 69. Navigation through Problem objects Tree from address bar

After such a jump is finished, all problem objects located on the selected level (for example, *Cameras*, see Figure 70) will be displayed in the **Problem detailed description block**. To jump to detailed description of the problem for any *Camera*, simply click this camera. Using this method one can move through any branches within selected node of the **Problem objects Tree**.

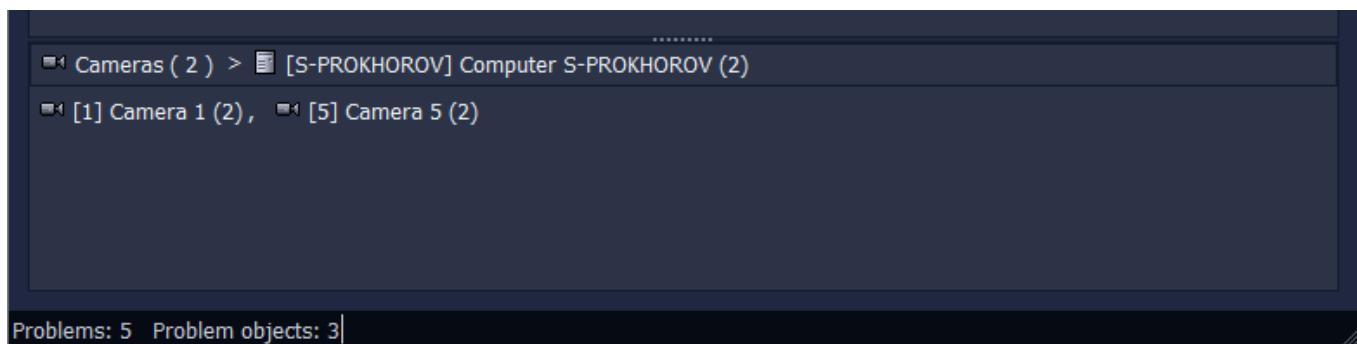


Figure 70. Result of moving through the levels

Diagnosed issues

Module can identify problems with different level of importance. List of issues to be detect and detailed problem description is presented in the following sections corresponding to the nodes of the **Problem Objects Tree**):

- [Video Server](#);
- [Camera](#);
- [Microphone](#);
- [Sensor](#);
- [Remote system](#);
- [Concentrator](#);
- SecurOS Auto (see [SecurOS Auto User Guide](#));
- SecurOS Cargo (see [SecurOS Cargo User Guide](#));
- SecurOS EDBE (see [SecurOS EDBE User Guide](#)).

4.6.1 Video Server

The following problems are diagnosed for the *Video Server* object:

- [Image Processor: task queue overloaded](#);
- [REST API: image export queue overloaded](#);
- [REST API: event queue for subscribers overloaded](#);
- [Archive was deleted because of insufficient drive space](#);
- [Archiver: drive is unavailable](#);
- [Archiver: file is corrupted](#);
- [Archiver: archive write error](#);
- [Video subsystem database is not available](#);
- [ACS database is not available](#);
- [Product version on Server does not match the one on the Configuration Server](#);
- [More than one Configuration Server was found in the system](#);
- [Server configuration is not up to date: update queue is currently overloaded](#);
- [Critical CPU load](#);
- [License expires in 24 hours](#);

- Give way to pedestrians detector's and LPR settings do not match;
- Failed to load synchronized files;
- Failed to start Movable PostgreSQL;
- Failed to connect iSCSI drive;
- Insufficient write speed;
- Insufficient speed of writing data to replicated database;
- Low free space on system drive;
- Not enough memory;
- There are unanalyzed dump files;
- Drive is not available;
- ACS is not available;
- Long-term archive file is corrupted;
- Disconnected;
- Archive write error;
- Audio archive write error;
- Alarms write error to Database;
- Application start error;
- Configuration update failed: Modules installed on servers do not match;
- Database query loss - insufficient database speed;
- Remote System objects exceed license limitations;
- Databases Replicator: error while writing into database;
- Replicated database is not available;
- Configuration Server is not available;
- ACS: time is not synchronized.

Image Processor: task queue overloaded

- The message appears if any *Image Processor*'s has more than 10,000 enqueued tasks. The queue may grow when the *Video Server* connection is lost or when exported frames aren't yet recorded into the video archive.
- The message disappears if the error does not repeat within 3 minutes.

REST API: image export queue overloaded

- The message appears if the *REST API*'s queue of image export requests is overloaded. New requests will be rejected.
- The message disappears if the error does not repeat within 3 minutes.

REST API: event queue for subscribers overloaded

- The message appears if the *REST API*'s queue of events is exceeded (10,000 events total for all subscribers). New events are not enqueued for sending to subscribers.
- The message disappears if the error does not repeat within 3 minutes.

Archive was deleted because of insufficient drive space

- The message appears if the primary video archive was deleted while the minimal retention period specified in the **Store at least** parameter of the *Camera* object (see [Recording Tab](#)) had not elapsed. This might happen when there is not enough space on the video recording drives (is specified in the **Archive** block of the [Computer](#) object settings) for the required archive retention time.
- The message disappears if the error does not repeat within 1 hour.

Archiver: drive is unavailable

- The message appears if it is impossible to connect to one of the drives specified in the *Archiver* object settings. Possible reasons are the following:
 - drive is disconnected;
 - hardware or driver error.
- The message disappears after the drive is reconnected.

Archiver: file is corrupted

- The message appears if the *Primary archive* file is corrupted and it wasn't added to the *Long-term archive*.
- The message disappears if the error does not repeat within 10 minutes.

Archiver: archive write error

- The message appears when it is impossible to save long-term video for any reason. For example, it appears when there is not enough disk space.
- The message disappears if the error does not repeat within 3 minutes.

Video subsystem database is not available

- The message appears if connection with the Video Subsystem database is lost. Information about alarms, bookmarks and EdgeStorage tasks is unavailable.
- The message disappears immediately after restoring the database connection.

ACS database is not available

- The message appears if the connection with the ACS database is lost.
- The message disappears immediately after restoring the database connection.

Product version on Server does not match the one on the Configuration Server

- The message appears if the version of the product installed on the *Peripheral Server* does not match the version of the product installed on the *Configuration Server*. System administration is limited.
- The message disappears immediately after the required version of the product is installed on the *Peripheral Server*.

More than one Configuration Server was found in the system

- The message appears if there are several *Configuration Servers* within the SecurOS network.
- The message disappears immediately after only one *Configuration Server* is left within the network.

Server configuration is not up to date: update queue is currently overloaded

- The message appears if the configuration update queue on the server contains more than 500 updates.
- The message disappears after the number of updates in update queue is reduced down to 100.

Critical CPU load

- The message appears if any single CPU core load exceeds 90%.
- The message disappears if all CPU core loads remains under 90% for several consecutive measurements.

License expires in 24 hours

- The message appears when the Product license is going to expire within 24 hours.
- The message disappears after the license key file is updated.

Give way to pedestrians detector's and LPR settings do not match

- The message appears if the license plate recognition event cannot be correctly processed because the number and/or values of the parameters of the *Give way to pedestrian* detector and the *License plate recognizer* are different. For example, there are 3 lines specified in the detector parameters and only 2 lines in the *License plate recognizer* object settings.
- The message disappears if the error does not repeat within 30 minutes.

Failed to load synchronized files

- The message appears if synchronized files could not be loaded. Possible reasons:
 - the file is damaged;
 - there is no access to the file.
- The message disappears if synchronized files have been downloaded successfully on server reboot.

Failed to start Movable PostgreSQL

- The message appears, if additional instance of PostgreSQL failed to start by any reason. For example due to internal data damage.
- The message disappears after additional instance of PostgreSQL successfully started.

Failed to connect iSCSI drive

- The message appears, if there was an error during connecting, authorizing or mounting iSCSI drive.
- The message disappears after iSCSI drive was successfully mounted.

Insufficient write speed

- The message appears if the total speed (bitrate) of the recorded streams exceed the actual drive write performance.
- The message disappears if the error does not repeat within 1 hour.

Insufficient speed of writing data to replicated database

- The message appears if the time of coping the data received from any of the original databases to the replicated database exceeds 3 minutes. Next data package from that database will be copied

after loading the previous one.

- The message disappears if the error does not repeat within 30 minutes.

Low free space on system drive

- The message appears if the system drive has less than 10 GB of free space.
- The message disappears if the free space on the system drive becomes more than 10 GB.

Not enough memory

- The message appears when more than 80% of server virtual memory is used during 1 minute. Virtual memory is the sum of the RAM size and the maximum size of the paging file.
- The message disappears if the error does not repeat within 1 minute.

There are unanalyzed dump files

- The message appears if C:\ProgramData\ISS\dumps folder (include subfolders) contains dump files.
- The message disappears after removing dump files from the specified folders.

Warning! To resolve this problem it is recommended to create an ISSInfo report (see [ISS System Report Utility \(ISSInfo\)](#)) and send it to the Intelligent Security Systems Technical Support Team.

Drive is not available

- The message appears if it is impossible to connect to one of the drives specified in the **Archive** tab of the *Computer* object settings. Possible reasons are the following:
 - drive is disconnected;
 - hardware or driver error.
- The message disappears after drive is reconnected.

ACS is not available

- The message appears if it is impossible to connect to the external ACS system:
 - there is no connection to the ACS server;
 - connection parameters are specified incorrectly;
 - SDK wasn't installed or installed incorrectly.

The message also appears if the connection with the ACS server is lost.

- The message disappears in 7 seconds after the connection with the ACS server is restored.

Long-term archive file is corrupted

- The message appears if the long-term archive file couldn't be found or read when performing playback in the *Media Client* or exporting video via *Archive Converter*.
- The message disappears if the error does not repeat within 1 hour.

Disconnected

- The message appears if the connection with the server is lost.
- The message disappears in 7 seconds after the connection with the server is restored.

Warning! This message is also displayed if an invalid or incorrect IP address is specified in the **IP address** parameter in the *Computer* settings.

Archive write error

- The message appears when it is impossible to save video for any reason. For example, not enough space on the hard drive, insufficient write speed, drive is unavailable, etc.
- The message disappears if the error does not repeat within 3 minutes.

Audio archive write error

- The message appears when it is impossible to save audio for any reason. For example, not enough space on the hard drive, insufficient write speed, drive is unavailable, etc.
- The message disappears if the error does not repeat within 3 minutes.

Alarms write error to Database

- The message appears if the alarms cannot be saved into the video subsystem database.
- The message disappears if the error does not repeat within 3 minutes after recording is resumed.

Application start error

- The message appears if an error occurred while starting the external application.
- The message disappears when the external application is successfully started.

Configuration update failed: Modules installed on servers do not match

- The message appears if the set of Modules installed on the *Peripheral Server* and the *Configuration Server* does not match. The current peripheral server configuration is incorrect. It will be updated automatically when the required Modules are installed on the *Peripheral Server*.
- The message disappears immediately after the configuration is updated.

Database query loss - insufficient database speed

- The message appears if the database transaction queue size is exceeded. New alarms, bookmarks and EdgeStorage tasks will not be recorded into the database.
- The message disappears if the error does not repeat within 1 hour.

Remote System objects exceed license limitations

- The message appears if the total number of *Cameras* or *License plate recognizers* in the *Remote systems* exceeds the numbers allowed by the SecurOS MCC license. Interaction with *Remote Systems* will be limited.
- The message disappears if the amount of the *Remote system* objects becomes less than the number allowed by SecurOS MCC license.

Databases Replicator: error while writing into database

- The message appears if replication is not possible or data cannot be copied in full for one of the following reasons:
 - distributed database or at least one of the original databases has incorrect markup;
 - a record cannot be copied due to corruption in the source database.

- The message disappears if the error does not repeat within 10 minutes.

Replicated database is not available

- The message appears if the connection with replicated database is lost.
- The message disappears immediately after the connection with the database is restored.

Configuration Server is not available

- The message appears when connection with the *Configuration Server* is lost.
- The message disappears in 7 seconds after the connection with the *Configuration Server* is restored.

ACS: time is not synchronized

- The message appears in the following cases:
 - event time stamp within ACS is more than 2 seconds ahead of *Video Server*'s system time;
 - time stamp of the current event within the ACS is less than the time stamp of the previous event.
- The message disappears if these errors are not repeated within 3 minutes.

4.6.2 Camera

The following problems are diagnosed for the *Camera* object:

- **Microphone is detached;**
- **Archive integrity error;**
- **Camera is detached;**
- **Frame corrupted;**
- **Stream N is disconnected;**
- **Stream N GOP exceeds recommended size;**
- **Edge Storage is not accessible;**
- **Edge: archive corrupted;**
- **Edge: time isn't in sync;**
- **Edge: Video Server response timeout expired;**
- **Edge: no information about archive;**
- **Edge: requested records not found;**
- **Edge: error downloading archive.**

Microphone is detached

- The message appears when there is no signal from the *Microphone* linked to the *Camera*.
- The message disappears in 7 seconds after the connection with the *Microphone* is established.

Archive integrity error

- The message appears if the primary video or audio archive file couldn't be found or read when performing playback in the *Media Client* or exporting video via *Archive Converter*.

Warning! The archive file can be deleted when the drives don't have enough free space or when it's retention period is expired. In this case it is not considered a problem.

- The message disappears if the error does not repeat within 1 hour.

Camera is detached

- The message appears when the system fails to receive the video stream selected as the **Stream for recording** in the *Camera* object settings. If the **Stream for recording** is unavailable then all other streams are disabled.
- The message disappears if the specified video stream is received from the *Camera* during 7 seconds and the content of this stream is correct.

Note. This problem is not diagnosed for *Cameras*, if their parent *Video Capture Device* has a **ISS Video Concentrator** type.

Frame corrupted

- The message appears if the frame couldn't be recorded or read when performing playback in the *Media Client* from primary or long-term archive.
- The message disappears if the error does not repeat within 1 hour.

Stream N is disconnected

- The message appears if it is impossible to receive the specified video stream from the *Camera* or the content of the video stream is incorrect.
- The message disappears if the specified video stream is received from the *Camera* during 7 seconds and the content of this stream is correct.

Stream N GOP exceeds recommended size

- The message appears if Stream N's GOP size exceeds the recommended 2 seconds.
- The message disappears in 1 minute if the issue doesn't occur.

Problems when working with EdgeStorage Sync (see [Camera Local Storage \(Edge Storage\)](#))

Edge Storage is not accessible

- The message appears if the attempt to connect to the camera's local data storage failed. This message appears in case of connection errors other than camera connection loss. For example, when authorization failed.
- The message disappears in 3 minutes after the camera's local date storage is connected.

Edge: archive corrupted

- The message appears if the camera's archive contains different recordings for the same time period.
- The message disappears if the error does not repeat within 3 minutes.

Note. In many cases this problem raises due to overlapping records by time caused by moving camera's system time backward.

Edge: time isn't in sync

- The message appears if the camera's time is not synchronized with the *Video Server*'s time.
- The message disappears if the error does not repeat within 3 minutes.

Edge: Video Server response timeout expired

- The message appears if the *Video Server* failed to provide information about the video archive during the specified timeout.
- The message disappears if the error does not repeat within 3 minutes.

Edge: no information about archive

- The message appears if the camera failed to provide correct information about the edge archive.
- The message disappears if the error does not repeat within 3 minutes.

Edge: requested records not found

- The message appears if the requested recordings are missing in the camera's edge archive. It won't be copied to the *Video Server* archive.
- The message disappears if the error does not repeat within 3 minutes.

Edge: error downloading archive

- The message appears if an error occurs when copying archive recording.
- The message disappears if the error does not repeat within 3 minutes.

4.6.3 Microphone

The following problem is diagnosed for the *Microphone* object:

Microphone is detached

- The message appears when there is no signal from the *Microphone*.
- The message disappears in 7 seconds after the connection with the *Microphone* is established.

4.6.4 Sensor

The following problem is diagnosed for the *Sensor* object:

Sensor is sabotaged

- The message appears when the *Sensor* produces a SABOTAGE event (see [SecurOS Programming Guide](#)).
- The message disappears in 7 seconds after receiving an event other than SABOTAGE.

4.6.5 Remote System

The following problems are diagnosed for the *Remote System* object:

- **Configuration update failed: some objects are not supported by SecurOS MCC;**
- **Disconnected.**

Warning! These problems are diagnosed for the *Remote System* object only for **Direct Connect** type of the *Monitoring Center* connection.

Configuration update failed: some objects are not supported by SecurOS MCC

- The message appears if the set of Modules installed on *SecurOS MCC* and the *Remote System* does not match. Interaction with the *Remote System* will be limited. The current configuration is out of date. It will be updated automatically when the required Modules are installed on *SecurOS MCC*.
- The message disappears immediately after the configuration is updated.

Disconnected

- The message appears if the connection with the *Configuration Server* of the remote system is lost or the server specified in the system settings is not a *Configuration Server*. Interaction with the *Remote System* will be limited.
- The message disappears in 7 seconds after the connection with the *Configuration Server* is established.

Note. This problem also raises if incorrect address is specified in the **Configuration Server address** parameter of the *Remote System* object settings.

4.6.6 Concentrator

The following problem is diagnosed for the *Concentrator* object:

Warning! This problems is diagnosed for the *Concentrator* object only for **VC/VR Connect** type of the *Monitoring Center* connection.

Disconnected

- The message appears if the *ISSVideoConcentrator* cannot receive a video stream from the remote system.
- The message disappears in 7 seconds after the connection with the remote server is established.

4.7 SecurOS Files Synchronization

Some modules, integrations and settings of SecurOS require additional or changed files to be located at every *Video Server* and *Operator Workstation*. The SecurOS *Configuration Server* syncs such files between all computers within the security network.

The synchronization process goes by the following rules:

- The following files are synchronized:

— *.dbi — only in SecurOS root folder;
— *.ddi — only in SecurOS root folder;
— Modules/map/*.ini;
— Modules/Map/scripts/*.js;
— skins/_common/acs/*.png;
— acs_*.json — only in SecurOS root folder;
— *.integration.json — in SecurOS root folder and its subfolders.

- Files to sync are being uploaded to the *Configuration Server* memory when SecurOS starts. If new files were created on the server or some files were changed, it is required to restart SecurOS on the *Configuration Server*.
- If SecurOS on the *Configuration Server* is restarted with new/changed files, all *Peripheral Servers* automatically restart their SecurOS instances to sync files.
- *Operator Workstation* downloads files from the *Video Server* it connects to. Received files are stored in C:\ProgramData\ISS\client folder.
- Synchronization is only possible between computers with the same version of SecurOS.

Warning! In case of cluster the files on the *Configuration Server* must be changed only in the service mode (see [Configuring Cluster](#)).

5 Core Subsystem

The core subsystem communicates with the computers in the SecurOS distributed network, with installed intelligent modules (such as license plate recognition module), and with other subsystems (such as the video or audio subsystem, or the telemetry subsystem).

5.1 Working Principles

The core subsystem is the SecurOS core and it monitors the status of all connected objects, modules and devices.

Status data and information about all on-stream events are sent from each SecurOS object to the core subsystem which establishes managing of the whole security network.

The computers interconnected by means of the core subsystem are nodes of the SecurOS distributed network. Every node connection or disconnection is registered in the SecurOS security network log file in real time.

The SecurOS core subsystem allows connection and disconnection of the security network nodes, configuration and synchronization of information between the security network nodes, as well as monitoring any changes in modules and objects status.

If any single node or a certain network segment is disconnected, it is assigned the disconnected status and it becomes inaccessible for administration until it is connected again. When the previously disconnected node is connected again, the updated network configuration data is loaded on it, and the events log on this node is synchronized with the up-to-date SecurOS security network log file.

Permanent updating of the security network configuration data allows the configuring of the security network from any computer running the necessary administration software, watching video from connected video cameras, listening to audio, sending commands to hardware, and monitoring and controlling alarm and fire alarm systems from every operator's workstation within the SecurOS network.

5.2 Object Reference

The core subsystem includes the following objects:

- [System](#).
- [Security Zone](#).
- [Database](#).
- [Department](#).
- [User Account](#).
- [Active Directory / LDAP](#).
- [User Rights](#).

- Computer.
- Event Filter.
- SNMP agent.
- External application.
- Databases Replicator.

5.2.1 System

This is the root object of the entire Object Tree and provides system-wide settings. This object cannot be deleted, moved, or disabled. Operations of viewing and editing object parameters are available only to the superuser (see [SecurOS Users](#)).

Parent object – none (root object).

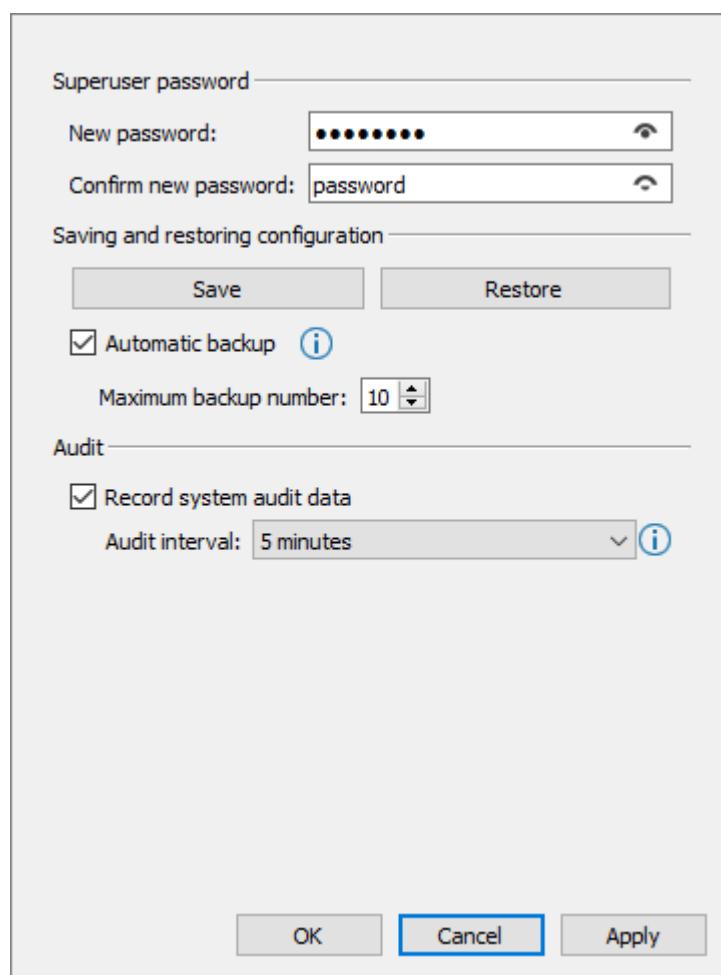


Figure 71. System object settings window

Table 5. System object settings

Parameter	Description
Superuser password (To display entered characters click the button. To hide them click the button.)	
New password	Enter new password (see Changing Superuser Password).

Parameter	Description
Confirm new password	Retype new password to confirm.
Saving and restoring configuration	
Save (button)	<p>Click this button to save the current configuration (Object Tree and all object settings) to an XML-file. Use Windows file manager to specify folder and file name. By default, file will be saved in the %ProgramData%\ISS\Sys_config folder as default.xml.</p> <p>Warning! It is not recommended to save the configuration as wizard.xml because this file name is reserved and used to automatically save the last successfully loaded configuration.</p>
Restore (button)	<p>Click this button to restore system configuration from the file. The configuration file is selected by the administrator from the list of previously saved ones. Configuration restoring procedure contains the following steps:</p> <ul style="list-style-type: none">Restoring configuration on the <i>Configuration Server</i>.Updating configuration on all <i>Peripheral Servers</i> from the <i>Configuration Server</i>. Configuration of the <i>Peripheral Server</i> that has been used before updating is saved to the file. <p>When it is impossible to restore the configuration from the file the current configuration is rolled back.</p>
Automatic backup	<p>The flag to control automatic backup mode of the current system configuration. By default it is selected. In this mode the backup copy:</p> <ul style="list-style-type: none">Is created daily at 01:45 local time.Is created only if the configuration has been changed during the last day.Is created on each <i>Video Server</i> even the connection between <i>Peripheral Server</i> and <i>Configuration Server</i> is lost. In this case the copies of the configuration will vary.Is created in the %ProgramData%\ISS\Sys_config folder with the Backup_<date>_r<configuration revision>.xml name, for example, Backup_2019-07-01_r000000016.xml. Date is specified in the ISO format.Is created out of schedule if the current non-empty configuration is restored from a file. A copy is also created at system startup, if at the start time the current system configuration is different from the last backup copy or there is no backup copy. <hr/> <p>Note. When working in the SecurOS MCC configuration any changing of the external system configuration results in changing of the SecurOS configuration.</p>

Parameter	Description
Maximum backup number	Specify maximum number of the backup copies. Range of values: [1; 30]. When the maximum value is reached, automatically created configuration copy files are deleted "by the ring". Configuration files with names other than the template ones are not deleted.
Audit	
Record system audit data	Select this checkbox to audit the system and record obtained data. Data will be recorded to the special audit database that will be automatically created after applying new settings.
Audit interval	<p>Select the audit interval from the list. Audit interval means the time period that is used to trace the prolonged user actions within the system. The following user actions are called prolonged:</p> <ul style="list-style-type: none"> • viewing live and archive video; • controlling PTZ. <p>Warning! Each astronomical hour contains several audit intervals. The beginning of the first audit interval in an hour coincides with the beginning of each astronomical hour.</p> <p>Specified value affects the database entries creation, which can be viewed via AuditClient utility. Analysis of the utility work results is considered in detail in the User Action Analysis Example section.</p>

5.2.2 Security Zone

This object is used to divide the entire security network into separate security zones. Security Zones are commonly used when the SecurOS system ranges over a large territory where independent centralized monitoring and supervision is needed for certain physically separated zones.

Additionally, one can organize events filtering between system's *Video Servers*. Using filter it is possible to permit or to forbid transmission of all system events to selected *Video Server* (see [Servers to Connect Tab](#)).

System users can be also granted with different access rights to implement multi-level access control for the security objects (see [User Registration and Configuring User Rights](#)). For example, in a security center the operators can observe the territory by watching the signals from the cameras. The supervisor can be granted the rules to control the monitoring modes, enable or disable cameras, control the PTZ cameras, and the head of the security center can generate reports.

Object settings allows to distribute loading from *Operator Workstations* between *Video Servers* (see [Servers to Connect Tab](#)). The white list of IP addresses, from which one can connect to the *Video Servers*, can be created as additional protection feature (see [Connection Restrictions Tab](#)).

Using security zones and user rights, administrative status can be assigned specifically to distribute control of secured territory between independent companies. In this case, SecurOS network is separated into several segments and each administrator may monitor and configure only one of those segments.

Note. A separate events log is used for each security zone.

It is recommended to use several security zones if:

- access control subsystem uses hardware identifiers (cards) with different facility codes on different territories;
- access control subsystem is distributed across several zones with different access schedule (different holidays), and if each zone has its own departments and persons (i. e. several organizations within one office building);
- you need to store separate event logs for a subset of SecurOS objects, with different database depth.

Parent object — **System**.

Parameter settings windows contains the following tabs:

- **General** Tab.
- **Servers to Connect** Tab.
- **Connection Restrictions** Tab.

5.2.2.1 General Tab

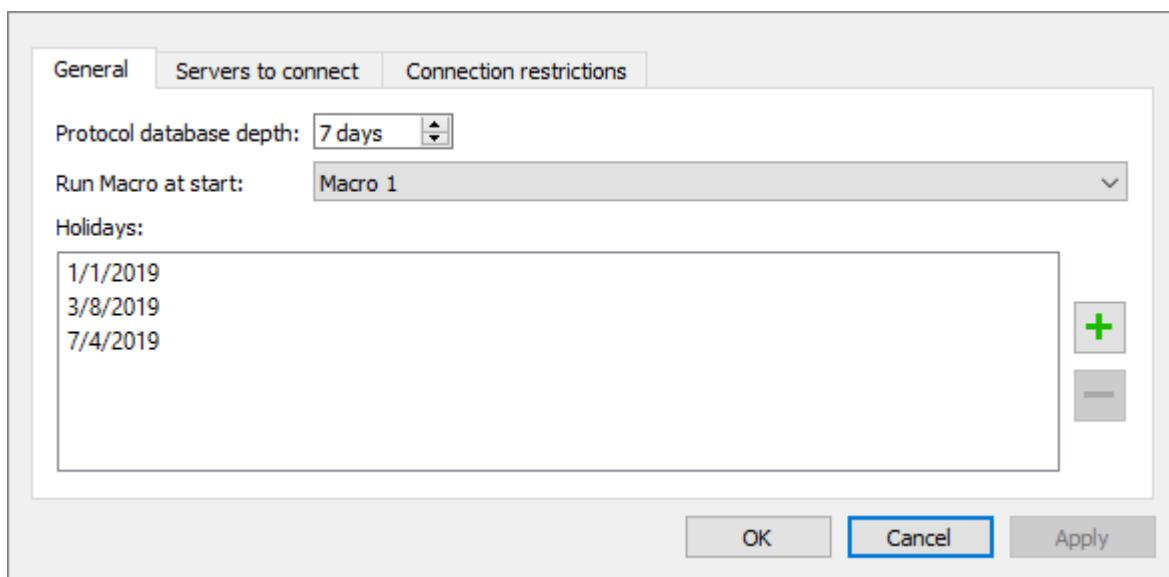


Figure 72. Security Zone object settings window. General Tab

Table 6. Security Zone object settings. General Tab

Parameter	Description
Protocol database length	Define the events storage period in the <i>Event Viewer</i> database (in days, max). Event database stores events from objects that belong to this security zone only. Possible values: [1 ; 9999]. Default value: 7. Messages will be deleted automatically when the retention period has expired. Removal is performed when SecurOS starts or once a day at 00:00:00 (hh:mm:ss) a.m.

Parameter	Description
Run Macro at start	Select from the list of accessible macros (<i>Macro</i> objects, see Macro) the one which will be activated on <i>Video Server</i> on system startup, if necessary (see Macro running conditions).
Holidays	Fill in the table containing a list of dates (in DD.MM.YY format) that will be used by a access control subsystem as holidays. Those days are also used in Schedule .

Macro running conditions

Macro will be started if all executors that implement the SecurOS features are successfully launched. If SecurOS' Intelligent Modules (for example, SecurOS Auto) are installed, all executors of these Modules must be started, too. If at least one of the executors has not started, the *Macro* will not be started.

5.2.2.2 Servers to Connect Tab

Operator Workstation is a client application and must be connected to the SecurOS server to work. For the first time connection is performed manually. Operator specifies server to connect in the **Authorization** window (see [Launching SecurOS On Operator Workstation](#)). Further automatic authorization can be adjusted (see [Auto login](#)).

Appearance of the tab is represented in Figure 73.

Tab allows to specify to which servers *Operator Workstations* can connect, to which can not, and also divide these servers into groups. Dividing servers into groups allows to balance servers loading. So, if some server fails, system will attempt to reconnect *Operator Workstation* to other server of the same group.

Note. To change server group to connect it is necessary logoff user and reconnect to the server from other group.

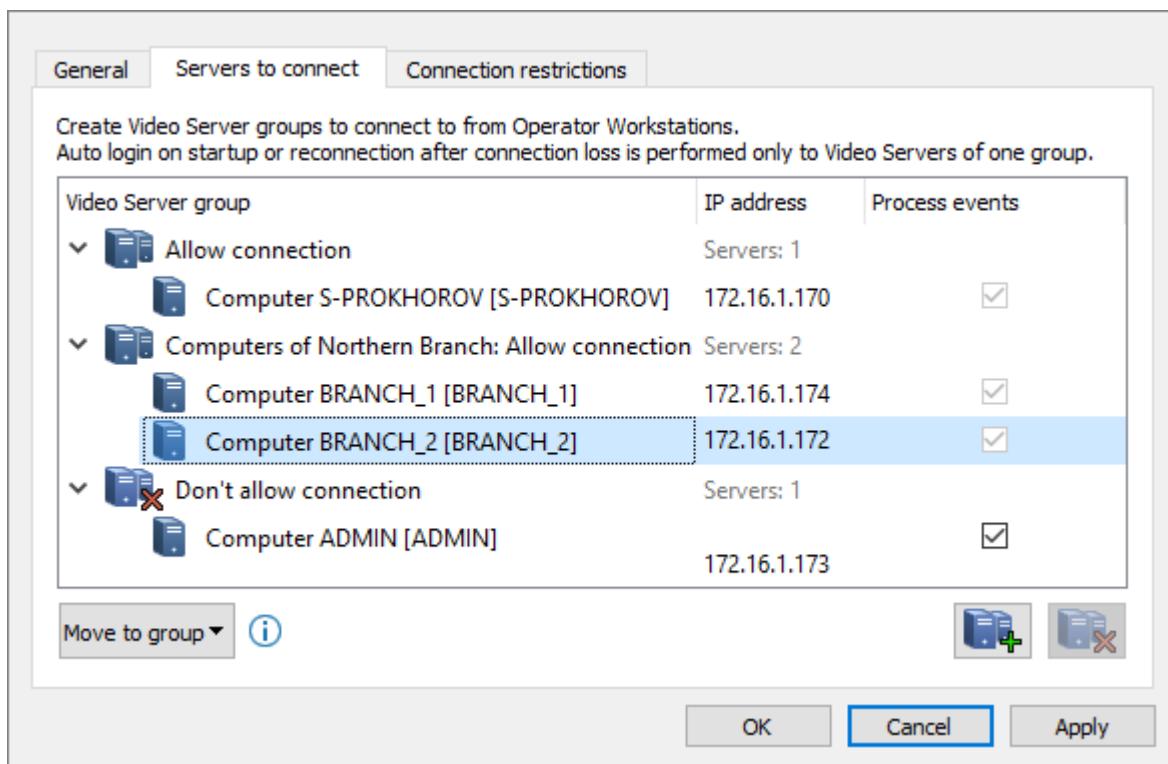


Figure 73. Security Zone object settings window. Servers to Connect Tab

By default, server list contains two groups – **Allow connection** and **Don't allow connection**. By default all servers, existed in the SecurOS, are located in the **Allow connection** group. All newly created *Video Servers* also are added to this group.

For the *Video Server*, depending on whether it belongs to a group, one can either allow or prohibit receiving and processing events from other *Video Servers* of the system. This setting applies to all events. Forbiddance to process an event reduces network loading associated with events transmission. If *Video Server* is included in the group:

1. **Allow connection** – the **Process events** checkbox is selected by default and can't be deselected. Such servers will always receive and process all events from other *Video Servers* of the system.
2. **Don't allow connection** – the **Process events** checkbox is selected by default and can be deselected. Thus, receiving and processing events from other *Video Servers* of the system can be prohibited for the *Video Servers* of this group.

Warning! When connecting to the servers from the **Don't allow connection** group logon can be performed only by superuser (see [SecurOS Users](#)). Other users can logon only when client application is connected to this server locally. Thus, if the **Process events** checkbox is not selected for such servers, then object's states on these servers will be irrelevant, because events from other servers of the system are not received and processed.

The following operations are available when working with the list:

1. *Creating group* – to create a new server group click on the  (**Create group**) button. Group will be created with the N: Allow connection name, where N – serial number of the group with this default name (if server list contains such groups).
2. *Rename group* – to rename group, click it and specify new name in the text field.
3. *Deleting group* – to delete group, select it in the list and click on the  (**Delete group**) button.

Warning! Group that contains servers can not be deleted. To delete such group, move all servers to other group first. System groups Allow connection and Don't allow connection can not be also deleted.

4. *Moving server to other group* — to move one or several servers select them, click on the **Move to group** button and select required group from the list. Also, the server can be moved to the required group using drag-and-drop.

5.2.2.3 Connection Restrictions Tab

This tab allows to set a list of computers, that can connect to the SecurOS servers. Tab appearance is represented on Figure 74.

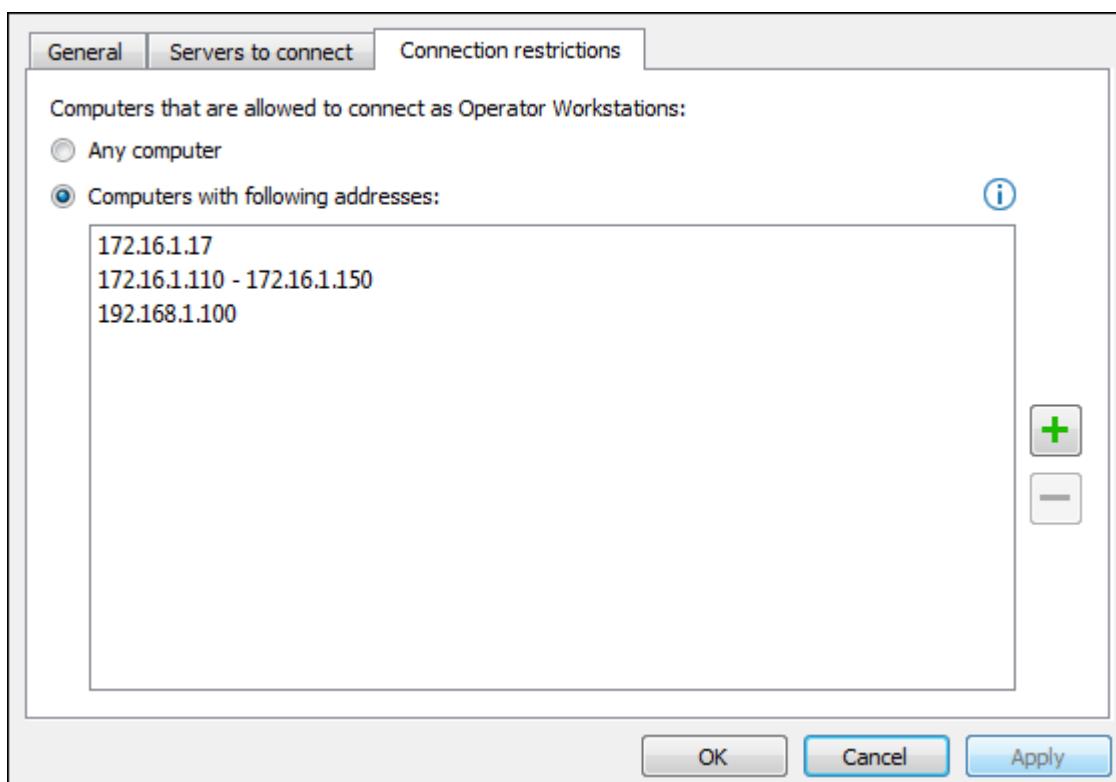


Figure 74. Security Zone object settings window. Connection Restrictions Tab

Any computer mode is set by default and means that any computer where SecurOS software is installed can connect to any system server taking into account **Servers to Connect** tab settings. It is enough to operator to know SecurOS user's login and password.

As an additional security option, you can restrict the list of computers from which the servers will accept the connection. To set such restriction do the following:

- Set the **Computers that are allowed to connect as Operator Workstations** parameter to Computers with following addresses.
- Add IP addresses of computers to the list below, using button. If there are many such computers and they have serial IP addresses, it is convenient to specify the range of IP addresses. For example, 172.16.1.110-172.16.1.150.

Note. When working in cluster configuration (see [Failover cluster](#)) and operator interface is planned to be used on cluster Hosts, all Hosts IP addresses, virtual IP addresses of the Nodes and virtual IP address of the Configuration Server must be added to the list.

5.2.3 Database

Within SecurOS this object represents the databases of the SecurOS security system, databases of the SecurOS' Modules and external databases.

Parent object – *Security Zone\Datasets group*.

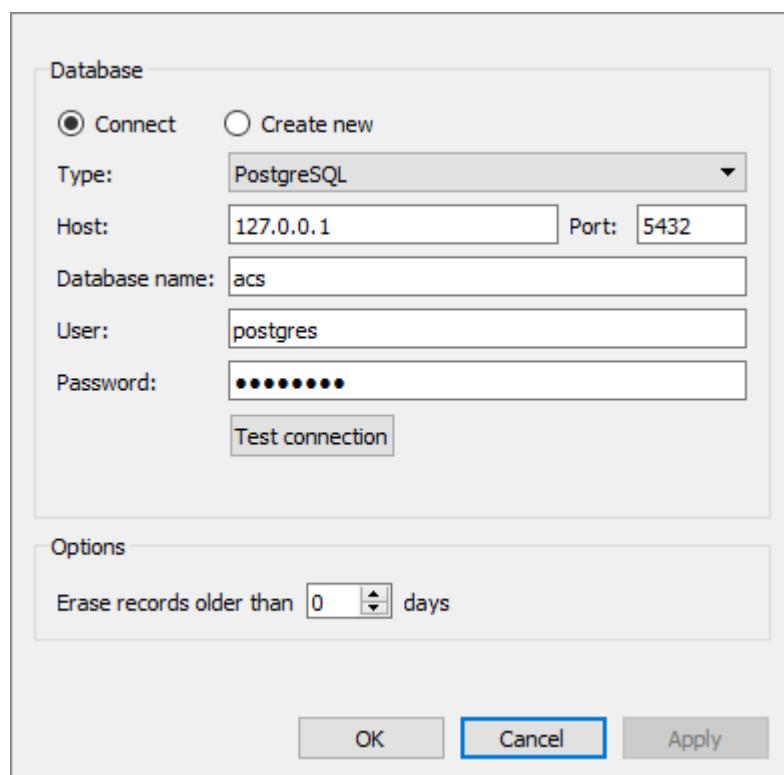


Figure 75. Database object settings window

Table 7. Database object settings

Parameter	Description
Database	
Connect (radio-button)	Connect to the previously created <i>Database</i> using specified below parameters.
Create new (radio-button)	Create new <i>Database</i> and <i>User account</i> (see Figure 76). Warning! Create new <i>Database</i> operation is performed only when working with the <i>SecurOS ACS Module</i> (see SecurOS ACS User Guide).

Parameter	Description
Type	<p>Database type. Possible values:</p> <ul style="list-style-type: none">• PostgreSQL – provides connection with PostgreSQL database;• SQL Server – provides connection with Microsoft SQL Server database. <p>Default value is PostgreSQL.</p>
Server	DNS-name or IP-address of database server. If the database is installed on the local computer which is used to configure the system, use default value.
Port	Port number for database connection. Default value is 5432.
Database name, Login, Password	<p>Database name, user name and password are as defined during the database installation.</p> <p>Warning! Use Latin characters only when specifying a Password. Latin-1 code page (Western European character set) is acceptable.</p>
Test connection (button)	To check the database connection with the defined parameters click the Test connection button. If the parameters are set correctly and there is a connection to the LAN, then OK will be displayed to the left of the button.
Options	<p>Retention period for records (in days). If set to 0, the records are not deleted.</p> <hr/> <p>Note. When working with some of the SecurOS intelligent Modules parameter is ignored.</p>
Erase records older than	

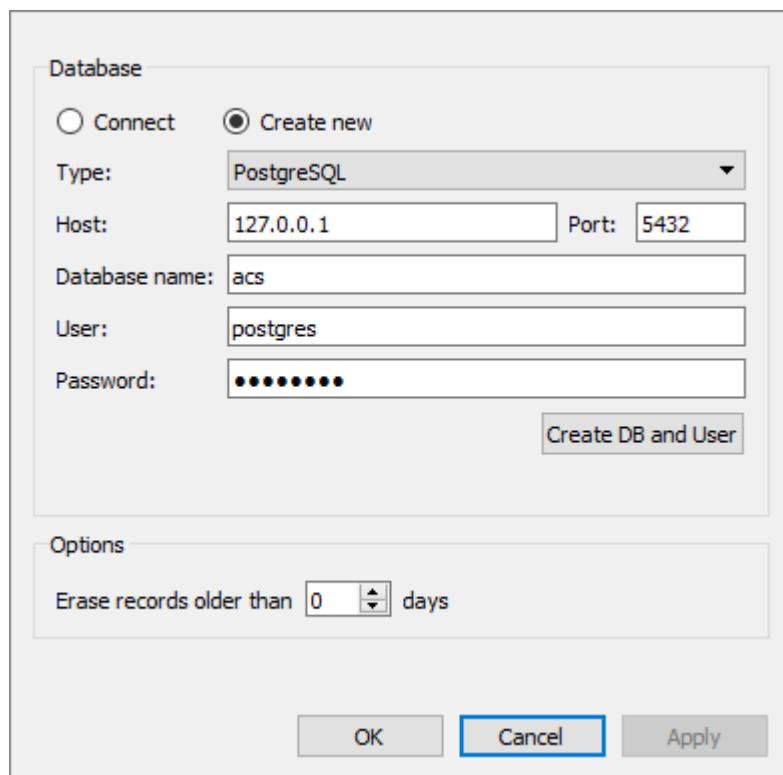


Figure 76. Creating new Database and User account

Table 8. Database object creation settings

Parameter	Description
Database	
Create DB and User	Create new <i>Database</i> to use it with external ACS systems (see SecurOS ACS User Guide). After specifying parameters, click on this button to create a new database in the PostgreSQL folder and its user account. Created database will be marked up to store data, received from an external ACS system.
Note. Other parameters of the created <i>Database</i> are similar to described above.	

5.2.4 Department

This object is used to organize system users into groups. Primarily it is used in conjunction with an access control subsystem to define users to manage their user right policies within the SecurOS network itself (see [User Registration and Configuring User Rights](#)).

Parent object – *Security Zone\Users & Permissions* group.

Object has no settings to configure.

Note. *Department* object is automatically created in the objects tree only if users with the *Power user* or *Simple user* rights were added during system configuration with the help of System Configuration Wizard.

5.2.5 User Account

This object represents a single person (either a person registered in an access control system or a user within the SecurOS network).

Parent object – **Department**.

Warning! Name of the *User account* object, specified in the **Parameters of created object** window, will further used as username when logging on the system. At the same time, the authorization is possible only on that Computers, which belong to the same *Security Zone*, as a created *User account*.

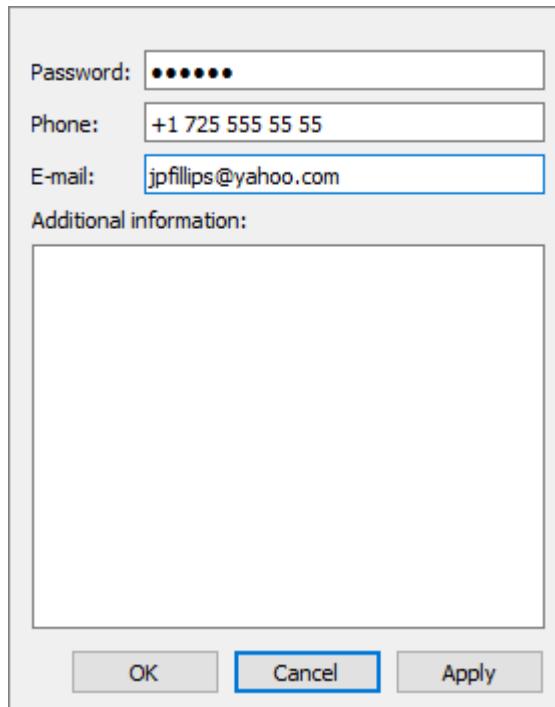


Figure 77. User Account object settings window

Table 9. User Account object settings

Parameter	Description
Password	User password. Is used to log on the system if some access rights were assigned to this user (see User Rights). Required parameter. To view hidden characters of the password click the button.
Phone	Insert person's phone number. Not used by the system itself. You can use this field when writing SecurOS scripts to send voice or SMS notifications.
E-mail	Insert person's e-mail address. Not used by the system itself. You can use this field when writing SecurOS scripts to send email notifications.
Additional Information	Insert any text in this field, for example, person's passport number, position or any other description you need. Not used by the system itself.

5.2.6 Active Directory / LDAP

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

This object is used to configure settings of the network domain to provide authorization in the SecurOS network. For further information see [Configuration of Network Domain User Rights](#).

Parent object – *Security Zone\Users & Permissions* group.

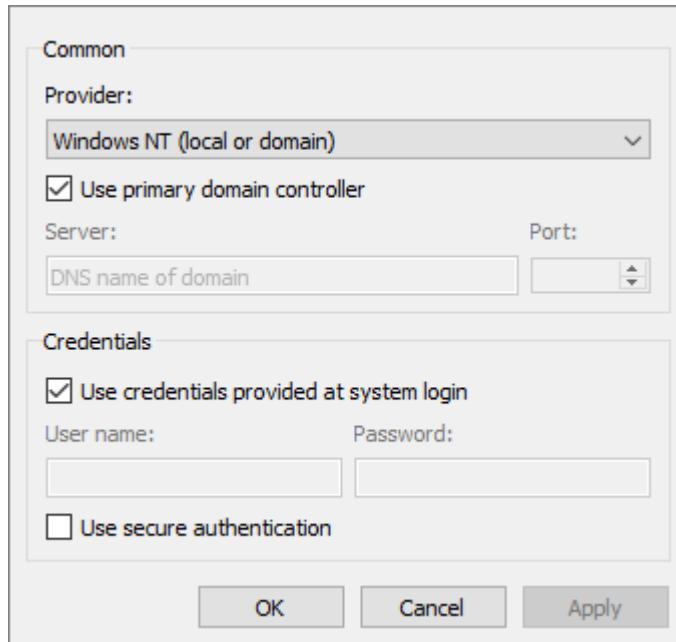


Figure 78. Active Directory / LDAP object settings window

Table 10. Active Directory / LDAP object settings

Parameter	Description
Common	
Provider	Select the type of protocol from the drop-down list. Possible values: <ul style="list-style-type: none">• Windows NT (local or domain) – only for Windows;• LDAP (domain) – for Windows and Linux.
Use primary domain controller	Enable this checkbox to use the primary domain controller for connection. Warning! If this field is checked, then the next two parameters will be unavailable.

Parameter	Description
Server	Specify domain controller parameters depending on selected Provider : <ul style="list-style-type: none">• Windows NT (local or domain) – specify short domain name (for example, OFFICE) to provide user authorization on the computer registered in the domain. To provide user authorization from the computer connected to the network, but not registered in the domain, specify full domain name (for example, OFFICE.COMPANY).• LDAP (domain) – to provide user authorization specify IP address or DNS name of the domain controller.
Port	<i>Optional:</i> specify server network port for connection. Must be specified for LDAP (domain) provider or when server has non-standard settings.
Credentials	
Use credentials provided at system login	Enable this checkbox to use name and password of Windows user currently logged in. Warning! If this field is checked, then the next two parameters will be unavailable.
User name, Password	Specify user name and password for authentication on server.
Use secure authentication	Enable this checkbox to use secure password authentication.

5.2.7 User Rights

This object is used for defining user rights within the system (see [User Registration and Configuring User Rights](#) for detailed description).

Note. All users in the *User Rights* object settings have the same level of access. To assign another set of rights to another user or user group, create a different *User Rights* object.

Parent object – *Security Zone\Users & Permissions* group.

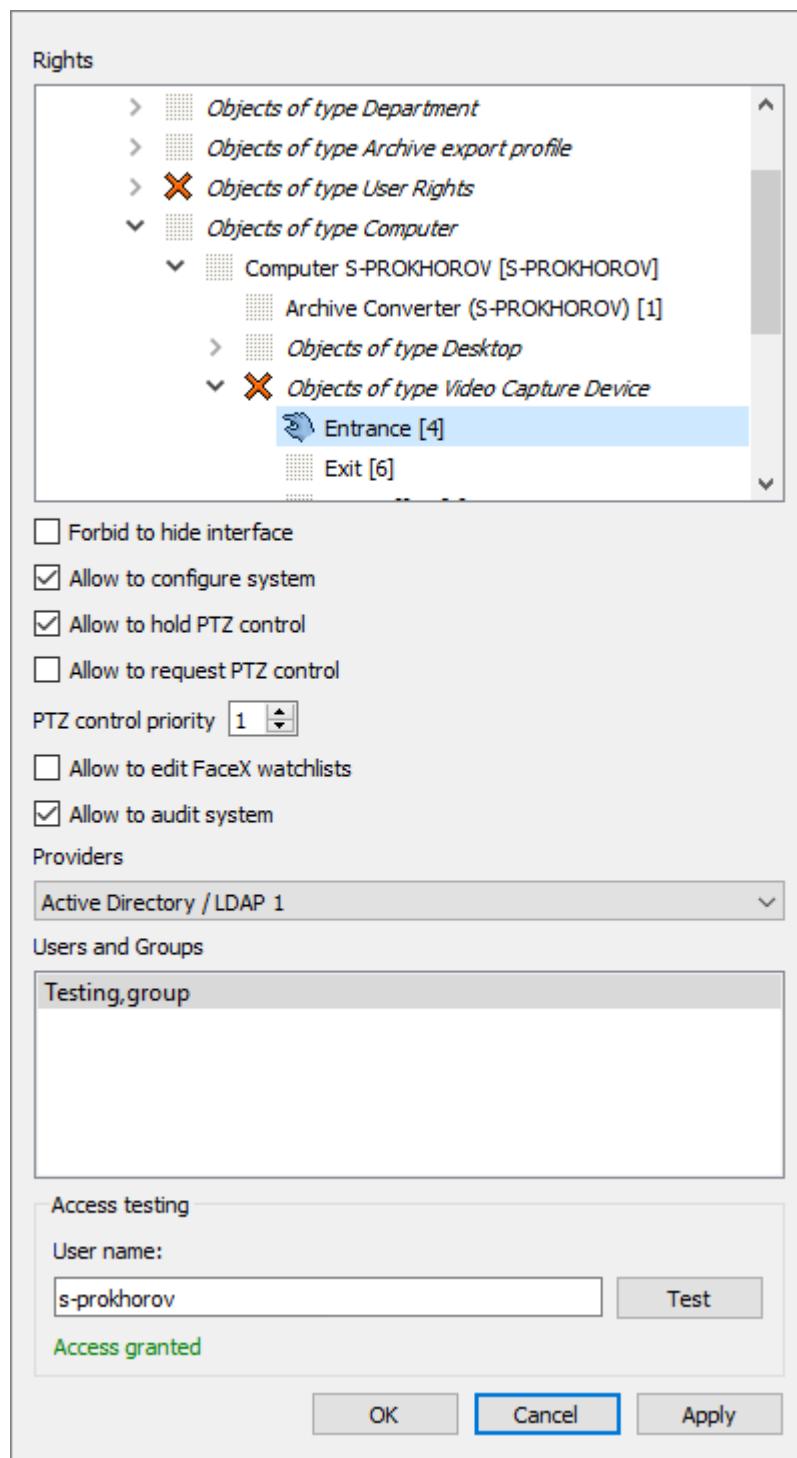


Figure 79. User Rights object settings window

Table 11. User Rights object settings

Parameter	Description
Rights	Object Tree with icons that depict user rights of each object. To define a user access to any object, click the icon to the left of the object or group (<i>Objects like...</i>) consecutively, until the required icon is displayed. Icons are described below.
Forbid to hide interface	Select this field if user is not allowed to hide user interface objects.

Parameter	Description
Allow to configure system	<p>This parameters defines user access to the SecurOS <i>Object Tree</i> with the help of the Configure the system button (see Administration Center).</p> <p>If this field is selected, then user has access to the <i>Object Tree</i> to view and change system parameters (Administrator mode, see icons description below).</p> <p>If this field is not selected, then user has no access to the <i>Object Tree</i> to view and change system parameters (Operator mode, see icons description below).</p>
Allow to hold PTZ control	Tick this checkbox to allow operator to hold PTZ control for a long time (see Holding PTZ Control for a Long Time).
Allow to request PTZ control	Select the checkbox to allow user to request access to PTZ control of the camera in case when the user with higher priority value is holding it.
Control PTZ priority	Parameter allows user ability to intercept camera telemetry control if shared telemetry control mode is off (see Camera). Preferences of telemetry control has the user with greater priority value. If two or more user have equal telemetry control priority, then preferences has that of them who capture control first. Possible values: [1; - 10].
Allow to edit FaceX watchlists	Select the checkbox to allow user to edit SecurOS FaceX watchlists (see SecurOS FaceX User Guide).
Allow to audit system	Select the checkbox to allow user to audit the system (see AuditClient Utility).
Providers	Choose SecuroOS (local) value to accept rights to access the selected objects for users from the Users and Groups list (see below) or choose the Active Directory / LDAP object name as it appears in the Object Tree to accept certain rights to user / user groups of the network domain (see Active Directory/LDAP).

Parameter	Description
Users and Groups	<p>List of users and groups that have above rights.</p> <p>If SecurOS (local) value is selected in the Providers field, then double-click the empty string and select user from the list of registered <i>User accounts</i> to add a new user. To delete user from the list select required entry then press the Delete key.</p> <p>On selecting the Active Directory / LDAP object from the Providers list, the list should be formed as described in Configuration of Network Domain User Rights.</p> <p>In each case the name of the person will be used as the username when logging into SecurOS.</p> <hr/> <p>Note. The same user (<i>User Account</i> object) cannot be added to 2 or more different <i>User Rights</i> objects.</p> <hr/> <p>Warning! When <i>User account</i> is logging on into the SecurOS, then the password specified in the settings of the appropriate object (see User account) will be used.</p>
Access testing	
User name	Enter the name of the OS user or typical SecurOS user for which it is necessary to check possibility of authorization in SecurOS.
Test (button)	Click this button to start testing. For the detailed description of the testing procedure see User Registration and Configuring User Rights .

Access level of the user/user group to the object/object group (the **Rights** block) is marked with appropriate icon. Icon can be changed by clicking on it.

The following icons are available:

-  – **No access**. This access level defines the following rules of the object behavior:
 - in the *Administrator mode* – object/group is displayed in the SecurOS *Object Tree*. Configuring and other operations with object/group are not allowed (all buttons on the *Administration toolbar* are disabled);
 - in the *Operator mode* – object/group is not displayed in the SecurOS operator's interface.

Warning!

1. If this access level is set for the *Security Zone*, then this object and all children objects are not displayed in the SecurOS *Object Tree*.
2. If this access level to the *Computer* object is set for the user/user group, then no one of these users can log on into system on this computer.

-  – **View**. This access level defines the following rules of the object/group behavior:
 - in the *Administrator mode* – object/group is displayed in the SecurOS *Object Tree*. Configuring and other operations with object/group are not allowed (all buttons on the *Administration toolbar*

are disabled);

- in the *Operator mode* – object/group is displayed in the SecurOS operator's interface. Object management is disabled. For example, *Camera* is displayed in the *Media Client* interface, but user can not start record.
-  – **Control**. This access level defines the following rules of the object/group behavior:
 - in the *Administrator mode* – similar to the **View** access level.
 - in the *Operator mode* – object/group is displayed in the SecurOS operator's interface. Object management is enabled. For example, *Camera* is displayed in the *Media Client* interface, user can start record, control PTZ, etc.
-  – **Configure**. This access level defines the following rules of the object/group behavior:
 - in the *Administrator mode* – object/group is displayed in the SecurOS *Object Tree*. Object configuring is allowed (the **Setup** button on the *Administrator toolbar* is enabled). All other operations with object/group not allowed (all other buttons on the *Administrator toolbar* are disabled);
 - in the *Administrator mode* – similar to the **Control** access level.
-  – **Full access**. This access level defines the following rules of the object behavior:
 - in the *Administrator mode* – object/group is displayed in the SecurOS *Object Tree*. Configuring and other operations with object/group are allowed (all buttons on the *Administration toolbar* are enabled);
 - in the *Administrator mode* – similar to the **Control** access level.
-  – **Inherited rights** – rights for this object/group are inherited from parent object. This access level is used by default when creating a new object.

5.2.8 Computer

This object represents an individual computer within SecurOS network (*Video Server* or *Operator workstation*).

Video Servers and *Operator Workstations* within SecurOS network are registered and represented as *Computer* objects in the system *Object Tree*. Server part of the SecurOS is started on *Video Servers*, and client part is started on *Operator Workstations*. Client part can also be started on *Video Server*.

SecurOS' *Video Servers* can send and receive events from other *Video Servers*. To reduce the network load associated with the events transmission one can exclude selected network servers from the event distribution list (see [Servers to Connect Tab](#)).

To denote role and state of the *Computer* within SecurOS network the following icons of the *Object Tree* are used (see Figure 80):

-  – *Configuration Server* (computer role is *Video Server*);
-  – any *Video Server*, configured and connected to the SecurOS network;
-  – any *Video Server*, disconnected from the SecurOS network;
-  – any *Operator Workstation* or *Operator Workstation Profile*; (connection to SecurOS is not indicated).

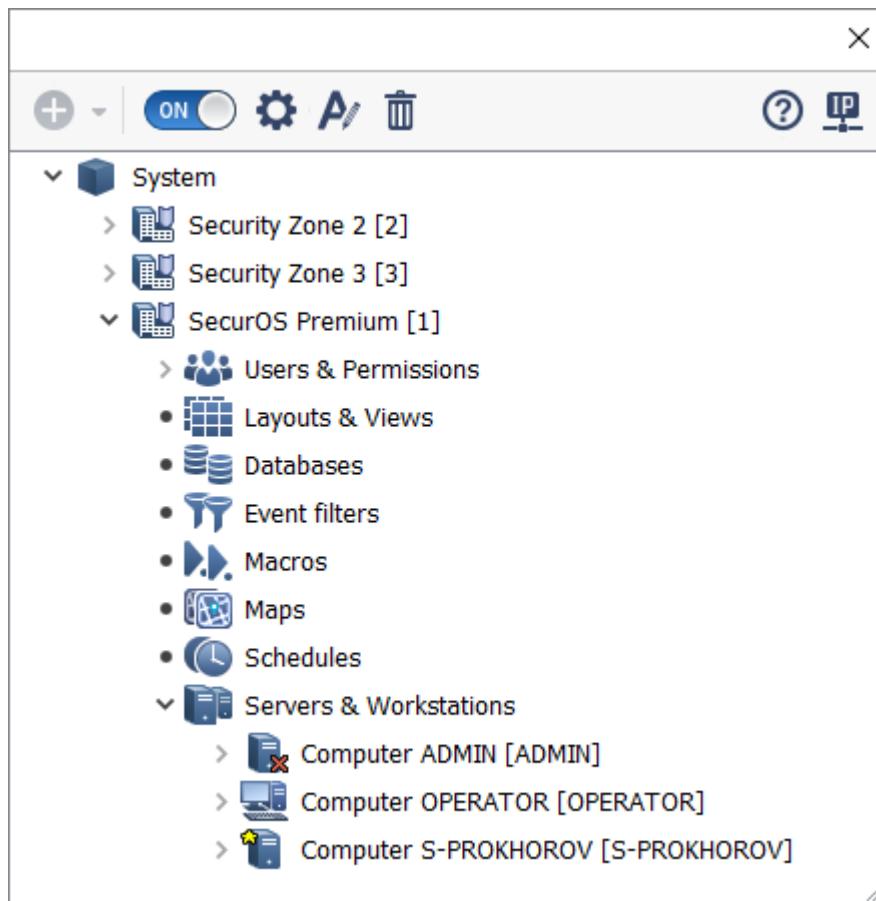


Figure 80. Computers and their states in the SecurOS Object Tree

Parent object – *Security Zone\Servers & Workstations* group.

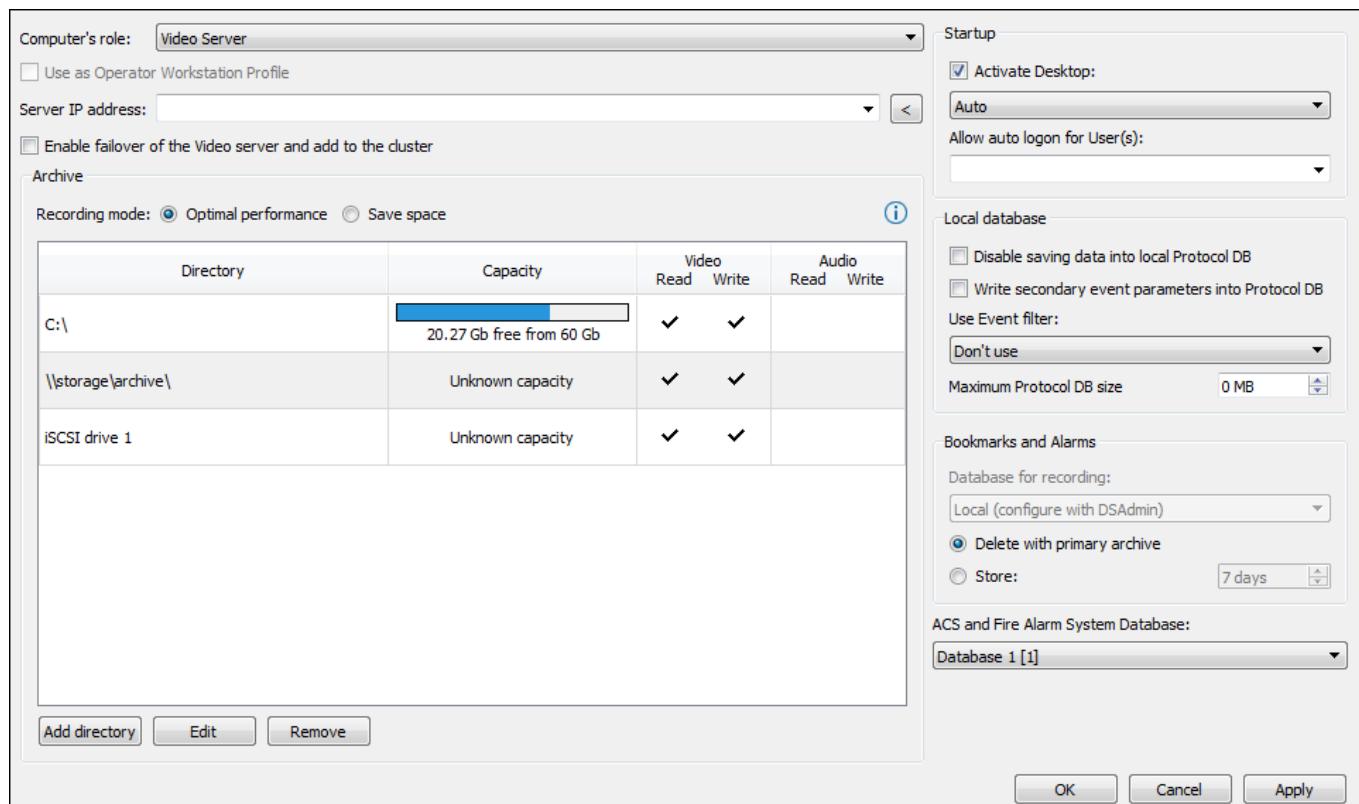


Figure 81. Computer object settings window

Table 12. Computer object settings

Parameter	Description
Computer's role	This value should correspond to the computer setup type, selected during software installation. It specified when object creating and can not be changed later. Possible values: <ul style="list-style-type: none"> • Operator Workstation – computer will operate as network client (even installed SecurOS has other setup type) or as <i>Operator Workstation Profile</i> (see Operator Workstation Profiles); • Video Server – computer will operate as a server.
Use as Operator Workstation Profile	Tick this checkbox to use object as <i>Operator Workstation Profile</i> (see Operator Workstation Profiles).
Server IP address	Specify IP address of the current computer within the TCP/IP network. You can choose from the list or use the [<>] button to determine the computer's IP address automatically. Warning! If the computers are located in different subnetworks, it will not be possible to get the IP address automatically. In this case, this parameter is mandatory, and the IP address must be entered manually.
Enable failover of the Video server and add to the cluster	Tick this checkbox to use object as cluster <i>Node</i> (see Failover cluster).
Archive Block (is enabled only for <i>Computer</i> object, role of which is <i>Video Server</i> , see the Archive section).	
Startup (settings that are applied automatically at system startup)	
Activate Desktop	Select this option to choose the default <i>Desktop</i> object from the drop-down list that will be shown on SecurOS startup on this computer. If the Auto value is set then the first desktop will be displayed (with minimal ID). If this option is not activated, no desktop will be displayed at startup.
Allow auto logon for User(s)	Option is available only for the <i>Video Servers</i> and <i>Operator Workstations</i> , that are not <i>Operator Workstation Profiles</i> . Select the name of the registered user or group to login automatically with (i. e. without entering Username and Password in the Authorization window). You will be able to select this option and set up its value only if you are logged in as superuser (see SecurOS Users). It is impossible to set up the field value to root. <hr/> <p>Note. For detailed information about setting order and rules of the procedure see the Auto login section.</p> <hr/> User group can be specified if an Active Directory / LDAP object is configured within the system. When specifying user group name use the @ prefix before its name, for example, @usergroup.

Parameter	Description
Local database	
Warning! If Computer's role is <i>Operator Workstation</i> the following parameters will be unavailable.	
Disable saving data into local Protocol DB	Select this checkbox to disable saving the local copy of the event log to the database. Since the event log is synchronized between computers and each computer saves its copy in the local database by default, you can turn on the event log saving on several machines without risk of loosing events.
Write secondary event parameters into Protocol DB	Select this checkbox to enable message parameters to be recorded into the PROTOCOL_PARAMS database. Warning! This option is used in conjunction with the ISS analytics modules only. In all other cases using this option can reduce system performance. So unless ISS analytics modules are being used, it is recommended to keep this box unchecked.
Use Event filter	Name of the filter, which will be used when saving events into the database. The list of values consists of names of all the Event filter objects, that are child objects to the current <i>Security Zone</i> . Optional parameter. If not set, all system events will be saved into the database. Otherwise, only the events allowed by the given filter will be saved. Warning! Using filters can reduce system performance.
Maximum Protocol DB size	Maximum database size before data will be updated in a ring mode (oldest deleted first). Default value is 0 (parameter is not used).
Bookmarks and Alarms	
Warning! If Computer's role is <i>Operator Workstation</i> the following parameters will be unavailable.	
Delete with primary archive	If this option is selected, then <i>Bookmarks</i> and <i>Alarms</i> will be deleted from database together with primary archive.
Store	If this option is selected, specify duration of storage for bookmarks and alarms in DB, days. Bookmark storage period starts from the beginning of the bookmark's validity; alarm storage period – from the time when alarm starts. Checking of expiration is performed every hour or when SecurOS starts. [1; 3660]. Default value is 7.
ACS and Fire Alarm System Database	Select from list the <i>Database</i> , created earlier for working with ACS Module (for details refer to the SecurOS ACS User Guide).

5.2.8.1 Archive

This block is designed to create a directories (information carriers) that allow to work with the SecurOS' archives. For each directory a list of available operations is specified.

Appearance of the block is represented in figure 82.

Archive					
Recording mode:		<input checked="" type="radio"/> Optimal performance		<input type="radio"/> Save space	
Directory	Capacity	Video	Read	Write	Audio
C:\	20.27 Gb free from 60 Gb		✓	✓	
\storage\archive\	Unknown capacity		✓	✓	
iSCSI drive 1	Unknown capacity		✓	✓	

Add directory **Edit** **Remove**

Figure 82. Archive Tab

The following operations are available in this block:

1. **Select archive recording mode** – select *Primary archive* recording mode;
2. **Add directory** – add a new directory to work with archives and specify a list of available operations;
3. **Edit directory** – change current list of available operations with archive for current directory;
4. **Remove directory** – remove current directory from the list of directories.

Select archive recording mode

One can use one of the following primary archive recording mode: with optimal performance or with disk space savings. To set archive recording mode select required option:

- **Optimal performance** – allows to increase archive write speed to disk due to decreasing archive file fragmentation. Efficiency of this mechanism depends of free disk space.

Note. Intelligent Security Systems recommends to use 10%. This value is also recommended by Microsoft Corporation for NTFS partitions. One can change this value in the **Computer** object settings.

This mode is recommended to use in case of long-time fragments recording (for example, for continuous archive recording). If archive is recorded in short-time fragments, then using this mode will shorten archive storage time and require more disk space.

- **Save space** – allow to use disk space more efficiently, but may decrease disk write speed. This mode is recommended to use in case of short-time fragments recording (for example, by commands

of intelligent Modules). For the details refer to [Video Recording Settings](#), description of MaxFrames parameter.

Add directory

The directory to work with archive can be represented by one of the following objects:

- local hard drive;
- removable storage;
- network drive;
- network folder.

To add a new directory do the following:

1. Click the **Add directory** button.
2. In the **Add new directory** window (see figure 83) set the following parameters:

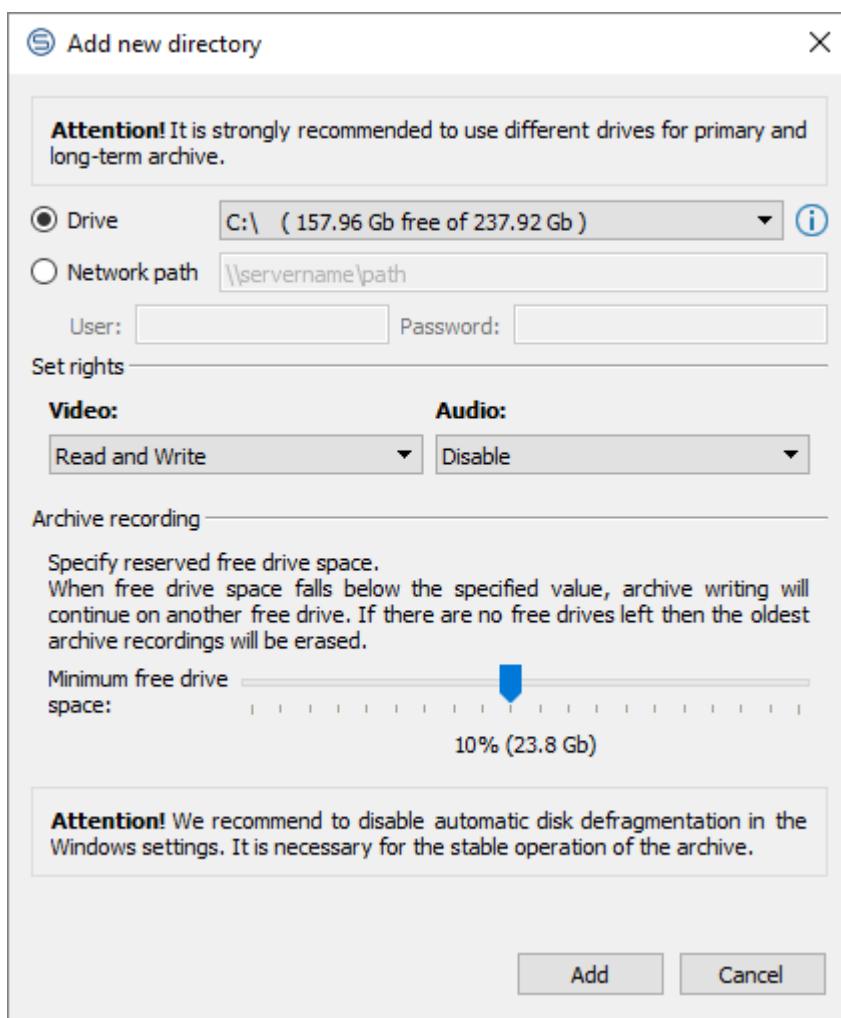


Figure 83. Add new directory window

- Select the option, that corresponds to the connected carrier:
 - **Drive** – use this option to connect a hard drive, removable storage or network drive;

Note. How to add local hard drives on the cluster's *Hosts* is described in the [Storing Video Archive on the Host's Local Drives](#).

- **Network path** – use this option to connect a network folder.

Warning! It is not recommended to use the same **Directory** to record *Primary* and *Long-term* archives (see [Archiver](#)).

If necessary, specify user name and password to get access to this network folder.

Note. If local computer is being configured the **Drive** list consists only of available drive letters. If a remote computer is being configured the list consists of all letters from A to Z. In this case select required letter.

- In the **Video** and **Audio** select from the list the operations, that can be performed with the archive on this directory:
 - **Disable** – the *Video Server* is not allowed to read and write an archive;
 - **Read Only** – the *Video Server* is allowed only to read an archive;
 - **Read and Write** – the *Video Server* is allowed both to read and write an archive.

Notes:

1. Operations with audio archives are disabled for network drives.
2. In the **Video** block the rights to perform operations with the video recorded with the accompanying sound are specified and in the **Audio** block rights only for audio files.

- In **Archive recording** check and, if necessary, modify the **Minimum free drive space** value.

Notes:

1. Parameter value is calculated and applied automatically when adding new directory.
2. It is recommended to allocate not less than 10% of full drive space. This value allows to write archive in **Optimal performance** mode as efficiently, as possible (see [Select archive recording mode](#)).

-
3. Click the **Add** button. Selected carrier will be added to the list of directories. Operations, enabled for this directory, will be marked with the symbol.

Warning! Scheduled defragmentation (for example, in Windows 7, **Control Panel → Administrative Tools, Defragment your hard drive** subsection) must be turned off for all hard drives selected to work with archive.

Edit directory

To change a list of operation applicable to a directory do the following:

1. Select required directory and click the **Edit** button.
2. In the **Edit existing directory** (see Figure 84) select new values for the **Video** and **Audio**.

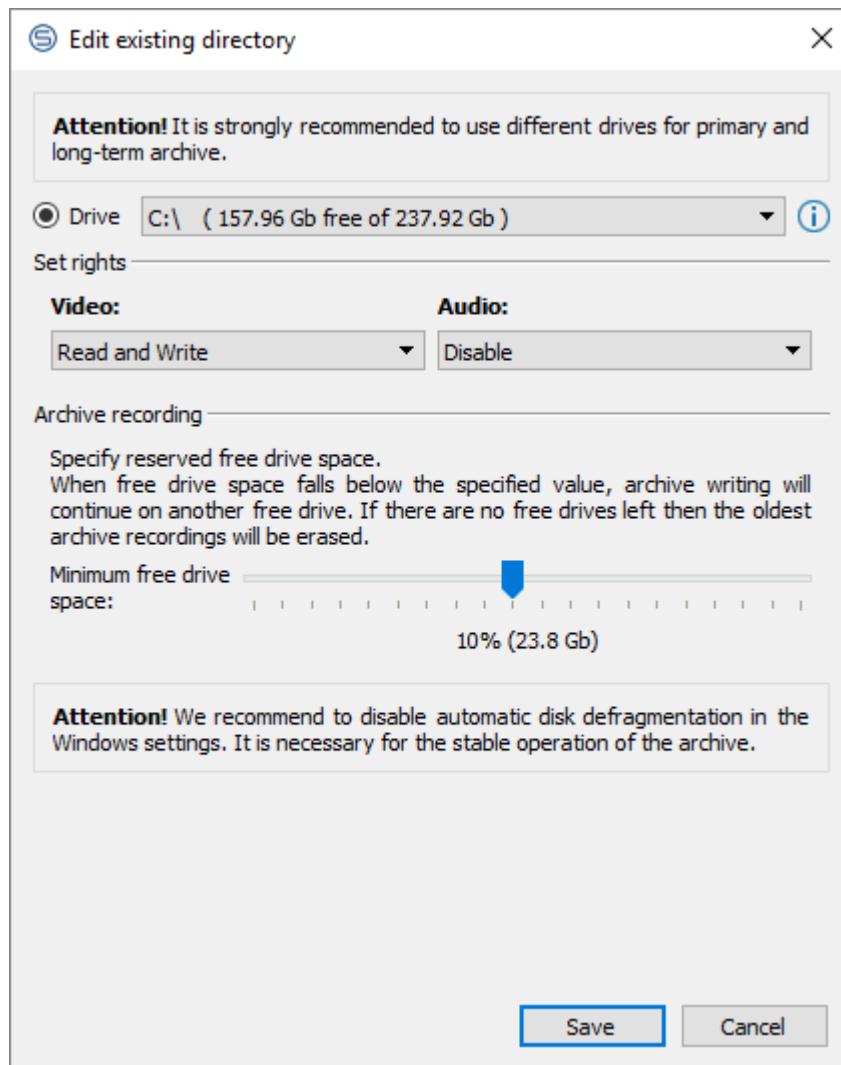


Figure 84. Edit existing directory window

3. Click the **Save** button.

Remove directory

To remove a directory from the list select connected one in the list, then click the **Remove** button. To confirm removing click the **Yes** button in the informational panel (see Figure 85).

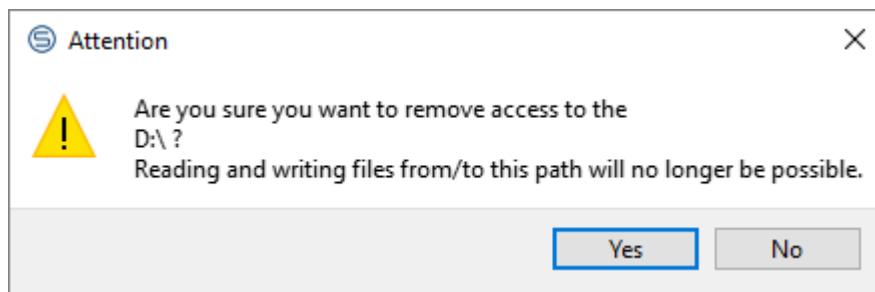


Figure 85. Confirm removing panel

5.2.8.2 Auto login

Auto login feature is available both for SecurOS *Users* and Windows/Linux users registered in the Windows Active Directory domain. If the credentials of these users match, the preference is given to the SecurOS users.

Allow auto logon for User(s) parameters can take the following values:

- Name of any user, registered in the current *Security Zone* object within the SecurOS network (**Object tree → Users & Permissions group → Department → User Account**), excluding the superuser (see [SecurOS Users](#)).
- Name of any Active Directory Group. For the given value, auto login may be performed for any member of the selected Group.
- Name of any Active Directory User. For the given value, auto login may be performed for the specified user only.

Warning! Active Directory domain of the Windows network can be used for the authentication only if there is an *Active Directory Storage* object registered in SecurOS and it is selected as a provider for the *User rights* object (see [Active Directory / LDAP](#)).

- "Not set" (default value). For the given value, auto login may be performed for any Active Directory User or member of any Active Directory Group, granted with the access rights defined in the *User rights* object.

5.2.9 Event Filter

This object is designed to set the rules used to filter events that must be either displayed in the [Event Viewer](#) window or saved into the database.

Parent object – *Security Zone\Event filters* group.

Type	Id	Name	Event	Mode
1 Camera	1	Camera 1	Alarm [A]	Allow
2 Camera	2	Camera 2	Alarm End; Defocused [A]; Detached [A]; Record start; Rec...	Allow
3 Computer	S-PROKHOROV	Computer S-PROKHOROV	alarm only	Allow
4 User account	1.1	Operator 1	information only	Allow
5 Microphone	1	Microphone 1	Record start; Record stop	Allow

Rules list

Add rule Remove rule Remove All Test filter Up Down OK Cancel Apply

Figure 86. Event Filter object settings window

Table 13. Event Filter object settings

Parameter	Description
Rules list	
Type	Type of the system object (that is the event source). Select the All option to address all possible objects.
Id	ID of the system object (that is the event source). Leave the list empty to address all the objects of selected type.
Name	<i>Information field:</i> name of the selected source object (the Id and Name parameters correspond to each other – if one is selected then the other is filled automatically). Leave the list empty to address all the objects of selected type.
Event	<p>Event to process. List of values depends on the object type.</p> <hr/> <p>Notes: Besides an individual or all events of an object, one of the following predefined event groups can be selected as well:</p> <ul style="list-style-type: none"> 1. Alarm only. 2. Information only. 3. Alarm and information.
Mode	<p>Rule result. Possible values:</p> <ul style="list-style-type: none"> • Forbid – event will be discarded (not displayed in the Event Viewer window or saved into the database). • Allow – event will be allowed (displayed in the Event Viewer window or saved into the database).
Buttons	
Add rule	Click to add a new rule to the list.
Remove rule	Click to remove selected rule from the list.
Remove all	Click to remove all rules from the list.
Test filter	Click to display Events to test block that allows to check the rule. Rule checking procedure is described below.
Up	Button is used to sort rules manually. Click to move the rule one position up.

Parameter	Description
Down	Button is used to sort rules manually. Click to move the rule one position down.

Rules list

Type	Id	Name	Event	Mode
1 Camera	1	Camera 1	<input type="checkbox"/> No danger for pedestrian	Allow
2 Camera	2	Camera 2	<input checked="" type="checkbox"/> Position altered	Allow
3 Computer	S-PROKHOROV	Computer S-PROKHOROV	<input type="checkbox"/> Position unchanged	Allow
4 User account	1.1	Operator 1	<input type="checkbox"/> Record error	Allow
5 Microphone	1	Microphone 1	<input checked="" type="checkbox"/> Record start	Allow
			<input checked="" type="checkbox"/> Record stop	Allow
			<input type="checkbox"/> Unblinding	
			<input type="checkbox"/> Video analytics event	

Add rule Remove rule Remove All Test filter Up Down OK Cancel Apply

Figure 87. Choosing multiple events for the object

To check the rule (i.e. to make sure what kind of action for the event this rule results in) do the following:

1. In the object settings block (see Figure 87) click the **Test filter** button.
2. System will display **Events to test** section (see fig. 88).

Rules list

Type	Id	Name	Event	Mode
1 Camera	1	Camera 1	Alarm [A]	Allow
2 Camera	2	Camera 2	Alarm End; Defocused [A]; Detached [A]; Record start; Rec...	Allow
3 Computer	S-PROKHOROV	Computer S-PROKHOROV	alarm only	Allow
4 User account	1.1	Operator 1	information only	Allow
5 Microphone	1	Microphone 1	Record start; Record stop	Allow

Add rule Remove rule Remove All Hide test filter Up Down

Events to test

Type	Id	Name	Event	Rule
1 Zone	1.0	Main_1	Alarm End	No filter rules, event is forbidden
2 Camera	1	Camera 1	Alarm [A]	Event is allowed by rule 1.

Add event Remove event Remove All Run test OK Cancel Apply

Figure 88. Events to test section

3. In the **Events to test** section click the **Add event** button. Set the event needed to be tested.

Note. Rule parameters of the **Events to test** section are the same as described above in **Rule list**.

4. Click the **Run test** button. System will execute test and display result in the **Rule** field:

- **No filter rules** – list of rules contains no rules for the defined event.
- **Event is allowed by rule N** – list of rules contains rule N that allows defined event.
- **Event is forbidden by rule N** – list of rules contains rule N that forbids defined event.

Note. "N" stands for the sequence number of the rule in the rule list.

5. To clear Events from test list, click the **Remove event** or the **Remove all** button. To hide the **Events to test** section click the **Hide test filter** button.

6. To save / discard changes and leave the administration mode click the **OK/Cancel** button.

Filtering algorithm is as follows:

- Rules are applied consecutively in order of appearance in the Rules list.
- Only the first corresponded rule is implemented for the event.
- If there is no one explicit rule that allows event then event will be discarded.

5.2.10 SNMP agent

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

This object is designed both to send events generated by the system's cameras and to transmit cameras' states to the specified computers as SNMP traps. Traps for the following events are transmitted automatically as soon as they arise in the system:

- Camera: changed state;
- Camera: focused;
- Camera: defocused;
- Camera: unblinding;
- Camera: blinding;
- Camera: attached;
- Camera: detached.

When changing cameras' states the current states are transmitted. Received traps are processed with the help of a SNMP Manager.

To get *Cameras* table and their states load into SNMP Manager the SecurOS MIB-file *ISS-SECUROS-MIB*, that is located in *<SecurOS_root_directory>\MIB*.

This object can only be used if the **Management and Monitoring Tools** component is installed on the computer (see [Setting up Windows Managing and Monitoring Tools](#) section).

Parent object – *Computer\Notifications* group.

Object has no settings to configure.

Note. Only one *SNMP agent* object is allowed in the object tree of the local computer. If the object is already created then the **Create → SNMP agent** command is unavailable.

5.2.10.1 Setting up Windows Management and Monitoring Tools

To set up the SNMP traps sending procedure do the following:

1. Install the **Simple Network Management Protocol** service:

- run **Programs and features** (**Control Panel**→**Programs and features**);
- click the **Turn Windows features on or off** tab and select **Simple Network Management Protocol (SNMP)** component including children;
- restart Windows.

2. Run the **Services** tool (**Control Panel**→**Administrative Tools**→**Services**) and open the **SNMP service (SNMP Service)** Properties.

3. Click the **General** tab and select **Startup type: Automatic**.

4. Click the **Traps** tab (see figure 89) and specify **Community name** and **Trap destinations** parameters.

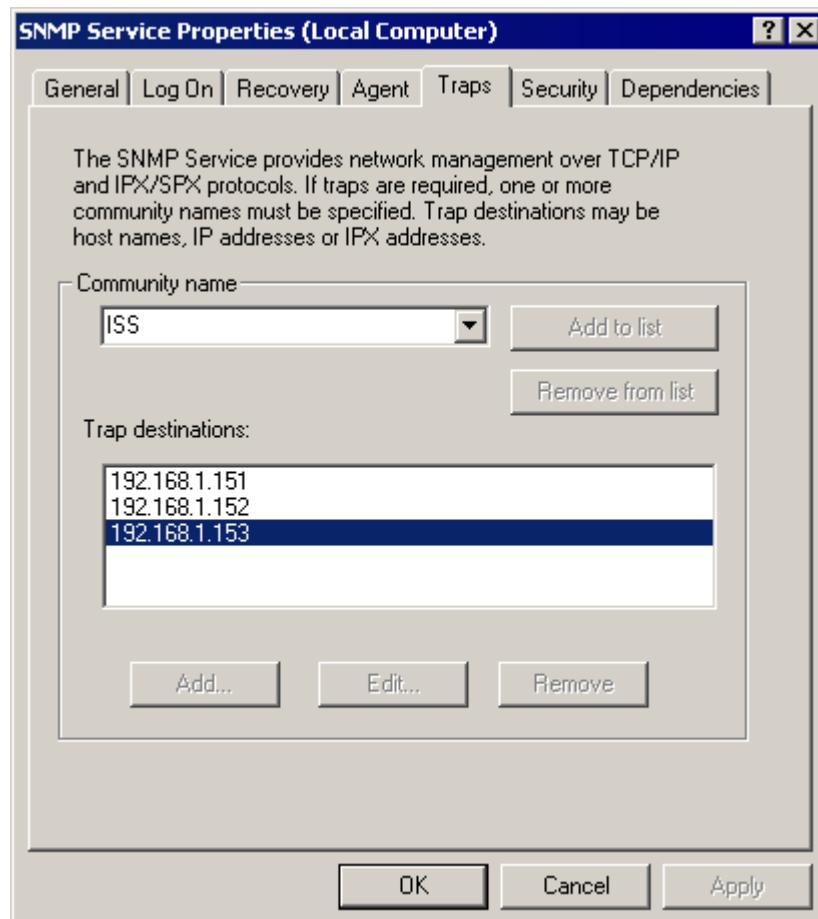


Figure 89. Traps tab of the SNMP Service settings window

5. Click the **Security** tab (see Figure 90).

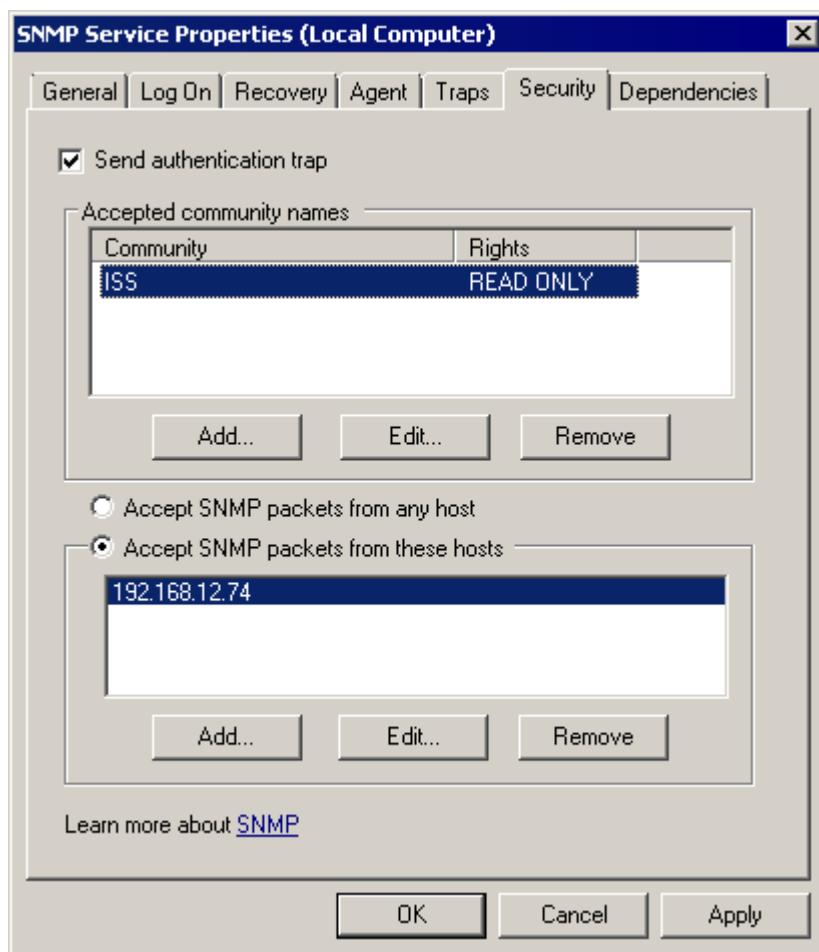


Figure 90. Security tab of the SNMP Service settings window

In the **Accepted community names** add SNMP community, which can interact with the local computer. Specify the following parameters of the community that is being added:

- **Community** – specify community name acceptable within the SecurOS network, for example, ISS;

Note. In general, one can use arbitrary community name, including public default value.

- **Rights** – assign computers of the added community any rights, including ability to read MIB file from the local computer, for example, READ ONLY.

If the **Accept SNMP packets from these hosts** is selected, specify IP addresses of the computers within the SecurOS network, where SNMP manager is installed.

6. Apply new settings.
7. Create the **SNMP agent** object in the SecurOS Object Tree.

After the steps described above are performed, SecurOS will automatically send traps to the specified IP addresses in real-time.

5.2.11 External application

The object is used to automatically start an external application from SecurOS. Application is started when SecurOS *Video Server* starts, and also after an object is created or enabled on the *Video Server*.

Parent object – *Computer\Integration and Automation* group.

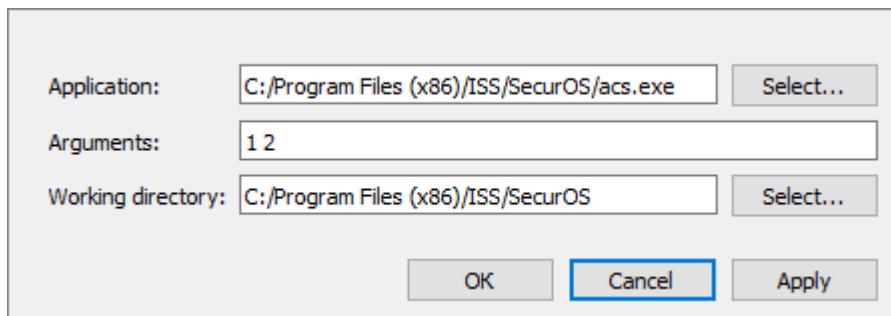


Figure 91. External Application object settings window

Table 14. External Application object settings

Parameter	Description
Application	Specify the name (executable file name) of the application or the name of the application and the full path to it. If only application name is specified, then start of an application is managed by OS system settings on given computer, for example, defined in the Path system variable. You can specify application name both manually and using the Select button. String value can contain any characters, allowed by Windows or Linux Operating Systems.
Arguments	Specify the parameters that must be passed to the external application when it starts. If there are several parameters, they must be separated by a space in the list, for example, 1 2 3. Optional parameter. If not set the application will be started without parameters.
Working directory	Specify application working directory or use the file manager to browse it. Optional parameter. If not set, the SecurOS root folder will be set as working directory.

External application launched from the SecurOS, has the following properties:

- External application that involves GUI, is started without loading this GUI.
- External application itself and all its children processes are terminated when deleting/disabling an *External application* object from the *Object Tree*.
- When closing an external application (due to failure or manually by user), it restarts automatically.

At startup/startup failure/close of the external application SecurOS generates appropriate Events (see [SecurOS Programming Guide](#)).

5.2.12 Databases Replicator

Object allows automatically copy content of the SecurOS Auto database into the common database. Such common database can be used for searching and viewing all the events of the SecurOS Auto (see [SecurOS Auto User Guide](#)).

Copying of the selected databases will start after object creating and configuring. Entries will be copied, starting with the oldest ones. After all entries are copied, replication is started in real time mode. All subsequent changes of the source database will also be taken into account in the replicated database.

Parent object – **Computer**.

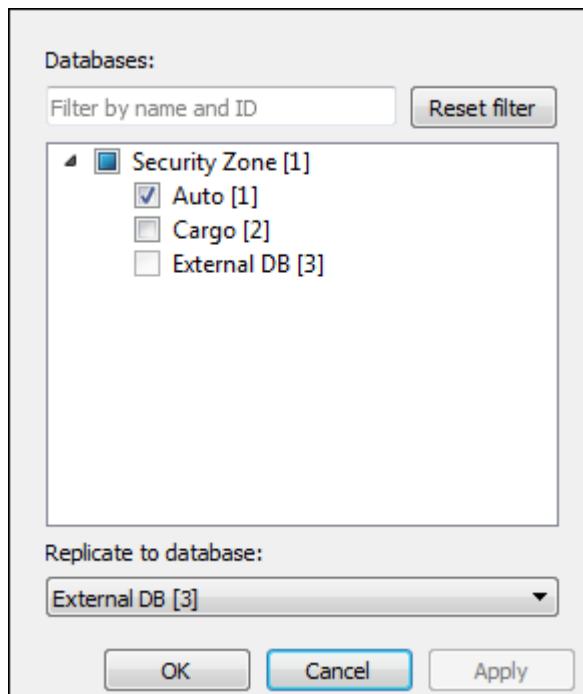


Figure 92. Databases Replicator object settings window

Table 15. Databases Replicator object settings

Parameter	Description
Databases	Select one or several source SecurOS Auto databases to replicate.
Filter	To search object by name (part of its name) or by ID, type required characters in the field; only those objects that meet the search condition will automatically be displayed in the tree. To clear the field click the Reset filter button.
Replicate to database	Select target database where source databases will be copied to.

6 Interface Subsystem

The Interface subsystem, contains objects responsible for visual representation of the system objects and is actually used by operators working with the system.

6.1 Object Reference

The interface subsystem includes the following objects:

- [Desktop](#).
- [Map](#).
- [Map Window](#).
- [Event Viewer](#).
- [External Window](#).
- [HTML Form](#).
- [HTML5 FrontEnd](#).

6.1.1 Desktop

This is a base user interface object that acts as a container to other user interface objects. It is used for placement of one or more user interface components.

Parent object – *Computer\Desktops* group.

Warning! All visual components of the user interface are displayed only by the means of SecurOS *Desktops*.

Example. There are two rooms in a secured area. There is a PTZ dome camera and a microphone in the first room and two cameras in the second room. The system administrator can configure two Desktop objects. On the first *Desktop* there could be a *Media Client* to control PTZ, view video and listen the sound. On the second *Desktop* there could be a second *Media Client* to watch cameras from the second room, and a *Map Window* displaying the map of the whole territory to provide visual access to all the security devices and to control their states. If several displays connected to the operator's computer one can create the one *Desktop* instead of several ones and place all required interface object on these available displays.

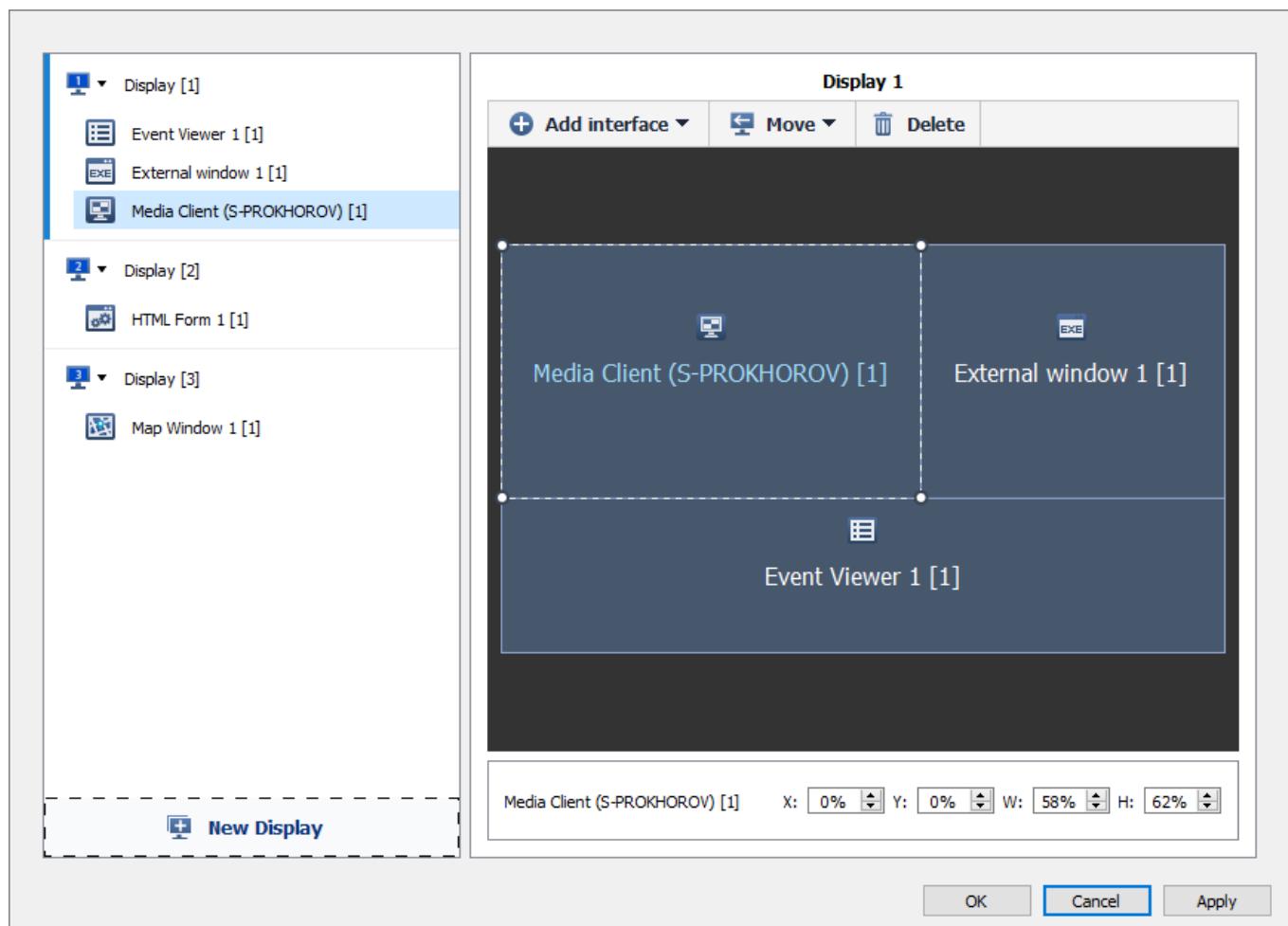


Figure 93. Desktop object settings window

Table 16. Desktop object settings

Parameter	Description
Object Tree	<p>Located on the left part of the window. Object tree displays all interface objects children to the <i>Desktop</i> that is being configured. If operator's computer has several displays, these objects will be grouped relative to the Display on which they are located. States of the objects in the object tree are displayed similar to the object states in the SecurOS <i>Object Tree</i> (see Disabling/Enabling Objects). Below the tree the New Display field is located, that is used to create a new display and place an object window on it.</p> <p>Note. Context menu (see Desktop Setup Operations) is available for each tree object.</p>
Visual settings area	Located on the right part of the window. Is intended for setting operator windows' sizes and positions in graphic mode and previewing settings result. Contains buttons to control interface object windows.
Information about configured window block	Located below the Visual settings area . In this block the name of the selected window, relative coordinates of its position and sizes are displayed.

6.1.1.1 Desktop Setup Operations

To place windows of the SecurOS or the SecurOS intelligent Modules user interface on the *Desktop* it is necessary to set relative coordinates of their position and sizes of these windows. *Desktop* object settings window allows to set these parameters and visually analyze the result (see Figure 94).

Note. These parameters can also may be specified in the each SecurOS object settings.

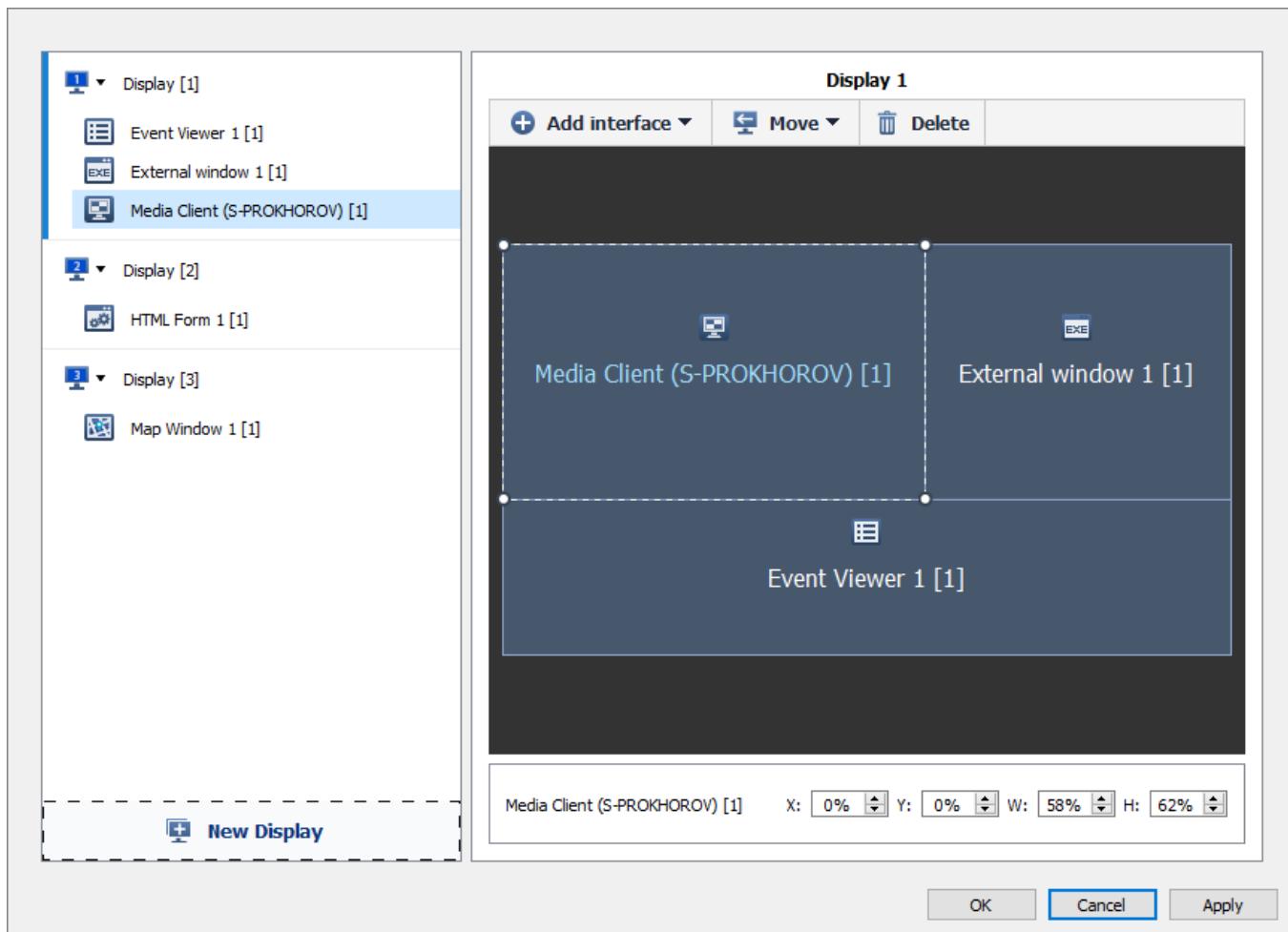


Figure 94. Desktop object settings window

You can perform the following operations in the settings window:

- **Adding new object to display.**
- **Changing object window position and size.**
- **Creating new display.**
- **Moving object window to selected display.**
- **Moving all object from one display to another.**
- **Deleting display.**
- **Other operations with object.**

Details of operations with the multi-window objects (for example, SecurOS Auto operator GUI) are described in the [Features of working with multi-window objects](#).

Adding new object to display

1. In the **Desktop object tree** select the *Display* to which a new interface object must be added. When configuring the *Desktop* for the first time an empty display is automatically created in the object tree.
2. In the **Visual settings area** click the **Add interface** button.
3. Select required SecurOS interface object in the drop-down list. System will display the **Parameters of created object** window (see Figure 95).

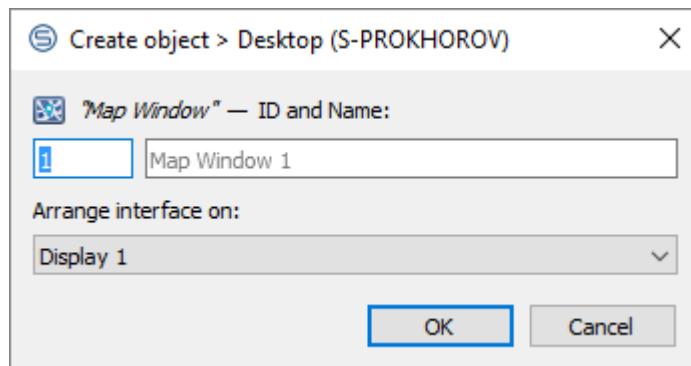


Figure 95. Parameters of created object

4. Specify required parameters and click **OK**. An object will be created in the SecurOS *Object Tree* and added to the selected display.

Note. This operation can also may be performed via *Display* object's context menu in the **Desktop object tree**.

Changing object window position and size

1. In the **Desktop object tree** select an object which window have to be configured. In the **Visual settings area** window of this object will be highlighted with a dotted line.
2. To change window's position drag-and-drop it to the required position.
3. To change window's size place mouse pointer over window vertex or any side then stretch the window horizontally or vertically.

Creating new display

A new display may be created in the following ways:

- Via **New Display** button in the **Desktop object tree**:
 1. Click the **New Display** button in the **Desktop object tree**. A new empty display will be created in the tree.
 2. Perform the **Adding new object to display** operation, othrwise created empty display will be removed from the **Desktop object tree**.
- By drag-and-drop from an existing display:
 1. In the **Desktop object tree** select an object which window must be placed on a new display. In the **Visual settings area** window of this object will be highlighted with a dotted line.
 2. Drag-and-drop object's window from the **Desktop object tree** or from the **Visual settings area** to the **New Display** field.
- Selected window can also be moved using the **Move** button located in the **Desktop visual settings area**:
 1. In the **Desktop object tree** select an object which window must be placed on a new display. In the **Visual settings area** window of this object will be highlighted with a dotted line.
 2. In the **Visual settings area** click the **Move** button.
 3. In the drop-down list select the **New Display**.
- Via **Move** command of the object context menu:

1. In the **Desktop object tree** select an object which window must be placed on a new display.
2. In the context menu select the **Move** command.
3. In the drop-down list select the **New Display**.

Warning! Number of displays connected to the operator's computer is not detected automatically and must be controlled by the administrator.

Moving object window to selected display

1. In the **Desktop object tree** select an object which window must be placed on another display. In the **Visual settings area** window of this object will be highlighted with a dotted line.
2. Drag-and-drop window from the **Desktop object tree** or from the **Visual settings area** to the required display from the list.

Note. Selected window can also be moved with the help of the methods described above, see [Creating new display](#).

Moving all object from one display to another

1. In the **Desktop object tree** click the  button to the left of the display all windows of which must be moved to another display.
2. In the drop-down list select required display.

Deleting display

To delete display from the **Desktop object tree** it is enough to move all object windows located on it to another display. Display will be automatically deleted when selecting another display in the **Desktop object tree** or after applying object settings if there is only one display in the tree.

Other operations with object

Other operations are performed via object context menu. Context menu is available both in the **Desktop object tree** and **Visual settings area**. The following operations are available in the context menu:

- **Moving object** – see [Moving object window to selected display](#);
- **Disabling object** – allows temporary disable an object (for the details see [Working with Objects](#)). In the **Desktop object tree** disabled object will be marked in the same way as in the SecurOS *Object Tree* (see Figure 96);

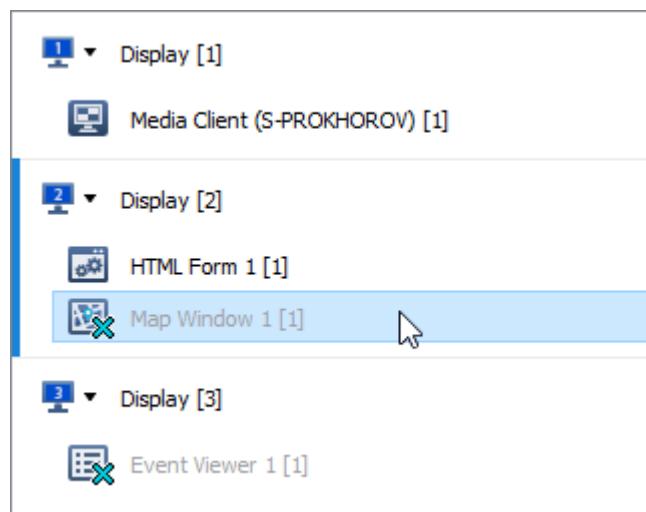


Figure 96. Disabled Object

- **Rename object** – allows rename an object (for the details see [Working with Objects](#));
- **Deleting object** – allows delete an object from the SecurOS *Object Tree* (for the details see [Working with Objects](#)).

Note. To move and delete objects one can also use the appropriate buttons located in the **Visual settings area**.

Features of working with multi-window objects

Besides pointed above operations, when working with multi-window interface objects one can control window displaying mode on the operator monitor directly from the *Desktop* object settings window. This operation is similar to the enabling/disabling window displaying mode in the object own settings (for example, *LPR: GUI*, see [SecurOS Auto User Guide](#)). When working with windows of such objects in the **Information about configured window block** select checkbox to the right of the objects name to display window (see Figure 97) or deselect checkbox to hide the window.

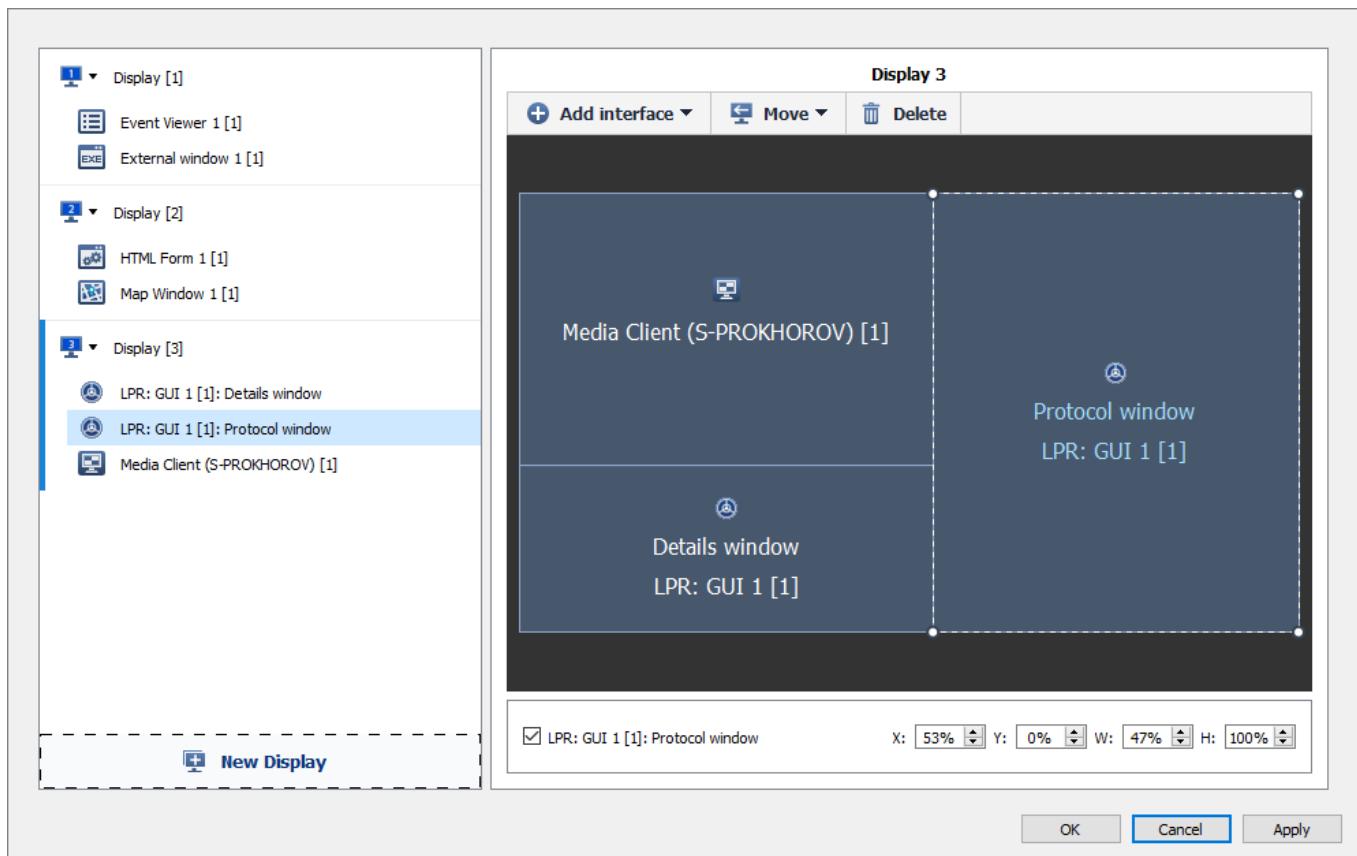


Figure 97. Window displaying mode control checkbox

When working with the SecurOS POS Module windows (see [SecurOS POS User Guide](#)) the **Information panel** window will always be displayed on the same display where the **Events log** window is placed, independently of its position in the *Desktop* object settings window.

6.1.2 Map

This object represents a multi-layered graphical map of the territory under surveillance.

Parent object – *Security Zone\Maps* group.

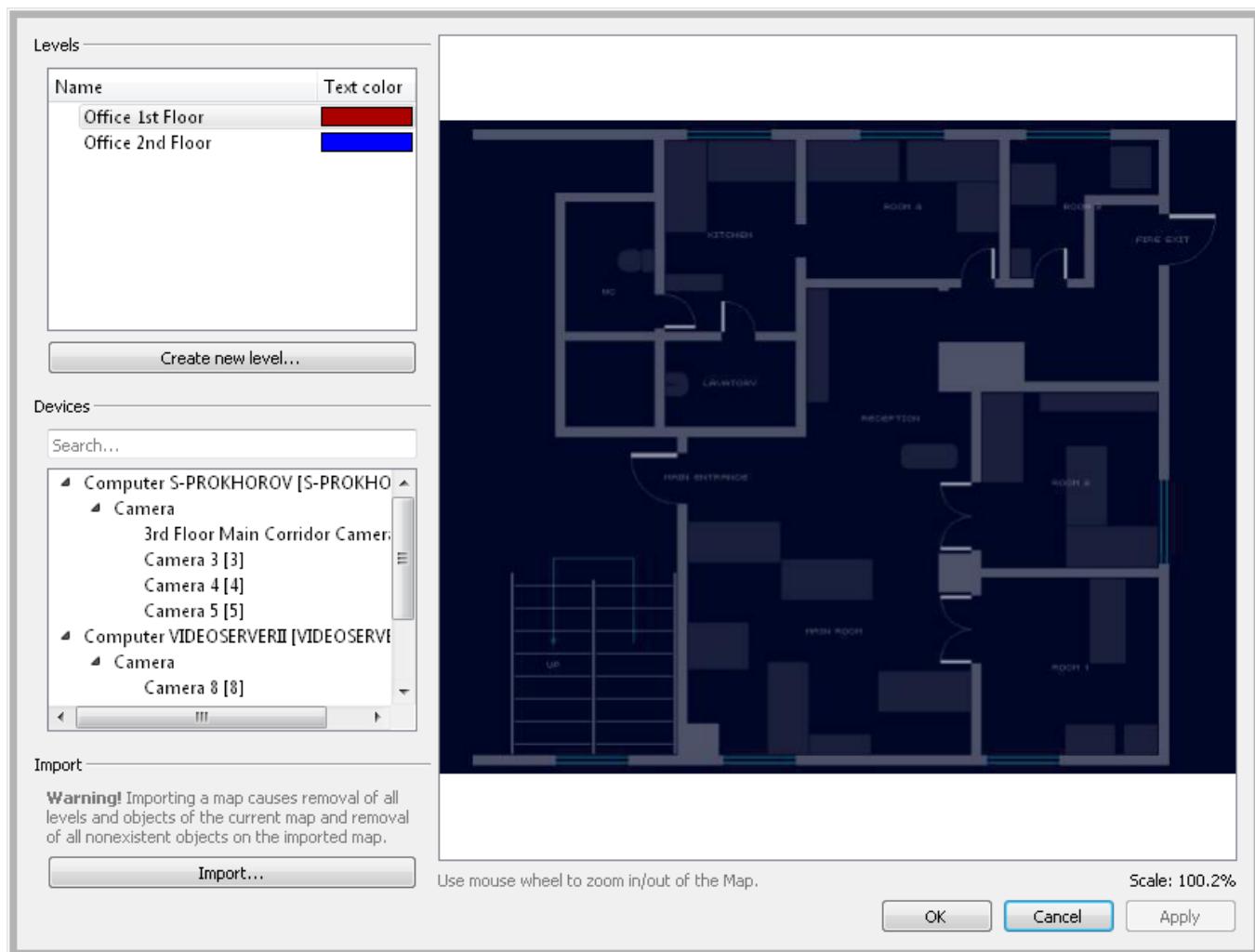


Figure 98. Map object settings window

Table 17. Map object settings

Parameter	Description
Levels	
Name	Map level tree and name.
Text color	Color of the object caption on the image of the map level.
Devices	
Search	Is used to search for devices (see Working with Map Objects).
Device tree	This box displays an SecurOS <i>Object tree</i> , that contains all system devices, that can be placed on the map.
Map image	
Map display area	Image of the current map level.
Scale	Current scale of the map level. To scale up/down click on the image, then use mouse wheel.
Buttons	

Create new level	Click the button to create a new map level (see Working with Map Layers).
Import	Click the button to load a <i>Map</i> from the file of the old Map v2 format (.map). Warning! Importing a map causes removal of all levels and objects of the current map and removal of all nonexistent objects on the imported map.

6.1.2.1 Maps Working Principles

To make monitoring a *Security Zone* more convenient it is recommended to use a *Map* – an image of the protected territory and security devices located on it. A *Map* can include a number of levels, that correspond for example, to parts of the protected territory, levels of the controlled building or separate rooms on each level. Each **Level** of the Map is represented by a map image of the protected area with icons of the security equipment, such as cameras, alarm sensors etc., placed on it in accordance with the area's physical locations.

To enable use of *Maps* in SecurOS one should perform the following operations:

1. Create a [Map](#) object;
2. Create a [Map Window](#) object on the *Operator / Administrator Workstation*;
3. Assign operator access rights to this object.

Note. The same *Map* object can be loaded into the *Map Window* on any number of *Operator Workstations*.

The operator can use maps to monitor the entire territory, and also use the icons allocated on a map for fast control of the corresponding object. If an intrusion alarm has been detected, an operator can immediately see the physical location of the target area, switch to the video cameras that are located close to this area by double-clicking on icons on map, switch the lights on within that area, lock certain doors, etc...

6.1.2.2 Drawing Map Layers

Use of map layers is convenient for large territory separation into several independent parts. Map layers are images in BMP, JPEG, JPG or PNG format. To draw your map images from scratch, one can use any graphical drawing software that allows you to save the images in the formats listed above. You can also export the images directly from CAD software where you or the owner of the building develops source documentation on the building or territory, or you can scan the previously printed plans of your territory.

The resulting image or images can have any colors and style, but you should consider the following:

1. All plans of your territory should be done in the same graphical style for better visual perception.
2. Keep the image dimensions in pixels comparable to dimensions of the target maps on the screen of the operator workstation to avoid redundant scrolling.
3. Colors should not distract operator from objects placed on map. Do not use gaudy colors; avoid using red and orange colors. The more neutral the background is, the better.

4. Provide descriptive captions for all territories. Text should be clearly visible and readable.
5. Give images meaningful names (i.e. map_floor1.png, map_floor2.png, map_room123.png etc.).

Warning! It is not recommended to use map image files greater than 4 MB.

6.1.2.3 Working with Map Layers

To add a new map layer:

1. Click the **Create new level** button in the object settings window. The level settings window will appear (see Figure 99).

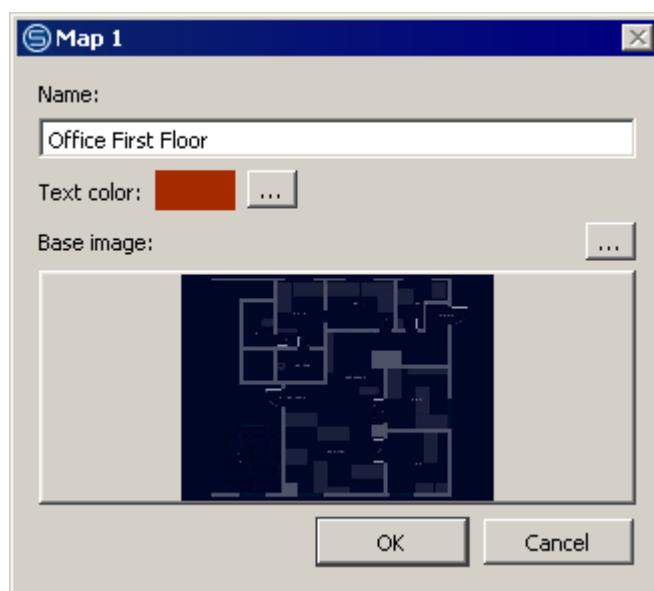


Figure 99. Levels settings window

2. Type in a new layer name in the **Name** field.
3. Click the button on the right of the **Text color** field and select a color of the object caption for the current map level in the standard window.
4. To select a level image click the button on the right of the **Base image** field, then use the file manager to select an image, that will be used as the main image for the new level (BMP, PNG, JPG and JPEG file formats are supported).
5. Click the **OK** button.

Note. The created level is placed into the **Name** list (*Level Tree*) in alphabetical order.

To switch between levels one can use a link, represented with a special icon (see Figure 100).



Figure 100. Map object link icon

To create a level link:

1. In the Level Tree select a level, where the link to the other level must be placed. The image of this level will be displayed in the **Map display area** of the *Map*.
2. Select a level that must be referenced, then click it in the **Name** list (*Level Tree*) and, holding the mouse button, move the mouse cursor to the first level image.
3. Release the mouse button.

Once created, a link icon will appear on the map (see figure 100). The link icon can be moved across the map by clicking the left mouse button on the icon, dragging the mouse pointer to the new location, and then releasing the left mouse button.

Now test this link by double-clicking on it: map will switch to the target layer. For easier navigation, we recommend to create another link on the target layer that points back to the source one. Thus, it will be possible to switch between layers in both directions smoothly.

A link icon must be placed on a map level image in accordance to the structure of the protected area. For example, if each map level represents a separate floor of the protected building, a link icon is reasonable to be placed on the stairs to the next floors, etc.

Note. A blinking link icon indicates an alarm has been detected on the referenced level.

Additional operations on a *Map*'s level are performed with the help of a context menu, opened by right-clicking on the level name in the **Name** list (*Level Tree*). The context menu contains the following options (see Figure 101):

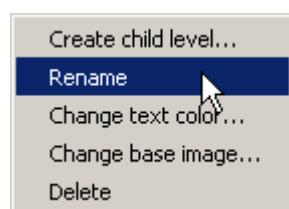


Figure 101. Map level context menu

- **Create child level** – create a child level to the current level in the **Name** list (*Level Tree*);
- **Rename** – rename current level;
- **Change text color** – change object caption color;
- **Change base image** – change level image;

- **Delete** – delete current level.

A child level can also be created by drag-and-drop. Click a level, that is supposed to be a child, then drag it on the level, that is supposed to be a parent (see Figure 102).

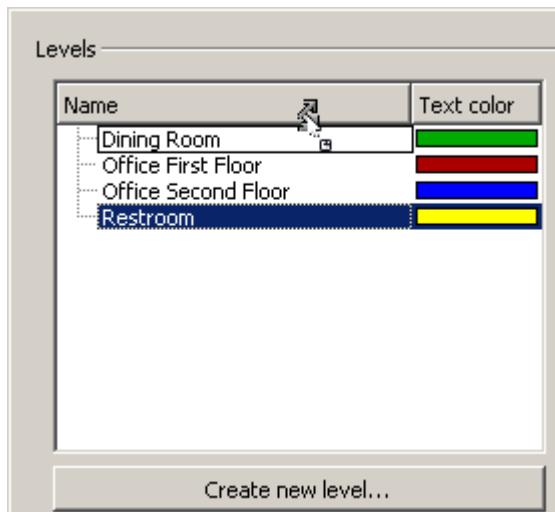


Figure 102. Creating child level by drag-and-drop

6.1.2.4 Working with Objects

One can perform the following operations with an objects on the *Map*:

- [Searching Object in the Device Tree](#).
- [Placing Object on the Map Layer](#).
- [Changing Object Position on the Map Layer](#).
- [Aligning camera FOV](#).
- [Moving Object Caption](#).
- [Changing Object Caption Appearance](#).
- [Removing Object from the Map Layer](#).

To find an object in the *Device Tree*, enter any character (or set of characters), that are part of the object name or object ID into the **Search** text box. All devices, whose names comply with the specified set of characters, will be displayed in the *Device Tree*. Later, one can place the found object on the *Map*.

To place an object on the *Map* level do the following:

1. In the **Levels** block select a level, to which an object must be placed. Level base image will be displayed on the right of the settings window.
2. In the **Devices** block select an object that must be placed on the selected level.
3. Click selected object and, holding mouse button pressed, move an object from the list to the required position on the level base image.

To change current object position on the *Map* layer do the following:

1. In the **Levels** block select a level, on which an object must be relocated.
2. Click object's icon and, holding mouse button pressed, move an object to the new position on the level.

To rotate Camera icon to align it with actual camera's FOV do the following:

1. Place mouse pointer over the icon of the *Camera* to be rotated. Double-sided arrow will be displayed on the right of the icon, see Figure 103.

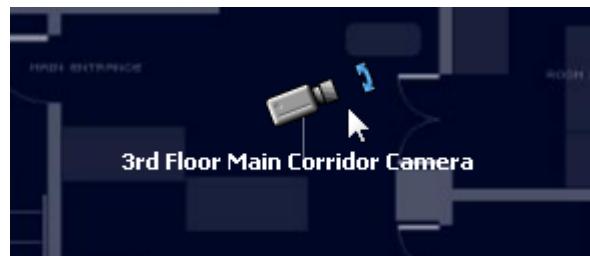


Figure 103. Rotating Camera Icon on Map

2. Place mouse pointer over this arrow and click the mouse button. Holding mouse button pressed rotate camera icon about its axis to align icon in accordance with actual camera FOV.

To move an object caption do the following:

1. Place mouse pointer over the object caption and press left mouse button. Pointer will be changed as it represented in Figure 104.



Figure 104. Moving Object Caption

2. Holding mouse button pressed move caption string in any place around the icon.

To change object caption appearance do the following:

1. Click the **A...C** icon on the right of the caption (see Figure 105).



Figure 105. Changing Object Caption

2. Object caption will be displayed on the *Map* in the short form (see Figure 106).

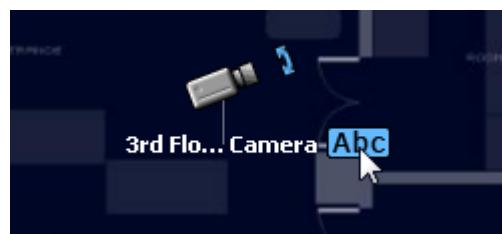


Figure 106. Short Object Caption

To display full object caption click the **Abc** icon on the right of the caption (see Figure 106).

To delete an object on the Map level do the following:

1. In the **Levels** block select a level, from which an object must be deleted.
2. Click an object and press the **Delete** button. Also one can use **Remove** context menu command to delete an object.

6.1.3 Map Window

This object provides a GUI to display a **Map**.

Parent object – **Desktop**.

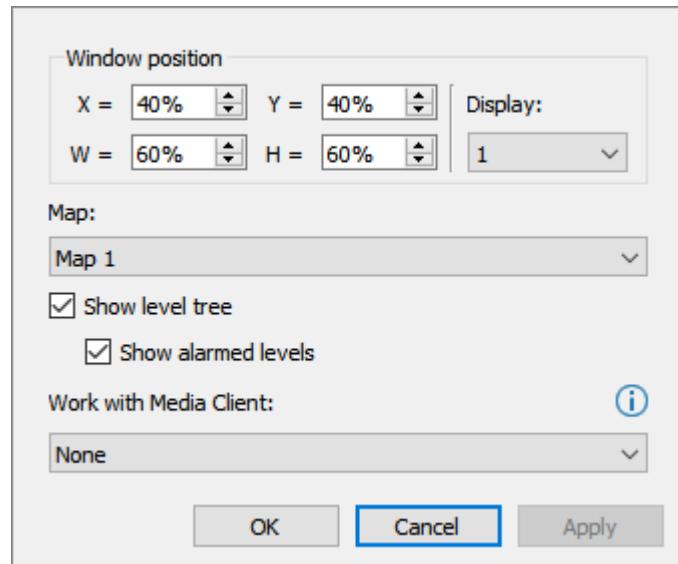


Figure 107. Map Window object settings window

Table 18. Map Window object settings

Parameter	Description
X, Y, W, H	Specify the object window's top left corner coordinates (X, Y) as well as its width and height (W, H), as percentages of the display's horizontal and vertical size.
Display	Choose the ID of the physical display this object belongs to.
Map	Select one of the previously created maps (see Map), that should be displayed in this map window.

Parameter	Description
Show level tree	<p>Select option to display the Levels tab in the <i>Map Window</i>. The tab contains the levels list of the <i>Map</i>, that allows switching between levels.</p> <p>By default it is selected.</p> <hr/> <p>Note. If not selected, then switching between levels in the <i>Map Window</i> is possible only with the help of level link icons (see Working with Map Layers).</p>
Show alarmed levels	<p>Select option to display the Alarms tab in the <i>Map Window</i>. The tab contains the alarmed levels list of the <i>Map</i>, that allows quick switching between alarmed levels.</p> <hr/> <p>Note. A level is considered alarmed if at least one of the objects placed on this level is alarmed.</p> <hr/> <p>By default it is selected. Unavailable if Show level tree is not checked.</p>
Work with Media Client	<p>Choose <i>Media Client</i> that will be used to watch video when jumping from <i>Map Window</i>. To jump to the <i>Media Client</i> to watch video click the icon of one of the objects located in the <i>Map Window</i>:</p> <ul style="list-style-type: none">• <i>Camera</i> – when jumping the cell of the corresponding <i>Camera</i> will be displayed in the 1x1 layout in live video mode;• <i>Sensor</i> – when jumping the cells of all <i>Cameras</i> specified in the selected <i>Sensor</i> object settings will be displayed in the most appropriate layout in live video mode.

6.1.4 Event Viewer

Object represents a visual log of the events that occur within the entire system.

Parent object – [Desktop](#).

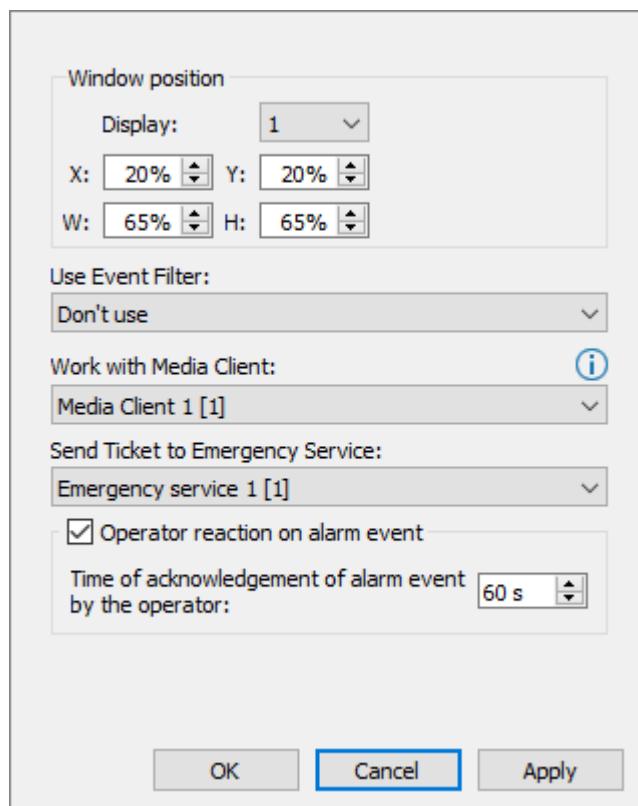


Figure 108. Event Viewer object settings window

Table 19. Event Viewer object settings

Parameter	Description
X, Y, W, H	Specify the object window's top left corner coordinates (X, Y), as well as its width and height (W, H), as percentages of the display's horizontal and vertical size.
Display	Choose the ID of the physical display this Event Viewer belongs to.
Use Event Filter	The Event Filter is used to control what events are displayed in the Event Viewer interface window. Optional parameter. If Don't use value is selected then all system events will be displayed. If filter is selected, only events allowed by selected filter (see Event Filter section) will be displayed.
Work with Media Client	Choose Media Client that will be used to watch video appropriate of event listed in the protocol. Warning! If Media Client is not selected, then you will not be able to jump from the <i>Event Viewer</i> to the <i>Media Client</i> to watch video.
Send Ticket to Emergency Service	Choose from the list an <i>Emergency service</i> object that will be used to create and send <i>Emergency ticket</i> (see Emergency service and Interaction with External Emergency Service).
Operator reaction on alarm event	Check this option to enable operator reaction on alarm events.

Parameter	Description
Time of acknowledgment of alarm event by the operator	Define the time for alarm event acknowledgement by the operator, in seconds.

6.1.5 External Window

Object is used to automatically launch an external application and position its window on the screen.

Parent object – **Desktop**.

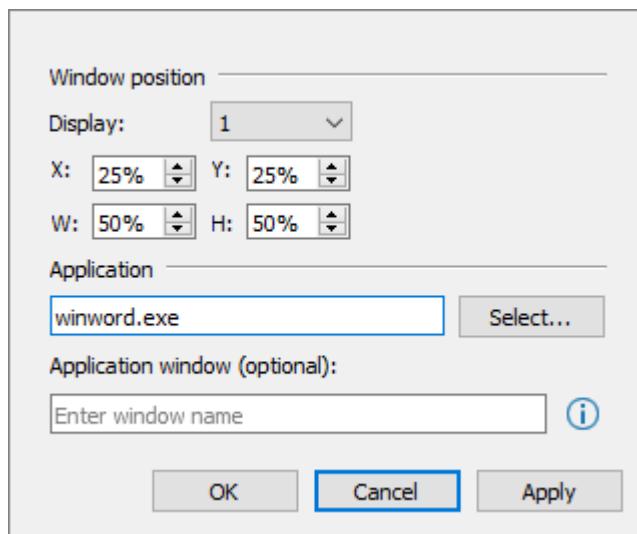


Figure 109. External Window object settings window

Table 20. External Window object settings

Parameter	Description
Display	Choose the ID of the physical display this object belongs to.
X, Y, W, H	Specify the object window's top left corner coordinates (X, Y), as well as its width and height (W, H), as percentages of the display's horizontal and vertical size. Window size may not be set for all applications when they are called by an external program. The range of possible values of the coordinates (X, Y) and the window sizes (W, H) – [0 ; 999]. For example, if X=150, Y=0, W=150 and H=100 values are specified, then the window of the external application will be located on the second and third displays (horizontally). Window vertical size will be equal to vertical size of the second display.
Application	Specify path to executable file. You can omit the exact path to the file if it is located in the directory specified in the Path environment variable.
Select (button)	Click on this button and use file manager to browse executable of an application to be started.

Parameter	Description
Application window (optional)	For the multi-window applications specify the name of the window that the operator needs to work with.

6.1.6 HTML Form

Object defines position and type of HTML forms permanently displayed on the screen of a parent *Desktop* object.

This object is intended for integration of any HTML form based user interface into SecurOS. Interface is being loaded when corresponding *Desktop* is activated.

Note. SecurOS includes several default *HTML forms* that can serve as a base for custom forms. Files have .html extension and can be found in <SecurOS_Folder>\Dialogscript\ directory. Content of this folder must be the same for all *Operator workstation* where *HTML forms* are going to be run.

More details on operations with HTML form are given in [SecurOS Programming Guide](#).

Parent object – [Desktop](#).

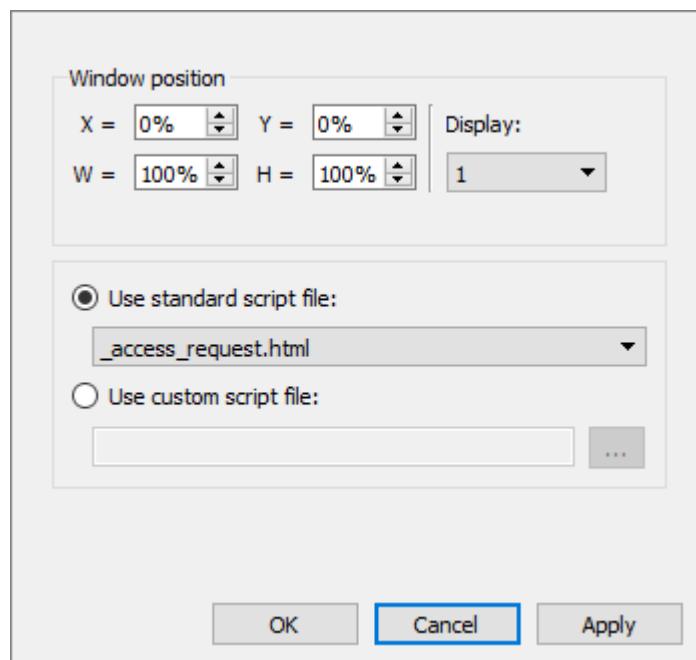


Figure 110. HTML Form object settings window

Table 21. HTML Form object settings

Parameter	Description
Window position	
X, Y, W, H	Specify the object window's top left corner coordinates (X, Y), as well as its width and height (W, H), as percentages of the display's horizontal and vertical size.

Parameter	Description
Display	Choose the ID of the physical display this object belongs to.
Scripting	<p>Select this option to use default HTML form that is included in SecurOS. Select file with form's HTML source code from the list.</p> <hr/> <p>Note. Default HTML forms are located in <SecurOS_Folder>\Dialogscript directory.</p>
Use standard script file	<p>Select this option to use custom HTML form created by user. Enter the following into the field:</p> <ul style="list-style-type: none">• HTML file name, if form's HTML source code is located in <SecurOS_Folder>\Dialogscript directory;• full path to HTML file, if HTML source code is located somewhere else. <hr/> <p>Notes:</p> <ol style="list-style-type: none">1. To specify the path with help of file manager click the  button.2. It is unable to specify path with file manager when configuring remotely.

6.1.7 HTML5 FrontEnd

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*.

The object is intended for creation the window on the SecurOS *Desktop* to display external HTML application that include SecurOS control interface. This application window is loaded when the corresponding *Desktop* is activated.

Using the object, one can integrate any external applications that support HTML5 into SecurOS.

Object allows:

- To specify size and arrangement of the external HTML application window on the SecurOS *Desktop*.
- To select *Media Client* and *Map Window* with which external HTML application can work;
- To transmit additional parameters from SecurOS to the external HTML application.

Parent object – **Desktop**.

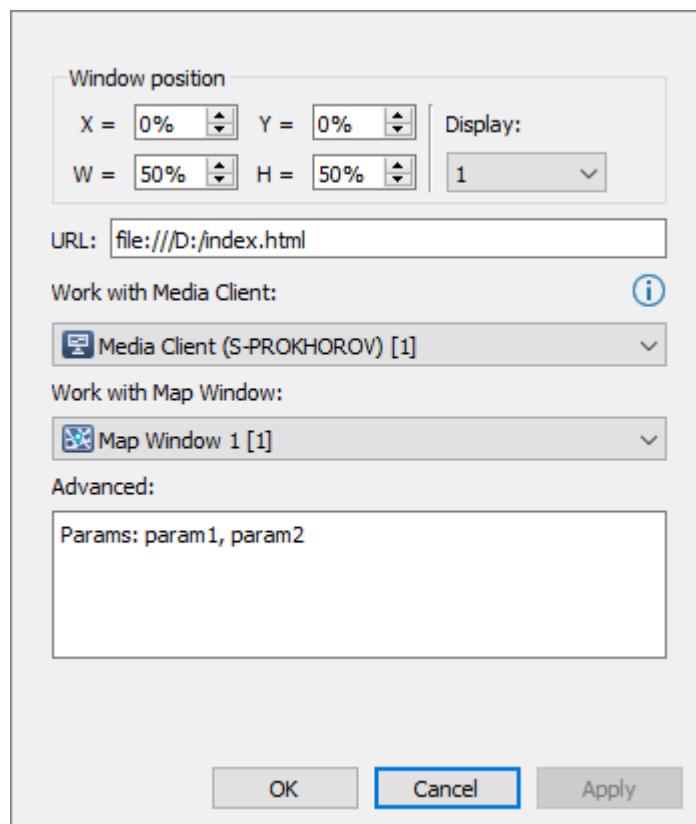


Figure 111. HTML5 FrontEnd object settings window

Table 22. HTML5 FrontEnd object settings

Parameter	Description
Window position	
X, Y, W, H	Specify the object window's top left corner coordinates (X , Y), as well as its width and height (W , H), as percentages of the display's horizontal and vertical size.
Display	Choose the ID of the physical display where the window of the external HTML application will be displayed.
URL	
	Specify URL of the HTML page of the external application or specify the path to the index file.
Work with Media Client	
	In the drop-down list select the <i>Media Client</i> that will be used to work with the HTML application. Working with <i>Media Client</i> means sending it <i>Events</i> or <i>Commands</i> in the SecurOS format.
	<i>Note.</i> <i>Media Client</i> control <i>Events</i> and <i>Commands</i> are described in the SecurOS Programming Guide .

Parameter	Description
Work with Map Window	<p>In the drop-down list select the <i>Map Window</i> that will be used to work with the HTML application. Working with <i>Map Window</i> means sending it <i>Events</i> or <i>Commands</i> in the SecurOS format.</p> <hr/> <p>Note. <i>Map Window</i> control <i>Events</i> and <i>Commands</i> are described in the SecurOS Programming Guide.</p> <hr/>
Advanced	<p>If it necessary to pass additional parameters from SecurOS to the external HTML application specify these parameter within this field. Specified parameters will be passed to the external application inside the <code>SETUP</code> message together with selected <i>Media Client's</i> and <i>Map Window's</i> IDs.</p>

7 Video Subsystem

The video subsystem is used to operate and configure the video devices within the SecurOS network. In addition, it is responsible for transmitting video streams between servers and workstations as well as working with live and archived video from within workstations.

7.1 Hardware Decoding

Hardware decoding allows to transfer loading, that is generated by H.264/H.265 stream transcoding, from the CPU to a special hardware module of the integrated Intel HD Graphics GPU – Multi-Format Codec Engine (MFX). This hardware module provides completely independent video processing that makes video processing faster, and allows to reduce CPU load and system power consumption in a whole.

Different manufacturers use independent trademarks to designate hardware decoding technology: Intel Quick Sync Video, NVIDIA PureVideo HD, ATI Avivo. Currently, the most commonly used is the Intel Quick Sync Video technology, which is several times superior to all competitive solutions in regards to decoding speed. SecurOS supports this technology when using the Intel HD Graphics 2500, HD4xxx, HD5xxx (based on the GT3 cores) graphic adapters and above.

All listed graphics adapters use Intel Quick Sync Video 2.0 technology.

All listed video processors are CPU integrated and support hardware decoding independently of central processor model (i3, i5, i7):

- For H.264 – on Intel Core 3xxx and above.
- For H.265 – on Intel Core 5xxx and above.

It should be noted, that not all CPU models have integrated graphics adapters (for example, some models of Intel Core i7 and Xeon).

Warning! Currently SecurOS does not support Intel Quick Sync Video 1.0 technology for the mobile and desktop Intel HD Graphics 2000 graphics adapters. Thus, hardware decoding is not performed for Sandy Bridge architecture based CPUs.

The key metric of the MFX block efficiency is its bandwidth (in Gbit/sec of the compressed video), that is limited not only by the number of video streams decoded at the same time, but the total number and size of these streams. For example, Intel Quick Sync 2.0 decoder can process about 40 – 50 streams of 2 Mbit/sec each.

RAM efficiency can be a limiting factor. In other words, the RAM should have time to process a specified number of the decoded streams. The data level directly depends on the used resolution. So to get maximal efficiency, dual-channel RAM should be used with a recommended frequency of 1600 Mhz and above.

If only the Intel HD Graphics integrated graphics adapter is installed and used, then hardware decoding mode is installed and used by default.

If a discrete graphics adapter is installed and used, then integrated one is automatically disabled by Motherboard's driver. To turn on the hardware decoding mode for such a computer configuration, do the following:

1. Enable integrated graphics adapter in the BIOS (location of the command in the BIOS menu depends on BIOS manufacturer and version). After this operation is complete, integrated graphics adapter is detected by the Windows **Device Manager**.
2. If monitor is plugged in the discrete graphics adapter connector, expand Windows' desktop to the dummy monitor of the Intel HD Graphics adapter:
 - Open screen resolution settings (**Control Panel→Appearance and Personalization→Display→Screen Resolution**):
 - Click the **Detect** button (see figure 112).

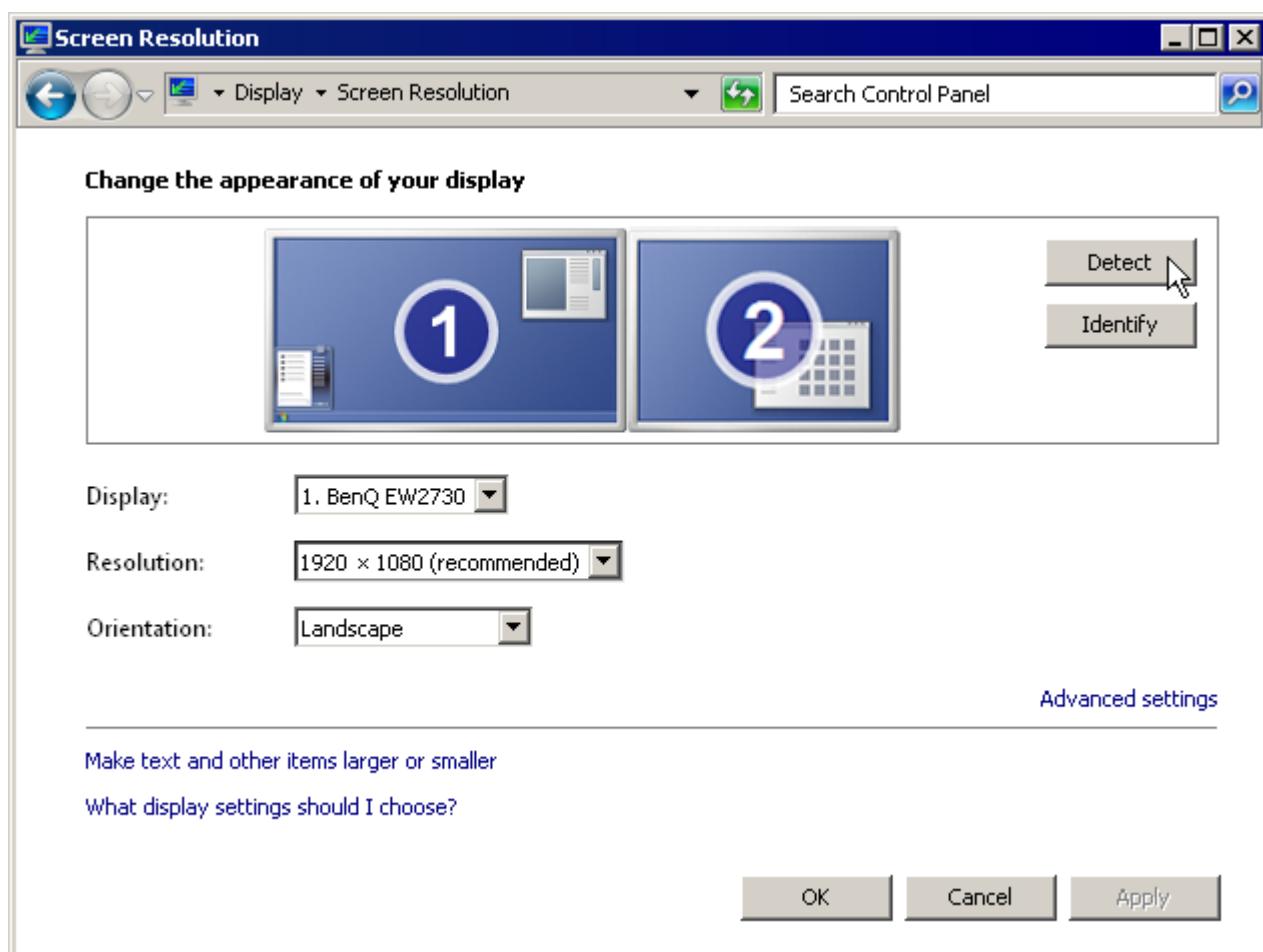


Figure 112. Detecting Intel HD Graphics adapter

- Click detected dummy display to select it. From the **Multiple displays** drop-down list choose Try to connect anyway to: VGA. Click the **Apply** button (see figure 113).

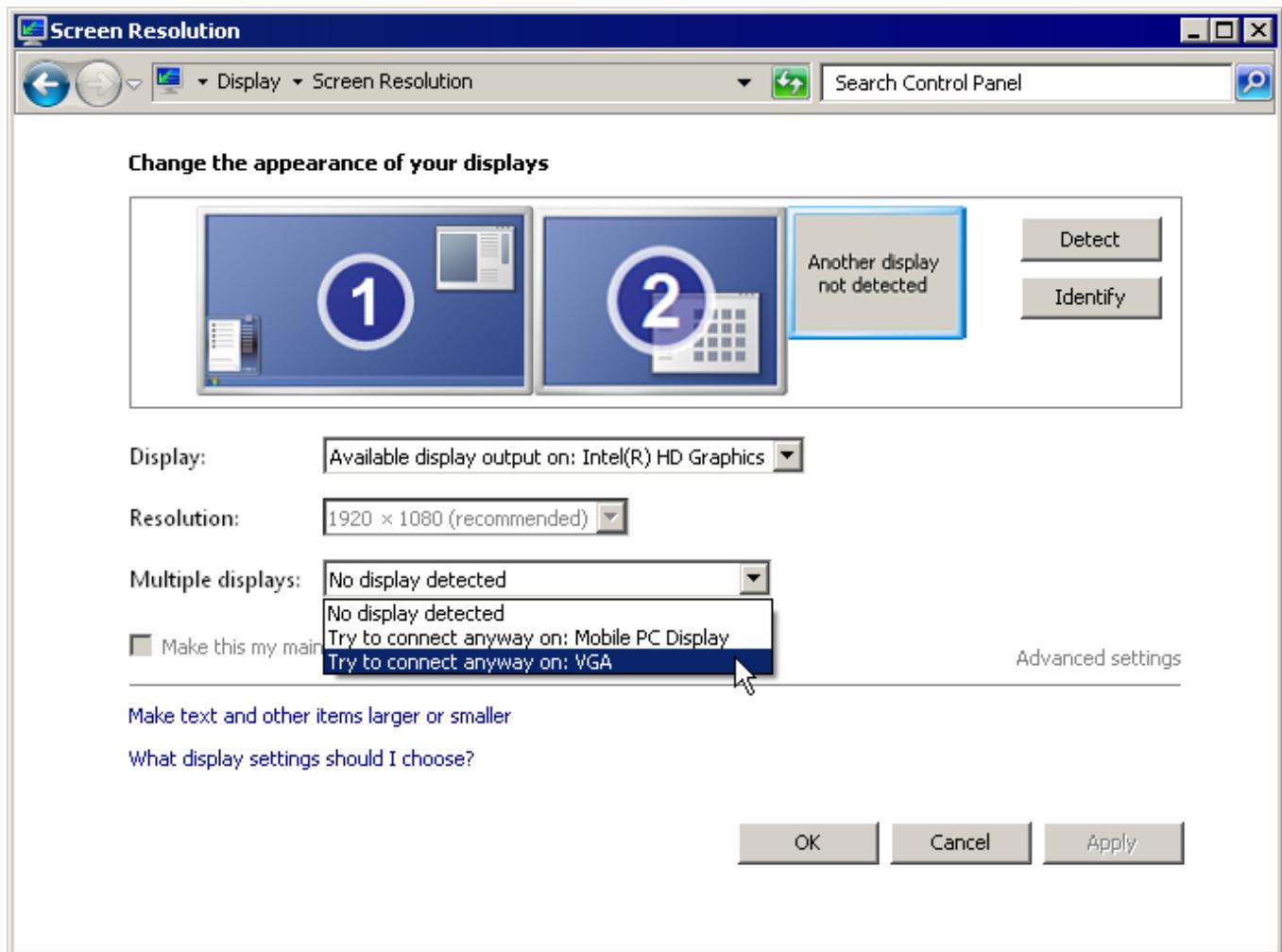


Figure 113. Choosing display to connect to

- Click dummy display to select it. From the **Multiple displays** drop-down list choose Extend desktop to this display (see figure 114). Click **Apply** button.

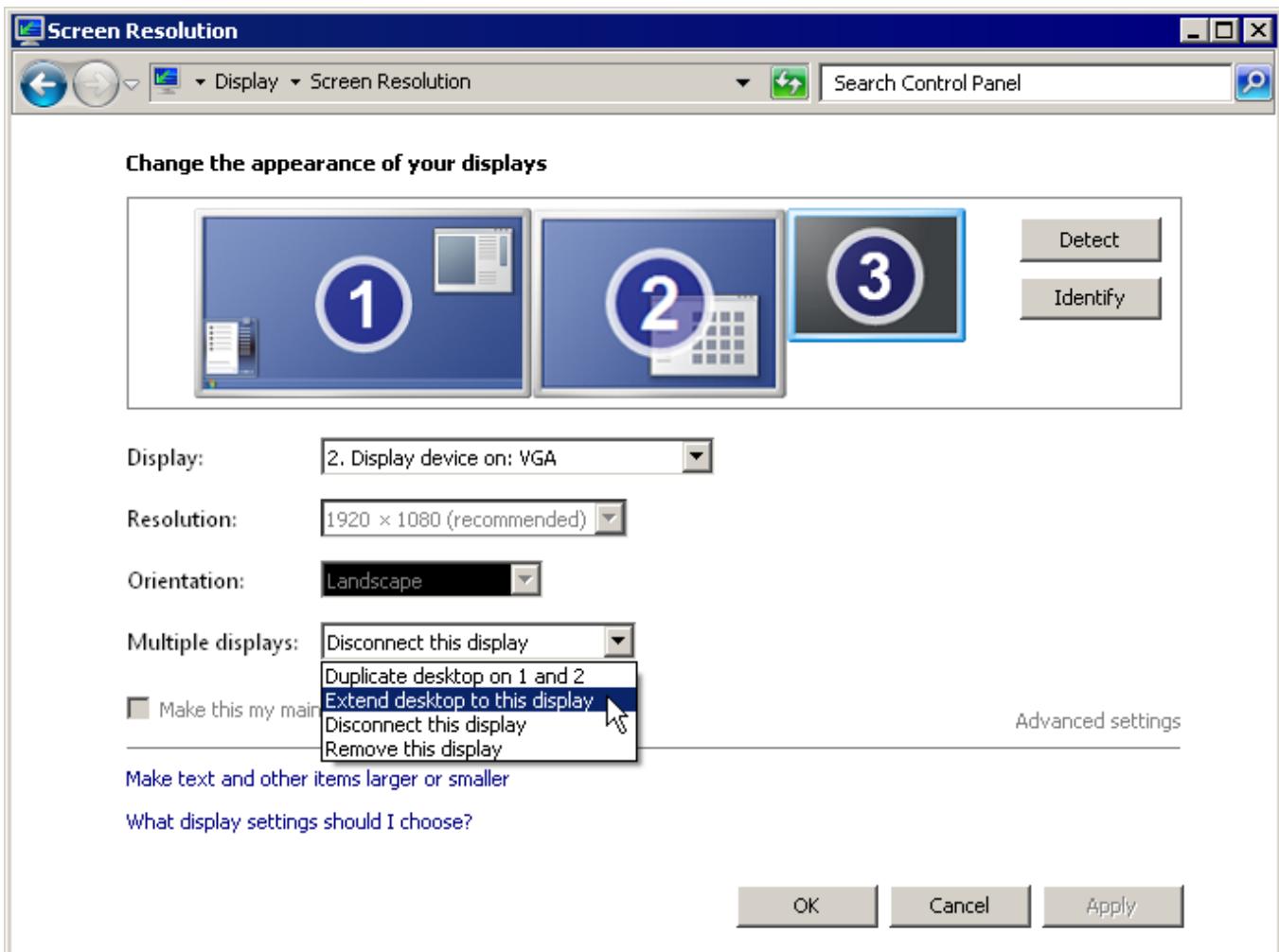


Figure 114. Expanding desktop to the selected display

Note. If single monitor, plugged in discrete adapter connector is used, choose Extend these displays.

7.1.1 Setting up Hardware Decoding

To turn hardware decoding on/off do the following on the *Computers with the Media Client (Video Server or Operator Workstation)*:

1. Stop SecurOS Control Service.
2. Launch the system utility for registry editing (type **regedit** in **Start → Run** box and click **OK**).
3. Open the **\HKLM\SOFTWARE\Wow6432Node\ISS\SecurOS\NISS400** branch, and create the **HWAcelEnable** parameter.

Warning! By default, if this parameter is missed, hardware decoding is on.

4. Specify parameter value:
 - 0 – hardware decoding is off;
 - 1 – hardware decoding is on.
5. Close the **regedit** utility.
6. Start SecurOS Control Service.

7.2 Multi-streaming

The most modern video cameras support multi-streaming - a feature, that allows a camera to generate several independent video streams. Streams can have different parameter sets (i. e. resolution, fps, compression, etc.) and can serve different purposes. These sets of parameters may be predefined and identified by the stream name, or can be specified in the camera's *Profile*, which is created by an administrator via the *Camera*'s web interface.

A larger size stream (having high resolution, fps, etc.) is used when it is necessary to output the *Camera*'s video in a large cell of a *Media Client*, use digital zoom, or record video archive. Smaller size streams (having low bitrate) are used to transmit video over channels with low bandwidth (for example, when transmitting video via 3g to mobile devices), to record "light" archive (when it is necessary to store archive in low capacity storage for a long time), to output video to the *Media Client* in a high cell layout, or to low a resolution display.

Using cameras that support multi-streaming allows for a balanced system configuration and to solve the following tasks:

1. To display video of different quality from the same camera on different *Media Clients*. For example, in one *Media Client*, video is displayed in a small cell. In this case it is not necessary to increase network load using a large size stream. At the same time one can watch the same video in the better quality (for example, with more resolution or fps) on a different *Media Client*, where network loading is not a critical parameter or where it is necessary to display high quality video.
2. Use different streams from the same *Camera* to display and record the same video in different quality. If the communication link between the *Video Server* and *Operator Workstations* has low bandwidth, it is possible to record high quality archive and transmit video with low bitrate to be viewed by the operator in real time without overloading the network.
3. To use different quality streams for display and to be analyzed by different detectors.

The SecurOS multi-streaming feature allows the use of three different streams generated by the *Camera* simultaneously. Each of them can be used as a stream for recording. The listed above tasks are solved by assigning stream types in the *Camera* object settings.

7.3 Frame Rate Reduction

Any value of **FPS**, specified in one of the *Media Client*, *Camera*, *Zone* (*Zone settings* tab) or *Archiver* objects, will cause frame rate reduction of the original video stream by I-frames. Frame rate reduction is a two-stage process:

- In the first stage, the video frame rate is reduced to the I-frame frequency, which is calculated as the video stream frequency divided by the value of the **GOP length**(**GOV length**, **Intra-Period** or **Intra-Refresh Period**) parameter, specified in the IP camera settings. For example, if the original video stream frequency is 30 fps and the **GOP length** parameter value is set to 10, then the reduced video stream frequency will be 3 fps.
- In the second stage, the frequency obtained in the first stage, is compared with the **FPS** value, specified in the *Media Client*, *Camera* or *Zone* object settings:
 - If the **FPS** value is greater than the frequency obtained by the initial reduction, then no further frame rate reduction is performed;
 - If the parameter value is less than the frequency obtained by the initial reduction, then further frame rate reduction of I-frames is performed (frequency is reduced to parameter value). For

example, if the I-frame frequency is 16 fps and **FPS** is 8 fps, in the final video each second I-frame will be reduced.

7.4 Working Principles of Motion Detection Zones

The SecurOS system provides a multi-zone motion detector to split the camera surveillance area into several independent areas (zones), which may have different motion detection parameters.

A **Zone** object corresponds to each motion detection zone (see [Zone](#) section). Basically, all zones are divided into two types:

- *Alarming* – designed to fire an alarm immediately upon motion detection.
- *Informational* – designed to generate a "motion detected" event, which can be used for scripting and other purposes. This event would not fire an alarm on the camera, though.

Example. For instance, the user needs to control an area with a gate and several windows seen above the gate. The task is to make alarm activation each time somebody appears at a window whereas to avoid generating alarms each time the gate is used. In this particular case, it is recommended to set two different **Zone** objects: the first for the gate and the second for the windows. The window zone should be configured as Alarming (to generate an alarm upon any motion detection), while the gate zone should be configured as Informational (to generate a motion detection event, but not to generate an alarm). Moreover, if different windows have different types of illumination, you can configure multiple **Zones** with different contrast parameters for reliable motion detection for each window.

Both alarming and informational zones should be armed by an administrator to detect motion. A zone can be configured to be always armed, meaning an operator does not have to arm it manually (see [Zone](#) section). All the other zones can be armed manually.

7.4.1 Creating Zones

Separate from the Main zone, you can create additional Zones for each secured area within the camera view.

7.5 SecurOS Archives

There are two types of video archives in SecurOS:

- *Primary archive* – an archive with a limited period of storage. This archive will be created automatically, for example, when camera recording video. By default it is stored in a VIDEO folder on the disk, specified in the [Computer](#) object settings.
- *Long-term archive* – archive with a long-term storage period, created by converting the files of the primary archive. By default it is stored in a Archive\VIDEO folder on the disks, specified in the [Archiver](#) object settings.

This *Long-term archive* functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

Primary archive is available by default, ability to work with *Long-term archive* should be enabled with additional settings (see below).

An **Archiver** object is used to copy a *Primary archive* to the *Long-term archive*. Procedure is started automatically or with the help of Automation Subsystem objects (see [Archiver](#)).

To view both type of archives use a **Media Client**. A *Primary archive* is available for viewing by default. To view *Long-term archive* one must additionally turn the **Access to Long-term archive** option on in the **Media Client** object settings (see [Display options Tab](#)).

Archive of any type can be exported from the SecurOS format to the file of the standard AVI/ASF format or the file of the special Evidence format. In the last case file can be encrypted and protected with the password (see [Archive Converter](#)). The **Media Client** is used for export. To provide export it is necessary to select the **Archive Converter** or turn on the **Archive export profiles** option (see [Archive export Tab](#)) in its settings. One can use digital signature when converting files (see [Digital Signature](#)).

Note. Alternatively, you can use the [ISS Media Export Utility](#) (backup.exe) to convert archive to the file of standard format.

See also:

- [Disk Volume Settings](#);
- [Video Recording Settings](#).

7.6 Camera Local Storage (Edge Storage)

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

Edge Storage is a technology that allows IP cameras to record and store video archive in their own storage. Such storage may be a built-in memory module, a removable media (for example, SD card) or a network folder. To use these technology within SecurOS the own **EdgeStorage Sync** technology has been developed, which provides continuous recording of the operational archive even in cases of temporary lack of communication between the camera and the *Video Server*.

The main uses of the **EdgeStorage Sync** technology in SecurOS are the following:

1. In cases of network failures and problems with equipment not related to the camera itself (for example, with a memory card). In such cases video fragments absent on the *Video Server* will be copied from the camera storage after the system recovery.
2. In cases when the camera is located in moving objects (buses etc.) and continuous connection with it is absent. In such cases the archive is copied from the camera local storage to the SecurOS primary archive after the connection between the camera and the *Video Server* is restored.

If errors occur with the **EdgeStorage Sync**, they are reported in SecurOS with the help of *Health Monitor* module (see [Health Monitor self-diagnostic Module](#)).

7.6.1 System Requirements to Provide Edge Storage Use

This section describes the following system requirements for working with the **EdgeStorage Sync**:

- [Hardware Requirements](#);
- [Time Synchronization](#);

- Requirements to the Camera Local Storage.

Hardware Requirements

SecurOS supports cameras local storages of the following brands:

- Axis;
- Bosch;
- Dahua;
- HikVision;
- Hanwha (Samsung);
- SecurOS Motus;
- Other cameras and devices that support ONVIF specification.

For some cameras **EdgeStorage Sync** feature is available in SecurOS via HTTPS.

Time Synchronization

To provide correct **EdgeStorage Sync** working it is necessary to use the NTP server to synchronize time on the SecurOS *Video Server* and the camera. The following restrictions are applied to the NTP server:

- It is not allowed to manually change the time on the NTP server.
- Automatic Daylight Saving Time changes are not supported.

The same Time zone must be specified in the camera's and the computer's settings.

Requirements to the Camera Local Storage

Most of the cameras use removable media such as a SD and a microSD cards as a local storage. Use only memory cards recommended by the camera manufacturer.

7.6.2 Configuring System to Use Edge Storage

To prepare the system to apply the Edge Storage feature do the following:

- **configure SecurOS**;
- **configure camera**.

Setting up SecurOS

Do the following:

1. On each *Video Server* where you going to use an **EdgeStorage Sync** technology for compatible *Cameras* create an **EdgeStorage Sync** object (see [EdgeStorage Sync](#)).
2. For cameras, archive of which must be synchronized with the local storage, select the **Recover archive from the local storage of Camera (Edge Storage)** checkbox on the **Recording** tab in the *Camera* object settings window (see Figure 115).

Note. Parameters required to configure interaction with the **Edge Storage** more flexible, are described in the **Recording Tab** subsection of the **Camera** section.

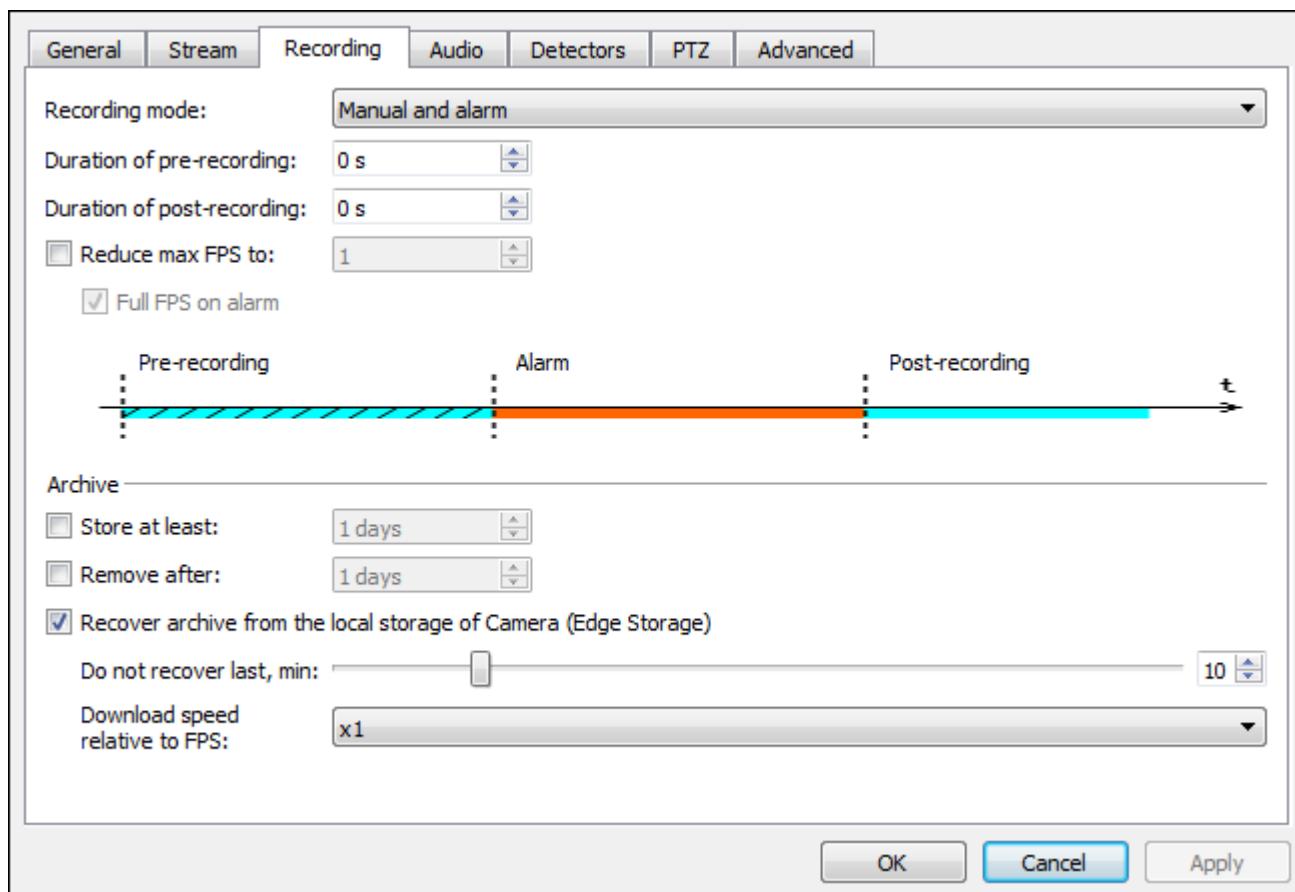


Figure 115. Recording Tab (for the Axis camera settings example)

Setting Up Camera

Setting up recording to the local storage is performed via camera's web interface.

To set recording to the local camera storage do the following (the following is an example from the AXIS Q7411 single channel video encoder):

Warning! Cameras of some brands may require additional steps to provide correct work of the SecurOS with Edge Storage (see [Features of configuration of some cameras](#)).

1. Open a web browser and in the address field enter the IP address, assigned to the camera when connecting to the network. To get access to the web interface enter the administrator login/password in the authorization window. In the application window open the **Setup** group (see Figure 116).

The screenshot shows the 'Continuous Recording' configuration page for the AXIS Q7411 Video Encoder. On the left, a sidebar lists various configuration tabs: Basic Setup, Video & Audio, Live View Config, PTZ, Detectors, Applications, Events, Recordings (with sub-options List and Continuous selected), System Options, and About. The main panel title is 'Continuous Recording'. It contains a section for 'Video Channel: 1' with an 'Enable' checkbox checked, a 'Disk' dropdown set to 'SD card', and a 'Stream profile' dropdown set to 'Quality'. At the bottom are 'Save' and 'Reset' buttons.

Figure 116. Setting up recording Tab

2. Select **Recordings** → **Continuous** from the group of settings.

3. In the **Continuous Recording** tab do the following:

- activate **Enable** checkbox to specify the device channel transmitting video to record.
- select **SD card** in the **Disk** list.
- in the **Stream profile** list select profile to record.

Notes:

1. The list consists of a predefined number of stream profiles. Default profile settings can be changed by the administrator in the **Video & Audio** tab.
2. To ensure smooth playback of the synchronized operative archive and provide correct working of video analytical modules, it is recommended to use the same stream profile to record video both on the camera and in SecurOS.

4. Click the **Save** button to save the changes.

Features of configuration of some cameras

Hanwha cameras (Samsung)

To provide **EdgeStorage Sync** correct work with the Hanwha cameras (Samsung) do the following:

1. Set recording type to **SD Normal**.
2. Disable recording by events (such as AlarmInput, MotionDetection, NetworkDisconnect and others).

Warning! When configuring Hanwha (Samsung) cameras be careful when changing the codec for recording video to the local storage. Video saved with another codec will not be restored to the SecurOS primary archive.

7.7 Special Settings for Video Subsystem Components

This section describes specifics of the video subsystem objects configuration procedure.

7.7.1 Camera Image Control

An administrator can configure the camera image in two different ways:

1. In the *Camera* object settings window (see [Camera](#) section);
2. Using operator workstation User Interface (see [SecurOS Quick User Guide](#)). Assuming that a *Video Capture Device* and a *Camera* object have been created, an administrator has to create a *Desktop* and a *Media Client* in order for the camera frame to appear.

7.7.2 Archive Recording

This section describes specifics of the archive recording operation and its configuration.

7.7.2.1 Disk Volume Settings

To avoid situations when there is no free space on a disk in case of permanent video recording in SecurOS format from the cameras (primary video archive), one should previously allocate mandatory free disk space.

This value is specified in *Computer* object settings (see [Archive](#)) and, by default, is set to 10% of hard drive volume.

If the free space threshold is reached then the archiver will try to record to other available disks. If there is no free disks then ring recording (FIFO) will be used (old files will be deleted automatically).

Warning! Network folders mounted as a network drives can be used to save archives. In this case each network folder must be used only by one network *Video Server*.

7.7.2.2 Video Recording Settings

Video recording procedure is controlled by the following keys of the Windows system registry:

- **MaxFrames** – controls archive recording mode with frame number limitation in the file (see [Archive](#), [Save space](#) archive recording mode);
- **MaxMemMb** – controls the queue of frames when writing an archive.

Archive recording with the limitation of the frames number in the file

When performing constant video recording, video files will be created containing a fixed number of frames. Once this number of frames is exceeded, the video-subsystem will start writing to a new file. If recording on motion, each video file might contain a different number of recorded frames. When an operator plays back the video recordings, the files will be scanned and played back sequentially. To make the video archive search more efficient, an administrator can change the number of frames that are recorded into one video file.

To change the frames recorded for one archive file, perform the following steps on the computer with the primary video archive disks:

1. Stop SecurOS Control Service.

2. Open the `\HKLM\SOFTWARE\ISS\SecurOS\NISS400\Video` folder and specify a the maximum number of frames for any new video record file in the `MaxFrames` key.

Note. When operating on 64-bit OS open the `\HKLM\SOFTWARE\Wow6432Node\ISS\SecurOS\NISS400\Video` branch.

Warning! Default value is 500.

3. Start SecurOS Control Service.

Controlling the queue of frames when writing an archive

When recording video, the video frames queue may cause a computer RAM overflow. By default, the RAM allocated for write queue is limited by 500 MB. This value can be changed by the `MaxMemMb` parameter in the following registry folder: `\HKLM\SOFTWARE\ISS\SecurOS\NISS400\Video`.

Note. When operating on 64-bit OS open the `\HKLM\SOFTWARE\Wow6432Node\ISS\SecurOS\NISS400\Video` branch.

Warning!

1. Possible values: [500, 2047]. Default value is 500.
2. Using a large value for the `MaxMemMb` parameter can lead to over consumption of the Windows allocated memory for a single process, thus causing the process to crash.
3. Too small value will result in a false occurrence of the **Insufficient write speed** problem (see [Health Monitor self-diagnosis Module](#)).

Note. In case for some reason the disk subsystem cannot properly handle the recording mechanism (e.g. read/write speeds) and video frame loss occurs, the following warning message can be found in the logs `\video.log` file: "WARN VideoFileRecorder Queue length has exceeded. Some frames were dropped.".

7.8 Object Reference

The video subsystem includes the following object classes:

- [System Objects](#).
- [User Interface Objects](#).

7.8.1 System Objects

The following are the System objects:

- [Video Capture Device](#).
- [Camera](#).
- [Defocus detector](#).
- [Layout](#).
- [View](#).
- [Zone](#).

- [Light Detector.](#)
- [Archive Converter.](#)
- [Archive Export Profile.](#)
- [Archiver.](#)
- [Image Processor.](#)
- [RTSP Server.](#)
- [ONVIF Server.](#)
- [EdgeStorage Sync.](#)
- [EdgeStorage Gate.](#)

7.8.1.1 Video Capture Device

Object represents IP camera connected to TCP/IP network.

Parent object – *Computer\Devices (Cameras & Microphones)* group.

Type Samsung

Model SPE-400

Protocol SUNAPI 2.0 (default)

PCI channel

Format

IP address 172.16.16.202

User admin

Password *****

View Show in web browser

Use secure connection (HTTPS)

OK Cancel Apply

Figure 117. Video Capture Device object settings window

Table 23. Video Capture Device object settings

Parameter	Description
-----------	-------------

Type	Select value that corresponds to device's brand. To identify <i>Video Servers</i> of a remote system within the <i>Monitoring Center</i> , working with remote archives (see Configuring VC/VR-connection), the ISS Video Concentrator type is used. To identify <i>Video Servers</i> of a remote system within the <i>Monitoring Center</i> , working with remote archives (see Configuring VC/VR-connection), the Video Repeater type is used. Functionality to support ISS Video Concentrator/Video Repeater types is available in the <i>SecurOS Monitoring & Control Center</i> only. The Virtual type represents an option for video emulation and is used to test system settings.
Model	If enabled, select the model of the <i>Video Capture Device</i> for the given Type.
Protocol	Select version of data transmission protocol used by camera that is being connected. <hr/> <p>Note. Parameter is available only if several version of integration software for camera with specified Type and Model, that correspond to different data transmission protocols and APIs, are supported by SecurOS.</p>
PCI channel	If the Virtual value is selected in the Type field then select a unique PCI channel number.
Format	Depending on the device type, choose video signal characteristic from the list (if enabled): H.264, MPEG4, MJPEG, PAL, SECAM etc.

Specify <host>[:<port>] component of the full device's URL.

One can specify the <host> value in the following form:

- as IP-address, for example, 172.16.1.12 – for devices of any **Type**, except Virtual.
- full domain name of the device, for example, axis.network.iss – for devices, which **Type** is Axis or Generic RTSP.
- short domain name of the device, for example, axis – for devices, which **Type** is Axis or Generic RTSP.

The [:<port>] component is optional and depends on used camera connection protocol, that is specified in the own camera settings via camera's web-interface.

If HTTP protocol is specified in the own camera settings, then port number can be set in the following form:

[:<http_port>] [:<rtsp_port>], where:

- [:<http_port>] – HTTP-port number;
- [:<rtsp_port>] – RTSP-port number to receive video stream via RTSP.

For example:

- 127.0.0.1:8080:554 – the 8080 HTTP-port and the 554 RTSP-port are specified.
- 127.0.0.1::554 – HTTP-port is not specified, the 554 RTSP-port is specified.

If RTSP protocol is specified in the own camera settings, then port number can be set in the following form:

[:<rtsp_port>], where:

- [:<rtsp_port>] – RTSP-port number to receive video stream via RTSP.

For example:

- 127.0.0.1:554 – the 554 RTSP-port is specified.

If device type is Generic RTSP in this field one can also specify the following:

- full URL of the device – <host>[:<port>]/<URL path>[?<parameters>].

	<ul style="list-style-type: none">• only <host>[:<port>] component of the full device's URL. In last case all other URL components (/<URL path>[?<parameters>]) must be specified in the <i>Camera</i> object settings (see Stream Tab, the Path parameter). Delimiter (/) can be specified both in IP address parameter and Path parameter in the <i>Camera</i> object settings.
User	Specify a user name for the IP device connection. Default value is securos .
Password	Specify individual device password or use default value. Warning! The password is displayed while typing, but on the next opening of the settings window "*" symbols are displayed in the field (the number of symbols differs from actual password length).
View	The link on the right allows user to quickly open the web page of the network camera settings in Internet Explorer web browser. If IP address , User or Password parameter is not specified, the link is disabled. <hr/> <p>Note. Fields of the IE web browser's authorization window are filled automatically with the User and Password values, specified in settings of this <i>Video Capture Device</i>.</p>
Use secure connection (HTTPS)	This parameter allows specify the type of connection with the camera. To use secure connection do the following: <ul style="list-style-type: none">• select this checkbox;• use camera's web-interface to select HTTPS for user and to select trusted certificate of encryption in own camera's settings. Warning! If at least one of the listed conditions is not met, then secure network connection with the camera will not be established. <hr/> <p>Notes:</p> <ol style="list-style-type: none">1. Parameter is available depending on selected device's Type. For the list of the supported devices contact Intelligent Security Systems Technical Support Team.2. If selected, then to transmit a video stream it is necessary to set the RTSP over HTTPS value for the Protocol parameter in the <i>Camera</i> object settings (see Stream Tab).3. If selected, then connection with the camera will always use TCP protocol, regardless of the RTP over RTSP (TCP) flag, see Stream Tab.

7.8.1.1.1 AC Recorder

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*.

Video Capture Device with **AC Recorder** type is designed to receive **Stream for recording** from active *Camera* located on one of the *Computers* within the security network. Received video stream is displayed in the child *Camera*'s standard cell in real-time mode and can be recorded into the video archive.

To configure **AC Recorder** do the following:

1. Enter the Administration Mode.
2. In the *Object Tree* select the *Computer* object to which the added device will be connected.
3. Create child *Video Capture Device* object in the *Devices (Cameras & Microphones)* group.
4. In the **Parameters of created object** window, select **AC Recorder** in the **Type** field.
5. In the created object settings window, in the **IP address** text box, specify the name of the *Computer* from which it is necessary to receive the stream of the active camera.
6. Create the *Camera* object (child object of the *Video Capture Device* object).
7. If *Media Client* on the given *Computer* works in the **Use only selected Cameras** mode add created *Camera* in the selected camera list. If *Media Client* works in the **Use all Cameras** mode, then created *Camera* will be added automatically.

7.8.1.2 Camera

This object represents a physical video camera or other video source.

Parent object – **Video Capture Device**.

Depending on camera's **Type** and **Model**, parameter settings window can include the following tabs:

- **General** Tab.
- **Stream** Tab.
- **Recording** Tab.
- **Audio** Tab.
- **Detectors** Tab.
- **PTZ** Tab.
- **Advanced** Tab.

Common *Camera* parameters, independent of the device's **Type** and **Model** are described in appropriate sections.

Besides settings, common for all integrated with SecurOS cameras, the last ones can have their own specific settings. These settings depend on camera's **Type** and **Model** and are used to control additional camera features. Description of such parameters one can find at the end of corresponding section.

Note. In this manual the most important additional parameters are described only. Description of other additional parameters one can see in screen tips in the *Camera* object settings window.

7.8.1.2.1 General Tab

Table 24 presents typical settings of the camera. Parameters, that depend on camera **Type** and **Model**, are described in Table 25.

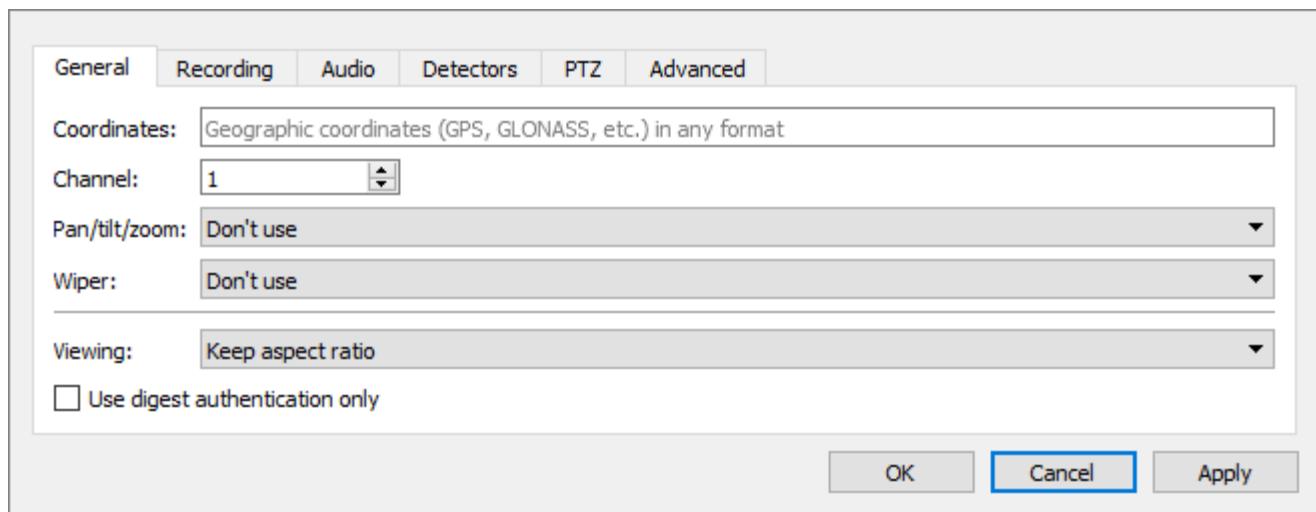


Figure 118. Camera object settings window. General Tab

Table 24. Camera object settings. General Tab

Parameter	Description
Coordinates	<p>Specify camera geographic coordinates (GPS, GLONASS, etc.) in any format. For example, 55.792461, 37.637515.</p> <p>Note. Camera coordinates will be transmitted along with other object settings when these settings will be queried from external system via REST API interface. Data will be transferred in the same form, in which they are specified in the object settings.</p>
Channel	Select the camera's channel number from the list.
Pan/Tilt/Zoom	<p>To switch IP device native telemetry control on select Use value from dropdown list (see Setting up telemetry). By default the Don't Use option is selected.</p> <p>Note. PTZ control panel becomes active when operator selects this camera on a Media Client.</p>
Wiper	<p>If the camera is equipped with the <i>Wiper</i>, select the object that can control it.</p> <p>Note. For more details see Configuring System to Work with Wiper.</p> <p>If camera is equipped with built-in wiper select the Built-in value. If this value is selected then Pan/tilt/zoom parameter will be automatically set to Use, which can not be changed.</p> <p>Note. To use this feature operator must have access right level for this camera not less than Control.</p>

Viewing	<p>This parameter defines the video image display format in the <i>Camera</i> cell for all <i>Media Clients</i> throughout the SecurOS security system. At the same time, for each <i>Media Client</i>, the video image displaying format can be locally changed for the selected <i>Camera</i> with the help of this <i>Camera</i> control (see SecurOS Quick User Guide). Possible values:</p> <ul style="list-style-type: none"> • Keep aspect ratio – original format of the video frame will be used when displaying video. Is the default value; • Stretch to cell – the frame is stretched to full size of the <i>Media Client's</i> cell; • Force 4 : 3 – when displaying, video will be scaled to 4 : 3.
----------------	--

Table 25. Optional General tab parameters

Parameter	Description
Use digest authentication only	<p>Tick this checkbox to encrypt credentials.</p>
Washing Kit	<p>If camera is equipped with washer set this parameter to Use.</p> <hr/> <p>Notes:</p> <ol style="list-style-type: none"> 1. This option is available for several models of the Axis cameras. For the list of the supported devices contact Intelligent Security Systems Technical Support Team. 2. To use this feature operator must have access right level for this camera not less than Control. 3. Washing procedure parameters are specified in the camera's own settings accessible via web interface.
Light	<p>If camera is equipped with built-in light, select the Built-in value from the drop-down list to turn light control on. If this value is selected then Pan/tilt/zoom parameter will be automatically set to Use, which can not be changed.</p> <p>Don't Use value disables illumination control. It is used by default.</p> <p>Some cameras allow to set the illumination rate. To set the rate pick required value from the list:</p> <ul style="list-style-type: none"> • Turn on LED group 1; • Turn on LED group 2; • Turn on all LED groups. <p>First, second or all LED groups will be used for illumination depending on selected value.</p> <hr/> <p>Note. To use this feature operator must have access right level for this camera not less than Control.</p>

7.8.1.2.2 Stream Tab

Table 26 presents typical camera parameters. Parameters, that depend on camera **Type** and **Model**, are described in Table 27.

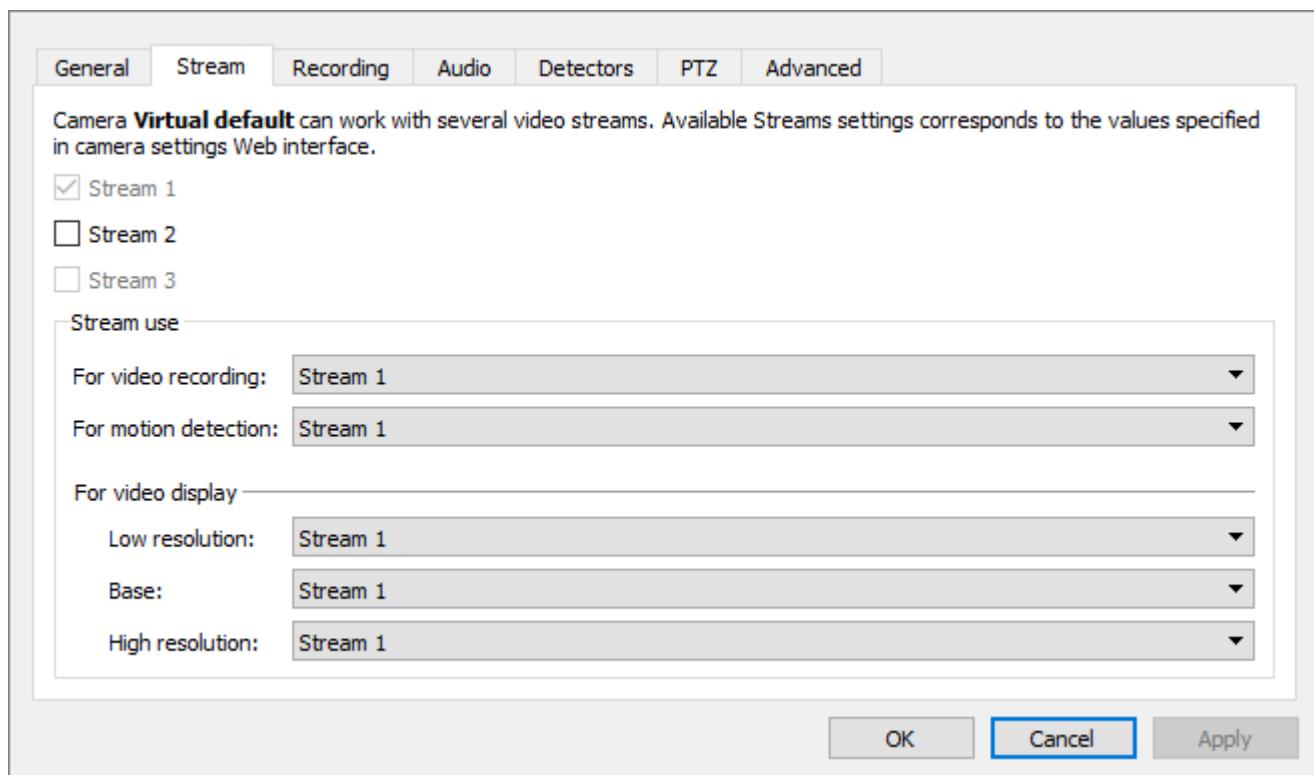


Figure 119. Camera object settings window. Stream Tab

Warning!

1. The tab represents typical settings of the camera, which supports multi-streaming.
2. For the cameras, which do not support multi-streaming, the set of parameters depends on the type of the parent *Video Capture Device* or this tab is not displayed.

Table 26. Camera object settings. Stream Tab

Parameter	Description
Stream 1 (activation of the Stream 1 configuration and use mode). By default it is active.	
<i>Note.</i> Settings of the Stream 1 , Stream 2 and Stream 3 are the same and depend on <i>Video Capture Device</i> type and model.	
Stream 2 (activation of the Stream 2 configuration and use mode). Tick this checkbox to make it possible to select this stream in the Stream use block.	
Stream 3 (activation of the Stream 3 configuration and use mode). Enabled only if Stream 2 is selected. Tick this checkbox to make it possible to select this stream in the Stream use block.	
Stream use	
For video recording	Select a stream for recording archive from the drop-down list.
For motion detection	Select a stream which will be analyzed by motion detector.

Parameter	Description
For video display	
Low resolution	Select a low resolution stream from the drop-down list.
Base	Select a base stream from the drop-down list.
High resolution	Select a high resolution stream from the drop-down list.

Warning! It is not recommended to set **GOP (GOV)** parameter greater than 32 frames or 2 seconds for the connected IP cameras and video servers. IP cameras can be configured through their web interface. For some types of *Video Capture Devices* this setting is available in the **Stream** tab of the *Camera* object settings window.

Some stream selecting recommendations are listed below.

1. To assign a **High resolution stream** it is recommended to choose a stream with the highest resolution, for example, to display video on the *Media Client* in large cells (for example, like in 1*1 or 2*2 layouts), or to display it on a *Video Wall Monitor*;
2. To assign a **Low resolution stream** it is recommended to choose stream with the lowest resolution, which complies with requirements to the particular security system. Such stream can be displayed on *Media Client* for 5*5 cell layouts and higher;
3. To assign a **Base stream** it is recommended to choose a stream, that has resolution sufficient to display video in average size cells (for example, in 3*3, 4*4 layouts on the *Media Clients* of the *Operator Workstations*, or in 4*4 and 5*5 layouts on *Video Wall Monitors*);
4. When assigning **Stream for recording** select a stream, which complies with requirements to the archive video for the given security system. When choosing a stream it should be considered, that the larger the stream, the larger the archive will be.

Warning! In current release all *Program detectors* and *Intelligent Modules* (SecurOS Auto, SecurOS Transit, SecurOS FaceX) operate with **Stream for recording**. Thus, when assigning **Stream for recording** it is necessary to consider Module's and Detectors' requirements and recommendations to the video settings of the *Camera*, which will be used by these Modules and Detectors.

In case if it is necessary to record high quality video, but communication link, connecting *Video Server* and *Operator Workstations* has low capacity, do not use **Stream for recording** when assigning any **Stream for display**. Under this condition high quality stream will not be transmitted outside the *Video Server* in real time mode (only when playing archives) and the communication link load will be significantly decreased.

Table 27. Optional Stream tab parameters

Parameter	Description
Options to work with streams (see Figure 120).	
Use camera settings	If this option is enabled, <i>Camera</i> stream will match the stream that corresponds to current camera settings in its web interface. By default it is selected.

Parameter	Description
Profile	With this field one can match each <i>Camera</i> stream to one of the streams, configured in camera's web interface. Pick from the list or type in manually the profile name, that corresponds to a stream configured in camera's web interface.
Stream	Some camera models has Stream checkbox (see table 26) is complemented by field named Stream . With this field one can match each <i>Camera</i> stream to one of the following original streams, configured in camera's web interface: <ul style="list-style-type: none">• Stream (1) – Stream (4);• MJPEG. <p>Warning! For cameras of <i>Video Capture Device</i> type Panasonic RTSP Stream when one selects MJPEG value, <i>Camera</i> stream will be matched with first of JPEG streams, configured in camera's web interface.</p>
Path	Specify the <URL path>[?<parameters>] components of the full device's URL to receive video stream via RTSP. For example, if full URL is as follows: <code>172.16.16.250/axis-media/media.amp?camera=1</code> then specify the following string in the Path field: <code>/axis-media/media.amp?camera=1</code> <p>Warning! Only for the devices, which Type is Generic RTSP.</p> <p>See also Video Capture Device, the IP address parameter.</p>
Camera ID in the edge device	Specify identifier, assigned to the <i>Camera</i> in the external device. Is used to view in SecurOS a video archive, stored in the external device, with the help of the <i>EdgeStorage Gate</i> object.
Protocol	This parameter specifies type of the connection with the camera. Possible values: <ul style="list-style-type: none">• RTP/UDP – UDP protocol will be used for interaction with camera.• RTP/TCP – TCP protocol will be used for interaction with camera.• RTSP/HTTP/HTTPS – insecure/secure TCP connection with tunneling will be used for interaction with camera. <p>Warning! To establish RTSP/HTTPS connection one should select trusted encryption certificate and HTTPS connection for the user in camera's own settings via camera's web-interface. The Use secure connection (HTTPS) checkbox must be selected in the <i>Video Capture Device</i> object settings.</p>

Parameter	Description
Use stream on request	Select this checkbox to transfer the live video stream to the system only if there is a stream consumer in the system. The consumer of the stream exists in the system when viewing live video, recording a video archive, during the operation of service analytics detectors (motion, defocus, blinding, etc.) or video analytic detectors. The parameter is designed to control the video stream when working in networks with low bandwidth.
Multicast, group of parameters (for the details see the Multicast section)	
Enable multicast mode	Select this checkbox to enable multicast translation from given camera.
Address (IPv4) for Multicast group	IP address to which video stream from given <i>Camera</i> will be translated (multicast group). Value must belong to the range of the D class IP addresses, reserved for multicast translation.
Port for Multicast group	Port number for multicast translation.
RTP over RTSP (TCP)	Select checkbox, if camera operates in a high-load network, network has low capacity, or within a network where RTP packets are filtered. Video will be transmitted using the TCP protocol.
Network latency, ms	Time period allocated to receive a frame at the current network bandwidth (in milliseconds). If actual network latency is known, it is recommended to set appropriate value. Otherwise use the default value. Note. This parameter is displayed only for several <i>Video Capture Devices</i> . If it doesn't, then 0, 5 s default value is used.

General Stream Recording Audio Detectors PTZ Advanced

Camera Axis XF40-Q1765 can work with several video streams. Available Streams settings corresponds to the values specified in camera settings Web interface.

Stream 1

Use camera settings

Profile:

RTP over RTSP (TCP)

Network latency, ms:

Stream 2

Figure 120. Stream Tab (for the multi-streaming Axis camera)

7.8.1.2.3 Recording Tab

Table 28 presents typical camera settings. Parameters, that depend on camera Type and Model, are described in Table 29.

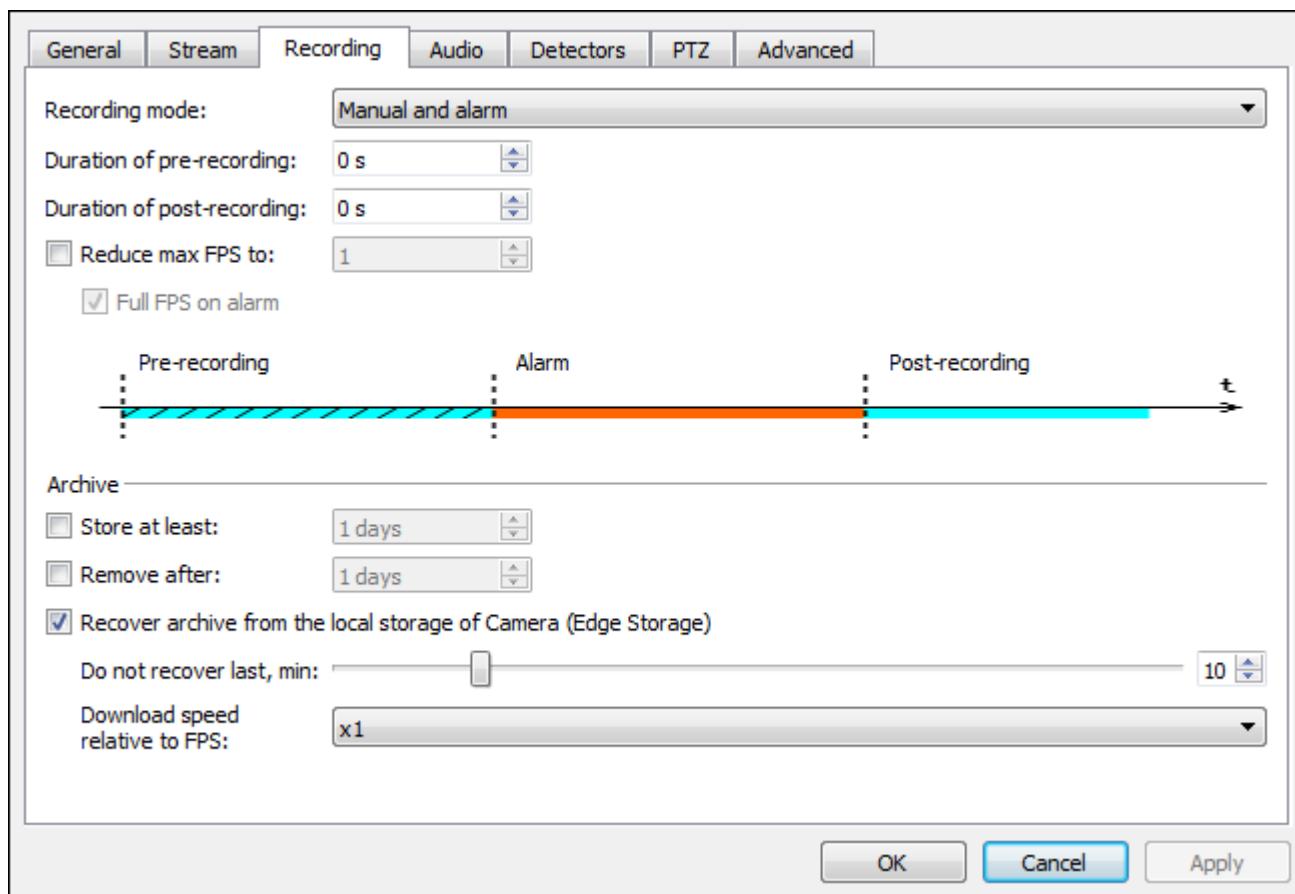


Figure 121. Camera object settings window. Recording Tab

Table 28. Camera object settings. Recording Tab

Parameter	Description
Recording mode	<p>Select the mode from the following:</p> <p>Manual – video recording will start either by an operator's command or with the help of the Automation subsystem.</p> <p>Manual and alarm – enable this option to allow to start recording video automatically when a motion by this camera is detected, and to stop it automatically when motion ends.</p> <p>Continuous – video recording will be performed constantly.</p> <p>Note. In this mode, recording can be stopped only by changing the <i>Camera</i> settings.</p> <p>Do not record – in this mode no one of the methods, known within SecurOS can be used to put camera to record mode (for example, record can not be started from <i>Media Client</i>, by program or <i>Macro</i>, from <i>Map</i> etc.).</p>

Parameter	Description
Duration of pre-recording	Specify the duration of pre-recording phase, in seconds. The more the length of this phase, the more RAM is used to cache video. Range of values: [0; 999]. If set to 0, pre-recording won't be used.
Duration of post-recording	Specify the duration of post-recording phase, in seconds. Range of values: [0; 999]. If set to 0, post-recording won't be used.
Reduce max FPS to	Use this parameter if you reduce the recording FPS. Range of values: [1; 99]. The mechanism of frame rate deduction is described in section Frame Rate Reduction .
Full FPS on alarm	<p>The original frame rate from the camera is maintained for the recording period during an alarm (motion detection). Only available if the Reduce max FPS to parameter is selected.</p> <p>In the Manual and alarm mode:</p> <ul style="list-style-type: none"> original frame rate of the video stream is used to record video during an alarm (motion detection). reduced frame rate of the video stream is used for pre- and post recording. <p>In all other recording modes parameter is ignored, specified reduced frame rate is used.</p>
Store at least	<p>Specify a minimum depth of video archive, in days.</p> <hr/> <p>Note. An hour of an archive creation is accepted as a beginning of a storage period, for example, 15:00 01.07.2015.</p> <hr/> <p>Checking of that, if archive files should be deleted is performed at system start and, further, at the end of each hour. An archive, storage period of which has not expired, will be automatically removed if there is no free space on hard disks to store new archive fragments. Removing starts with the oldest records; archive recording is suspended until released free space is enough. When such archive is removed the appropriate information message is displayed (see Health Monitor self-diagnostic Module). Range of values: [1; 9999].</p>
Remove after	<p>Specify a maximum depth of video archive, in days. Checking of that, if archive files should be deleted is performed at system start and, further, at the end of each hour. When specified value is reached, all archive records in an hour time interval are deleted depending on the Store at least parameter value (if specified). If you keep this field blank, the archive will be kept as long as there is free space on hard disk to store new archive fragments. Range of values: [1; 9999].</p>

Table 29. Optional Recording tab parameters

Parameter	Description
Playback archive from the edge device	Select this checkbox to work with archive, stored on the remote device (see EdgeStorage Gate). Warning! In SecurOS it is impossible to record video from the <i>Cameras</i> working with a remote archive.
Do not adjust frame timestamp for fast forward playback	Is used when viewing archive stored on the remote device with increased playback speed. Select this checkbox if archive position pointer offset speed does not match the playback speed. Is enabled, if Do not adjust frame timestamp for fast forward playback is selected.
Recover archive from the local storage of Camera (Edge Storage)	Select this checkbox to recover the <i>Video Server</i> 's archive from the local <i>Camera</i> 's archive when using the Edge Storage (see Camera Local Storage (Edge Storage)).
Do not recover last, min	<p>Specify the time shift to record an archive. When restoring the <i>Video Server</i>'s archive from the local camera storage will be copied the fragments up to the $T_{cur} - N$ timestamp, where:</p> <ul style="list-style-type: none"> • T_{cur} – current time; • N – specified parameter value. <p>The remaining part of the archive will be recorded with a time delay equal to the specified value of the parameter.</p> <p>This setting is recommended for use on the cameras that record video to the local storage in the large fragments. Set the parameter value that equal to or exceeds duration of the recording of the largest video fragment in the camera local storage.</p> <p>For example, specified parameter value is 10 minutes. Connection with the camera is lost for 15 minutes, then restored. After the connection is restored, the first 5 minutes of the archive starting from the moment of connection lost will be loaded from the local storage of the camera. The remaining 10 minutes of archive gap will be restored part by part in the next 10 minutes.</p> <p>This setting allows to avoid false error messages that appear due to inability to download an archive from the camera before it is actually stored in the local storage.</p> <p>Range of values: [0; 60].</p> <p>Default value is 10.</p>

Download speed relative to FPS	Specify speed of downloading archive from the local camera storage relative to the FPS of the live video stream. High speed allows to restore archive gaps faster, but increases network loading. Possible values: x1, x2, x4, x8, x16, x20. Default value is x1. When using default value the time required to restore archive gap is equal to gap duration.
---------------------------------------	---

7.8.1.2.4 Audio Tab

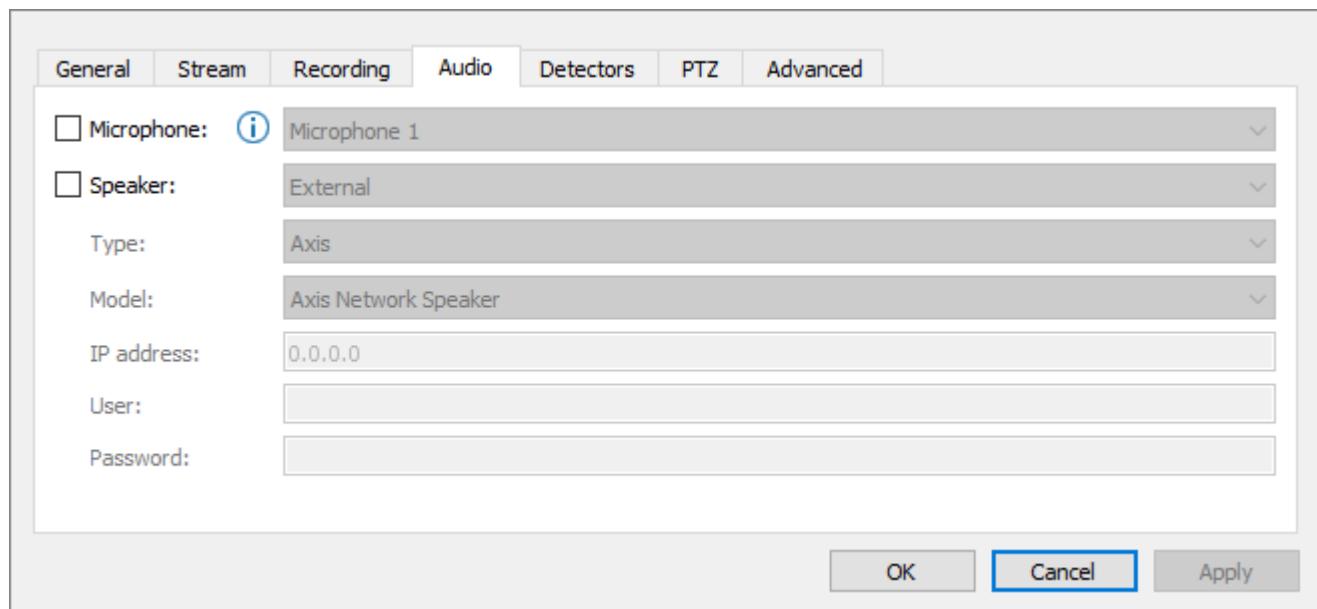


Figure 122. Camera object settings window. Audio Tab

Table 30. Camera object settings. Audio Tab

Parameter	Description
Microphone	Select an external <i>Microphone</i> to view video with sound both in live and archive mode.

Parameter	Description
Speaker	Select checkbox and choose type of the camera's speaker, to which sound will be translated. Possible values: Internal — use camera's built-in speaker. If camera is equipped with built-in speaker, this value is used by default. If this value is selected, then parameters below are disabled. External — use separate external network speaker. Notes: 1. Internal speaker is supported only by some Axis and Beward B camera models. 2. External speaker with Axis type may be connected to Camera with any Type and Model.
Type	Select a type of the external speaker.
Model	Select a model of the external speaker.
IP address	Specify IP address of the external speaker.
User/Password	Specify user name and password to operate the external speaker.

7.8.1.2.5 Detectors Tab

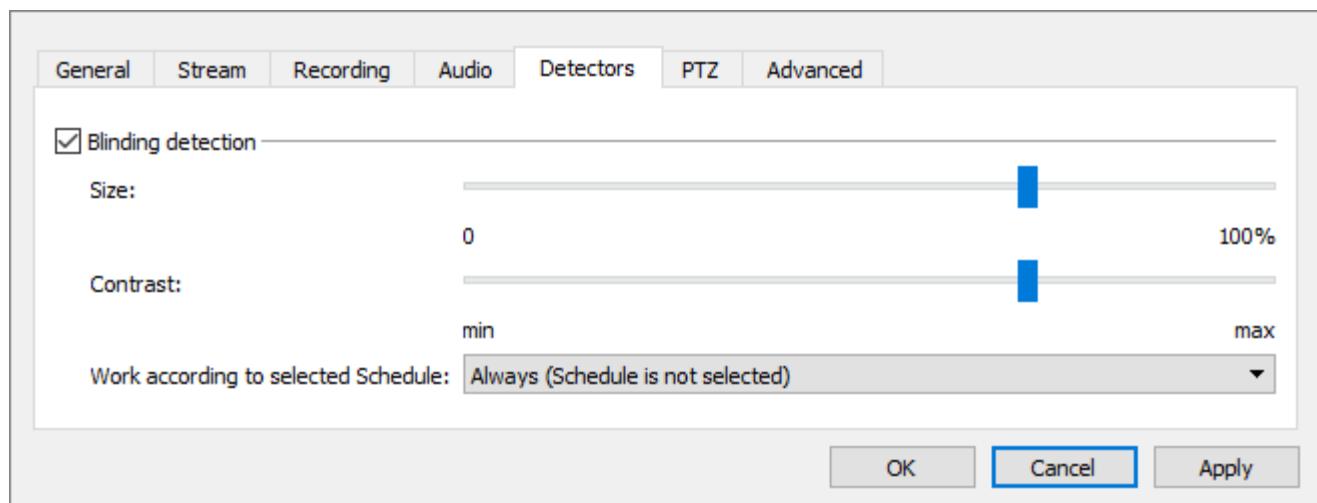


Figure 123. Camera object settings window. Detectors Tab

Table 31. Camera object settings. Detectors Tab

Parameter	Description
Blinding detection	Select this checkbox to force the system to generate special events each time camera blinding is detected. These events can be used in macros or scripts.

Parameter	Description
Size	Move slider to specify detection size sensitivity. Boundary values: 0% – camera is treated as always blinded. 50% – blinding will be detected if 50% of the frame area has low contrast. 100% – only full blinding (entire camera view has low contrast) will be detected.
Contrast	Move slider to specify detection contrast sensitivity. Boundary values: Min – only areas of minimal contrast are taken into consideration (e. g. evenly colored surfaces like sheet of paper). Max – areas with higher contrast are also taken into consideration.
Work according to selected Schedule	Select the Schedule if the blinding detector should work in the specific time range.

7.8.1.2.6 PTZ Tab

Table 32 presents typical settings of the camera. Parameters, that depend on camera **Type** and **Model**, are described in Table 33.

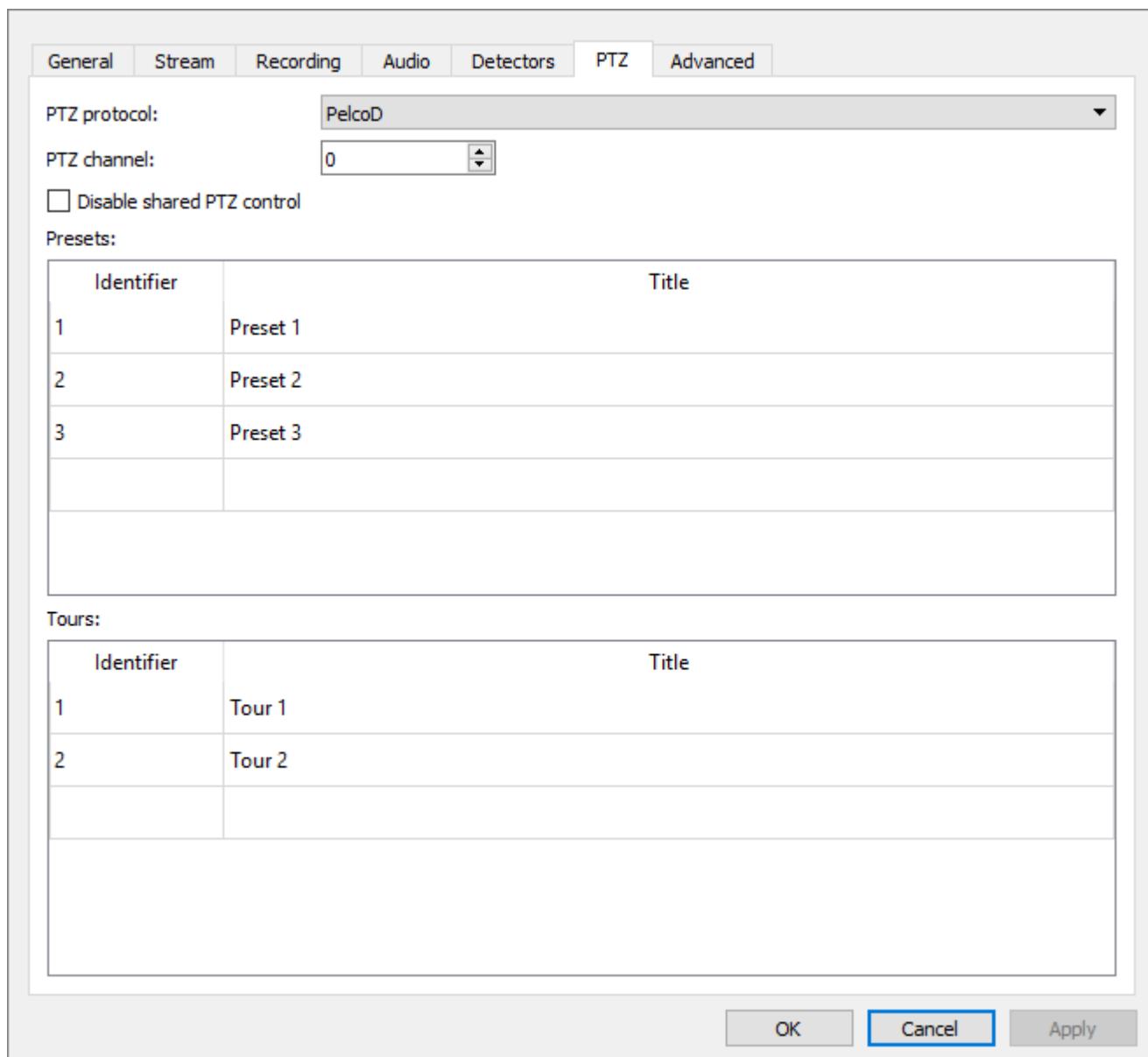


Figure 124. Camera object settings window. PTZ Tab

Table 32. Camera object settings. PTZ Tab

Parameter	Description
PTZ protocol	Select from the drop-down list the PTZ Protocol supported by the current <i>Camera</i> model. Note. The parameter is available depending on the type of the parent <i>Video Capture Device</i> object.
PTZ channel	Select the PTZ channel number.

Parameter	Description
Disable shared PTZ control	Select telemetry control mode (see Shared Telemetry Control and Exclusive Telemetry Control).
Presets (table of pre-installed settings)	
Note. Obsolete block of settings. Is used only for cameras that do not support automatic update of their own settings in SecurOS. For detail contact Technical Support Team.	
Identifier	Type ID of the preset, preliminary specified in the camera settings with the help of web interface.
Title	Specify preset name. List of the specified presets will be displayed in the <i>Media Client</i> PTZ control panel.
Tours (table of tours)	
Note. Obsolete block of settings. Is used only for cameras that do not support automatic update of their own settings in SecurOS. For detail contact Technical Support Team.	
Identifier	Type ID of tour, preliminary specified in the camera settings with the help of web interface.
Title	Specify tour name. List of the specified tours will be displayed in the <i>Media Client</i> PTZ control panel.

Table 33. Optional PTZ tab parameters

Parameter	Description
Tour type	Select the type of tours, that will be available for this <i>Camera</i> . Possible values: <ul style="list-style-type: none"> • By presets — tours, that are pre-defined in camera settings with the help of web-interface. • Recorded — tours, that are recorded on camera by user with the help of web-interface.
Serial port number	Select serial port, that will be used to control camera PTZ. Range of values: [1; 16]. Default value is 1.

7.8.1.2.7 Advanced Tab

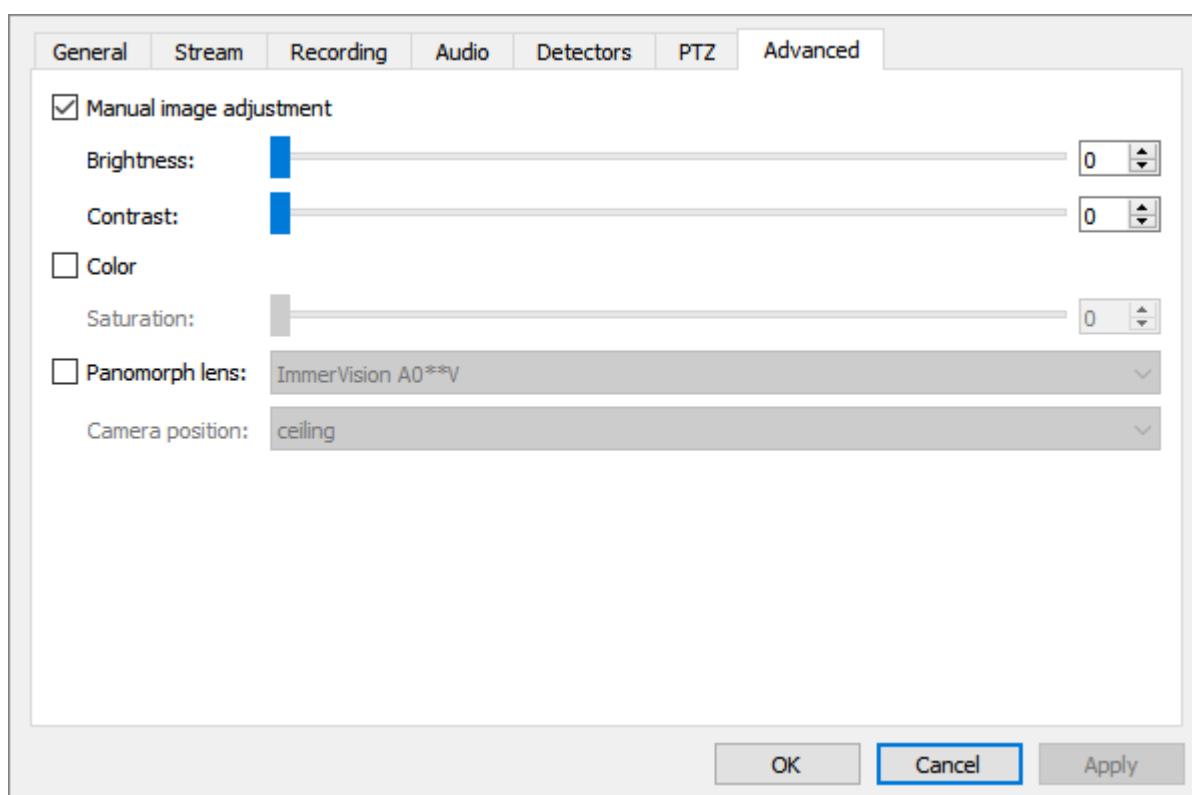


Figure 125. Camera object settings window. Advanced Tab

Note. The Axis M3204 parameter set is presented in figure 125.

Depending on the *Camera* model the list of available parameters may vary. This section describes the following parameter sets:

- Additional parameters of the ONVIF Camera (Video Capture Device with the ONVIF Type);
- Additional parameters of the SecurOS Motus Camera (Video Capture Device with the SecurOS Motus Type);
- Additional parameters of the Virtual Camera (Video Capture Device with the Virtual Type);
- Other additional parameters.

Table 34. Additional parameters of the ONVIF Camera (Video Capture Device with the ONVIF Type)

Parameter	Description
Manual exposure control	Select the checkbox to manually set camera's exposure. Note. If this option is enabled the exposure can not be controlled from SecurOS operator interface.
Exposure Time	Available only if the Manual exposure control is selected. Possible values: [0 ; 100]. Default value: 50.
Gain	Available only if the Manual exposure control is selected. Possible values: [0 ; 100]. Default value: 50.

Parameter	Description
Iris	Available only if the Manual exposure control is selected. Possible values: [0; 100]. Default value: 50.
Brightness	Select this checkbox to manually set the image brightness. Possible values: [0; 100]. Default value: 50.
Saturation	Select this checkbox to manually set the image saturation. Possible values: [0; 100]. Default value: 50.
Sharpness	Select this checkbox to manually set the image sharpness. Possible values: [0; 100]. Default value: 50.
Contrast	Select this checkbox to manually set the image contrast. Possible values: [0; 100]. Default value: 50.
White Balance	Select the checkbox to manually set the white balance of the frame.
Rgain	Available only if the White Balance is selected. Controls the amount of red color in the image. The higher the value the more intensively red color is displayed. Possible values: [0; 100]. Default value: 50.
Bgain	Available only if the White Balance is selected. Controls the amount of blue color in the image. The higher the value the more intensively blue color is displayed. Possible values: [0; 100]. Default value: 50.
Backlight Compensation	Select the checkbox to engage the backlight compensation algorithm.
Level	<p>Available only if the Backlight Compensation is selected. Defines how strong the backlight compensation will be. Possible values: [0; 100]. Default value: 50.</p> <hr/> <p>Note. In case the camera does not support level control the backlight compensation will be controlled by rules defined by the manufacturer.</p>
WDR mode	<p>Select this checkbox to enable the WDR feature.</p> <hr/> <p>Note. WDR feature (Wide Dynamic Range) allows to obtain the image of high quality at scenes with significant illumination fluctuations.</p>
Level	<p>Available only if the WDR mode is selected. Defines how strong the WDR influence will be. Possible values: [0; 100]. Default value: 50.</p> <hr/> <p>Note. In case the camera does not support level control the WDR feature will be controlled by rules defined by the manufacturer.</p>
IR filter mode	<p>Select the checkbox to define the IR filter operation mode. Possible values:</p> <ul style="list-style-type: none"> • auto on/off (default value);

Parameter	Description
	<ul style="list-style-type: none"> • always on; • always off.

Table 35. Additional parameters of the SecurOS Motus Camera (Video Capture Device with the SecurOS Motus Type)

Parameter	Description
Use SecurOS Motus built-in controller	<p>Select this checkbox to control camera's light, zoom and focus.</p> <hr/> <p>Note. If not selected all of the following parameters are disabled.</p>
	<p>Warning! To control a camera with the help of the Motus controller it is necessary to set the Pan/tilt/zoom parameter of the <i>Camera</i> object settings to Use (see General Tab). Otherwise it will be impossible to control the camera.</p>
Device control IP address	Specify IP address of the Motus controller that will be used to control camera's illumination, zoom and focus.
User/Password	Specify user name and password to get access to control camera's illumination, zoom and focus.
Illumination mode	<p>Select the Illumination mode. Possible values:</p> <ul style="list-style-type: none"> • always on (default value) – when this value is selected all zones are illuminated constantly with specified level; • always off – when this value is selected the illumination of all zones are constantly turned off; • auto on/off – when this value is selected, the illumination turns on/off automatically depending on the actual light level in the zone (determined by the camera sensor). If actual light level is less than specified by the Day/Night shift level parameter illumination turns on for all zones with intensity specified for each ones.
Short/Middle/Long range	Specify illumination level for each zone (in %, in the range defined in the controller). For example, if the [15; 75] range is set in the controller settings and parameter is set to 40 then actual illumination level will be 39.
Day/Night shift level	Specify the threshold for automatic on / off illumination for the auto on/off mode.
Force camera night mode shift	Warning! Only for cameras with IR illumination.
Illumination control of SMT-LT357-IR Model (with IR lighting)	

Parameter	Description
Illumination control	Select the checkbox to control camera's IR lightning. Provide access to all parameters described below.
Day/Night mode	Defines the lightning source operation mode. Possible values: <ul style="list-style-type: none"> • auto on/off (default value); • day; • night.
Sensitivity	The option is available only when the Day/Night mode is set to Auto on/off. Defines the light sensitivity that controls switching between day and night modes. The higher the value the earlier the camera will switch to the night mode when it gets darker. Possible values: [0 ; 9]. Default value: 7.
Illumination level control mode	Select the mode by which the illumination level will be controlled. Possible values: <ul style="list-style-type: none"> • auto; • manual.
Short/Long illumination range	The option is available only when the Illumination level control mode is set to Manual. Defines the level of illumination at short/long range. Possible values: [0 ; 1000]. Default value: 500. Note. Zones illumination level control may be partially or fully unavailable for some camera models.

Illumination control of SMT-LT556-WL Model (with white lighting)

Illumination control	Select the checkbox to control camera's white lightning. Provide access to all parameters described below.
Illumination mode	Defines the lightning source operation mode. Possible values: <ul style="list-style-type: none"> • auto on/off (default value); • always on; • always off.
Sensitivity	The option is available only when the Illumination mode is set to Auto on/off. Defines the light sensitivity that controls switching between illumination modes. The higher the value the earlier the camera will turn the light on when it gets darker. Possible values: [0 ; 9]. Default value: 7.
Short/Long illumination range	Defines the level of illumination at short/long range. Possible values: [0 ; 1000]. Default value: 500. Note. Zones illumination level control may be partially or fully unavailable for some camera models.

Table 36. Additional parameters of the Virtual Camera (Video Capture Device with the Virtual type)

Parameter	Description
Enable synchronization	Select this checkbox to synchronize all video streams from all <i>Cameras</i> children to given <i>Video Capture Device</i> . After applying the settings, all video streams are combined into a single synchronization group. For this group a common time interval is searched and then the video from each <i>Camera</i> is played synchronously in a circle within this interval. If the common interval is not found the video is not synchronized.
Use interframe delays from file	Select this checkbox to play the video archive with the same interframe intervals with which this archive was recorded. The original interframe intervals will be exactly reproduced with each random playback of the archive. This mode is used to demonstrate changes in the operation of video analytics algorithms as they are improved. If this checkbox is not selected then interframe intervals will be calculated by the <i>Video Capture Device</i> automatically and will be different for each separate playback of the archive.

Table 37. Other additional parameters

Parameter	Description
Ignore qop (Quality of protection) parameter with auth value when using digest authentication	This checkbox affects the server response when digest authentication is used: <ul style="list-style-type: none"> • if selected, server response is calculated as follows: MD5 (HA1 : nonce : HA2); • if not selected and the qop="auth" is specified in the query, then compute the response as follows: MD5 (HA1 : nonce : nonceCount : clientNonce : qop : HA2). <p>Note. Directive qop="auth" is specified automatically by the RTSP server.</p>
Pixel format	Select from the drop-down list pixel format of the uncompressed video, which is supported by given model of the <i>Camera</i> . If selected value is not supported, video stream from given <i>Camera</i> will not be received. Warning! For a complete list of supported values, see the User's Guide for the selected <i>Camera</i> model.
Camera serial number	To receive in SecurOS video stream from required <i>Camera</i> , specify its serial number. This parameter is used when several cameras are connected to the <i>Computer</i> via USB 3.0.

Parameter	Description
Auto white balance	<p>Warning! Parameter is intended only for those Basler Pylon GigE (Area Scan Camera) and Basler Pylon USB 3.0 camera models, that have auto white balance option in their own settings. Otherwise, using this parameter may cause <i>Camera</i> malfunction in SecurOS.</p> <p>This option allows to compensate for differences in color, that appear when camera operates in conditions of volatile illumination. Select the checkbox and select one of white balance adjustment mode:</p> <ul style="list-style-type: none"> • Off – auto white balance is turned off; • Once – white balance adjusts automatically until the optimal value for current illumination is reached. After reaching such value the option will be automatically set to Off mode, and obtained value will be permanently used for all frames in future; • Continuous – while balance will be automatically corrected for every frame until mode is changed to Off or Once.
Autogain	Select this checkbox to control the gain automatically. By default is not selected.
Gain	Set the gain of the camera output signal.
Frame width, px	Set width of the frame (in pixels) if it is not required to use maximum possible matrix horizontal resolution.
Frame height, px	Set height of the frame (in pixels) if it is not required to use maximum possible matrix vertical resolution.
Exposure time, μs	Specify a maximum exposure time of the frame (in microseconds). This parameter defines brightness of a frame: the more this value is, the brighter will be the image.
Automatic center align by X	Select this checkbox to automatically center the frame horizontally. By default is not selected.
X-offset, px	Set horizontal offset for a frame (in pixels). This parameter sets offset of top left corner of the frame regarding to top left corner of the matrix in case if horizontal frame size is smaller than maximum acceptable (see Frame width parameter).
Automatic center align by Y	Select this checkbox to automatically center the frame vertically. By default is not selected.
Y-offset, px	Set vertical offset for a frame (in pixels). This parameter sets offset of top left corner of the frame regarding to top left corner of the matrix in case if vertical frame size is smaller than maximum acceptable (see Frame height parameter).
Codec	Select codec, that corresponds to required camera video stream.
Codec for recording	Select codec, that will be used when writing video to archive.

7.8.1.2.8 Multicast

Video from surveillance camera can be transmitted to the operator's workstations in two modes:

- unicast-translation – frame is translated on the **Camera**→**Video Server**→**Operator Workstation** route. In this mode number of identical video streams transmitted from the *Video Server* to the *Operator Workstation* is equal to number of operators, who watch the camera.
- multicast-translation – in this mode a single video stream is transmitted into network on route from camera to operator workstation. Further this stream is translated via network hardware to the *Video Server* and non-limited number of the *Operator Workstations*.

Benefits of multicast-translation

Use of multicast-translation allows to get the following benefits when it applied in the network with large number of operators:

- significantly reduce charges for purchasing and operating required network hardware;
- reduce video server work-loading.

For example, there are several *Video Servers* within SecurOS network and each server is connected with 100 *Cameras*. Each *Camera* translates the 5 Mbps video stream. There are 40 *Operator Workstations* within the network and each operator watches 20 *Cameras*.

Let's analyze the worst case, when all 40 operators watch *Cameras*, connected to the same *Video Server* at the same time. In this case we have the following result:

- **Unicast Mode**

- Total *Video Server*'s input stream will be $100 \times 5 = 500$ Mbps. To work with such video stream only one 1 GE network interface is enough.
- Total *Video Server*'s output stream will be $20 \times 5 = 4000$ Mbps. To work with such video stream one 10 GE interface on the video server and the same 10 GE interface on the network hardware are required yet. For now, such equipment is significantly more expensive than widespread 1 GE equipment.
- In addition, *Video Server*'s CPU must have enough reserve of performance.

- **Multicast Mode**

- Total *Video Server*'s input stream is the same (500 Mbps). To work with such video stream only one 1 GE network interface is enough.
- There is no output video stream on the *Video Server*. Thus, 1 GE network interface on the video server and the same 1 GE interface on the network hardware that are already available is enough.
- Extra performance of the *Video Server*'s CPU to translate video stream into the network is not required, too.

Conditions for use multicast-translation

Multicast-translation is expedient for using under the following conditions:

- network hardware support IGMP Version 3;
- network hardware is configured to use multicast and provides video delivery to any client, connected to the SecurOS network;
- bandwidth of any network segment excludes losses of UDP packets when translating video.

Additional Information

The loss of UPD packets results in significant frame rate reduction, and it will look like "jumps" and "jerks" during video playback.

Otherwise use of multicast mode is not justified and will not provide an expected result.

Setting Up Camera

Warning! In current Release multicast mode is supported only for ONVIF protocol.

To enable multicast translation specify the following parameters on the **Stream** tab in the *Camera* object settings window (see Figure 126):

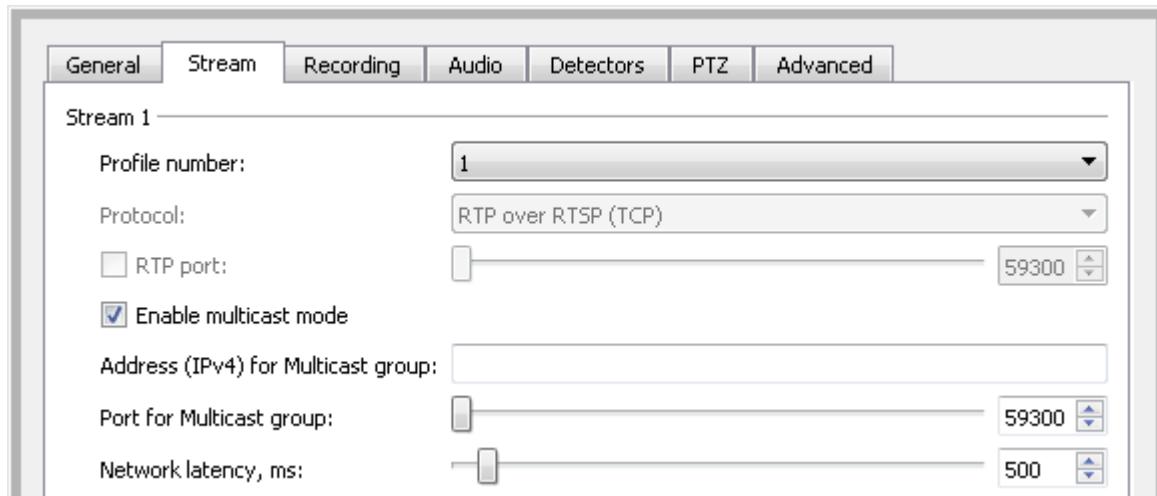


Figure 126. Setting up multicast translation mode

1. **Enable multicast mode.**
2. **Address (IPv4)** and **Port** for multicast group.

Warning! Each specified **Address (IPv4)/Port** pair of values must be unique. It is system administrator responsibility to provide and control this uniqueness.

7.8.1.2.9 Configuring Panoramic Cameras

Initial image of the panoramic camera can be dewarped to a form suitable for the perception of the operator. For such dewarping different algorithms appropriate to the **Type** and **Model** of the camera. Configuring panoramic camera supposes a selection of the correct algorithm that allow to view dewarped image obtained by cameras equipped with different types of lenses.

Configuring is performed in the **Advanced** tab (see Figure 127). Depending on camera's **Type** and **Model** the following configuring options are possible:

- **Configuring cameras equipped with panomorph lens supporting ImmerVision technology;**
- **Configuring other cameras equipped with panoramic lens.**

Possibility to control supported panoramic cameras with the help of electronic PTZ is switched on automatically after configuring is finished.

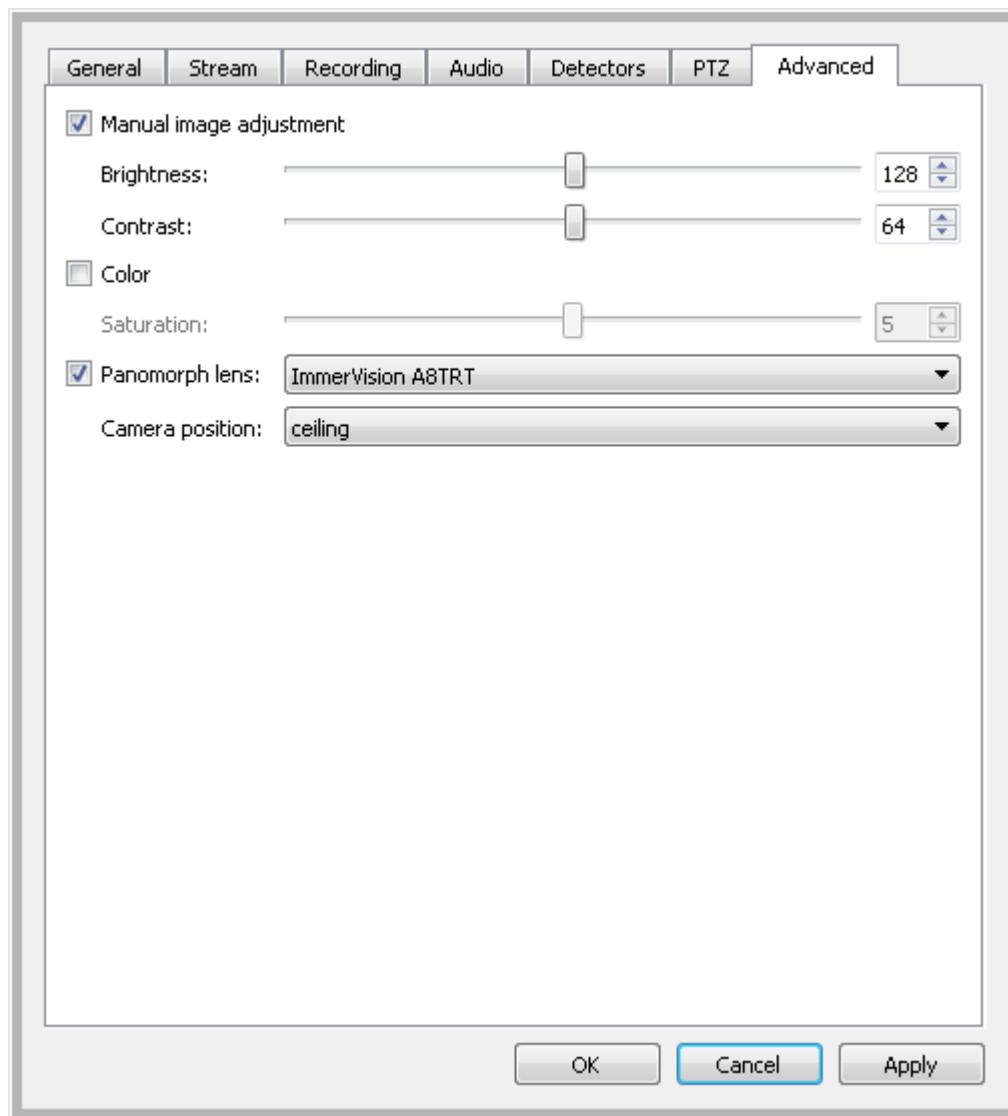


Figure 127. Advanced tab for the cameras with panoramic lenses

Configuring cameras equipped with panoramorph lens supporting ImmerVision technology

To configure camera do the following:

1. Select the **Panomorph lens** checkbox, select model of the used lens in the list on the right.
2. Choose camera position from the **Camera position** list.

Configuring other cameras equipped with panoramic lens

Choose camera position from the **Camera position** list.

7.8.1.3 Defocus detector

This object is designed to specify parameters, used by the *Camera* defocus determination algorithm.

Parent object — **Camera**.

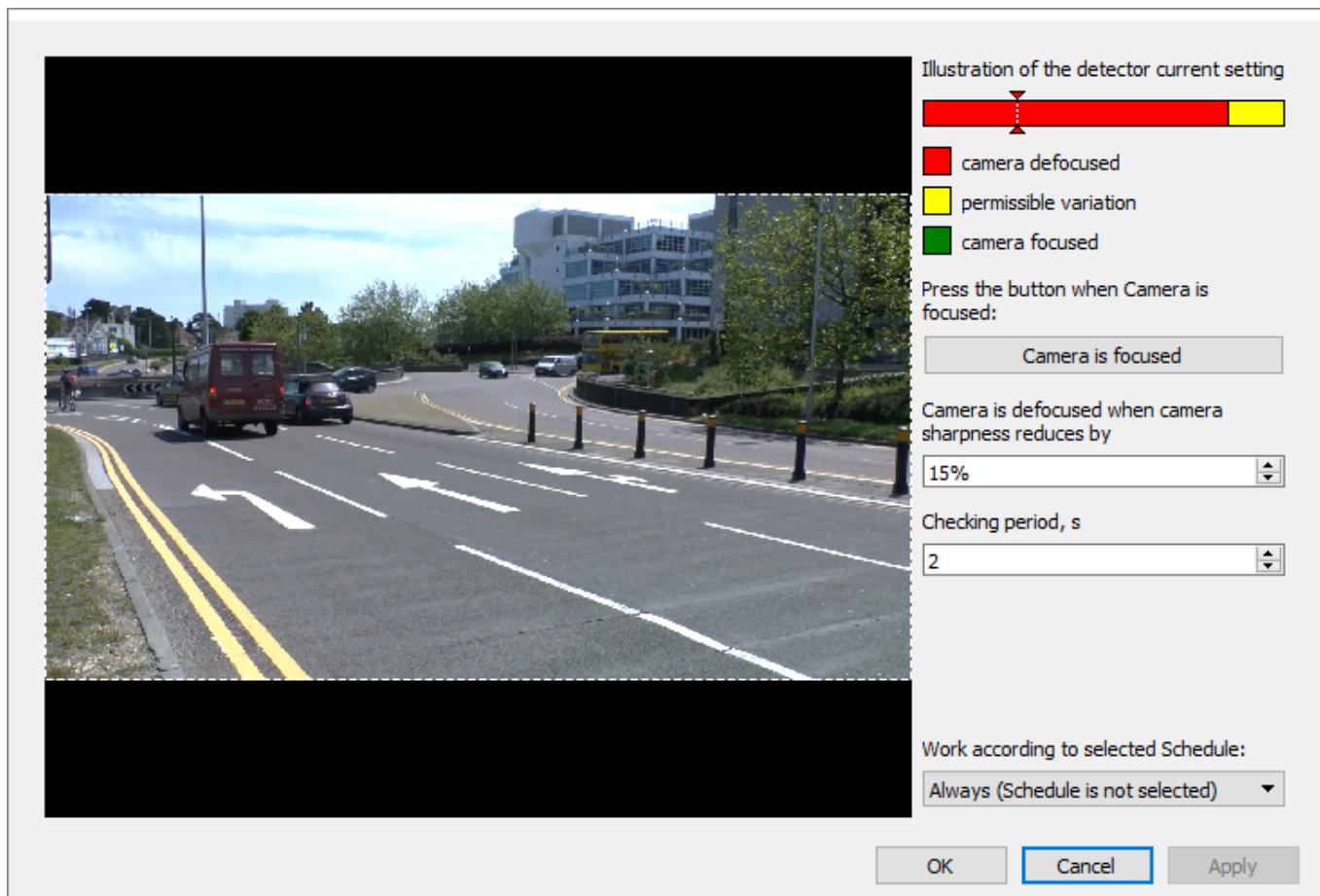


Figure 128. Defocus detector object settings window

Table 38. Defocus detector object settings

Parameter	Description
Detection area	An area, located in the left part of the object settings window. The detection area is represented by a rectangular area, bounded by a white dotted line, in which a video stream is displayed without distortion. Sharpness of the image inside the detection area is considered a reference quantity. To change the area size place the mouse cursor over any side of the rectangle, then move the cursor in the required direction holding the mouse button. To move the detection area, click inside it and drag rectangle to the new location. By default, the detection area is set to the whole frame size.
Camera is focused	When detection parameters are specified, click this button to store reference image.
Camera is defocused when camera sharpness reduces by	Deviation of the current image sharpness from the sharpness of the reference image, in percent. If exceeded, the camera is considered to be defocused. When the specified value is exceeded, then appropriate event is generated (see SecurOS Programming Guide).
Checking period	Camera defocus checking period, in seconds. Range of values: [1;120].

Parameter	Description
Work according to selected Schedule	Select the Schedule if the defocus detector should work in the specific time range. If option is not selected, defocus checking is always performed.

Recommendations for choosing the detection area and configuration of the other detector parameters are shown below (see [Fine Tuning Recommendations](#)).

7.8.1.3.1 Fine Tuning Recommendations

When specifying a detection area it is recommended to comply with the following requirements:

1. Image inside detection area must be static as much as possible.
2. Image inside detection area must contain max possible number of small objects, having sharp borders.
3. Shading of the image inside detection area must be minimized.

For the detection areas that will normally not be shaded, it is recommended to specify a short **Checking period**. This allows to capture short-time shading caused by sabotage.

When specifying a **Schedule** it is recommended to use such a time period, when changing of lighting conditions inside detection area is minimum.

If the detection area and other parameters are specified correctly, then the indicator of the detector's current settings will look as follows (see Figure 129):

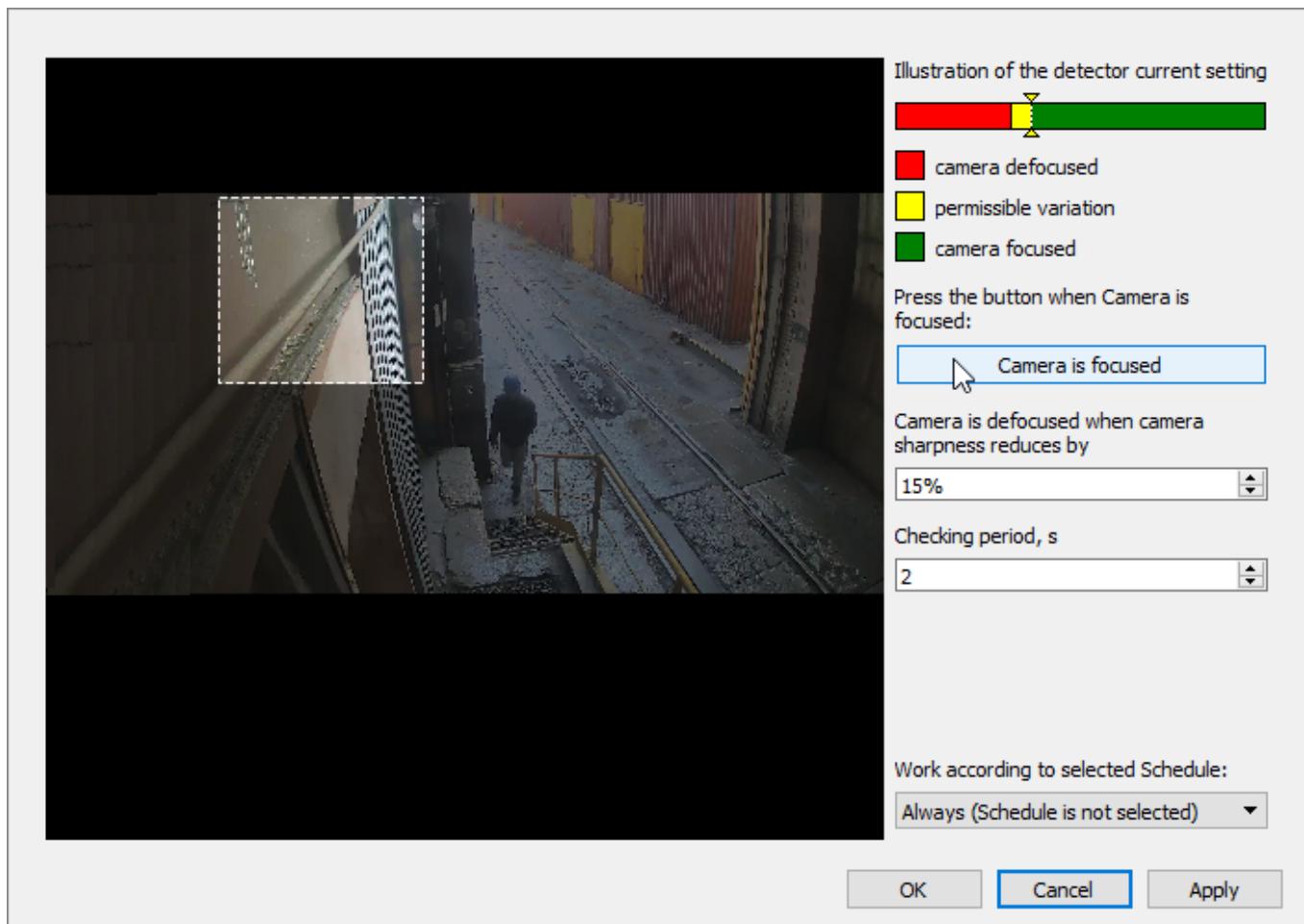


Figure 129. Adjustment of the Defocus Detector

7.8.1.4 Layout

This object is used to create a custom layout of the *Media Client*'s video page – a form, dimensions and arrangement of cells to display video from the *Cameras*. To use created custom layouts, select the required ones on the **Layouts** tab (see **Media Client** section). Similar to system layouts, using custom layouts it is possible to move cameras around to the any cell of the layout.

Parent object – *Security Zone\Layouts & Views* group.

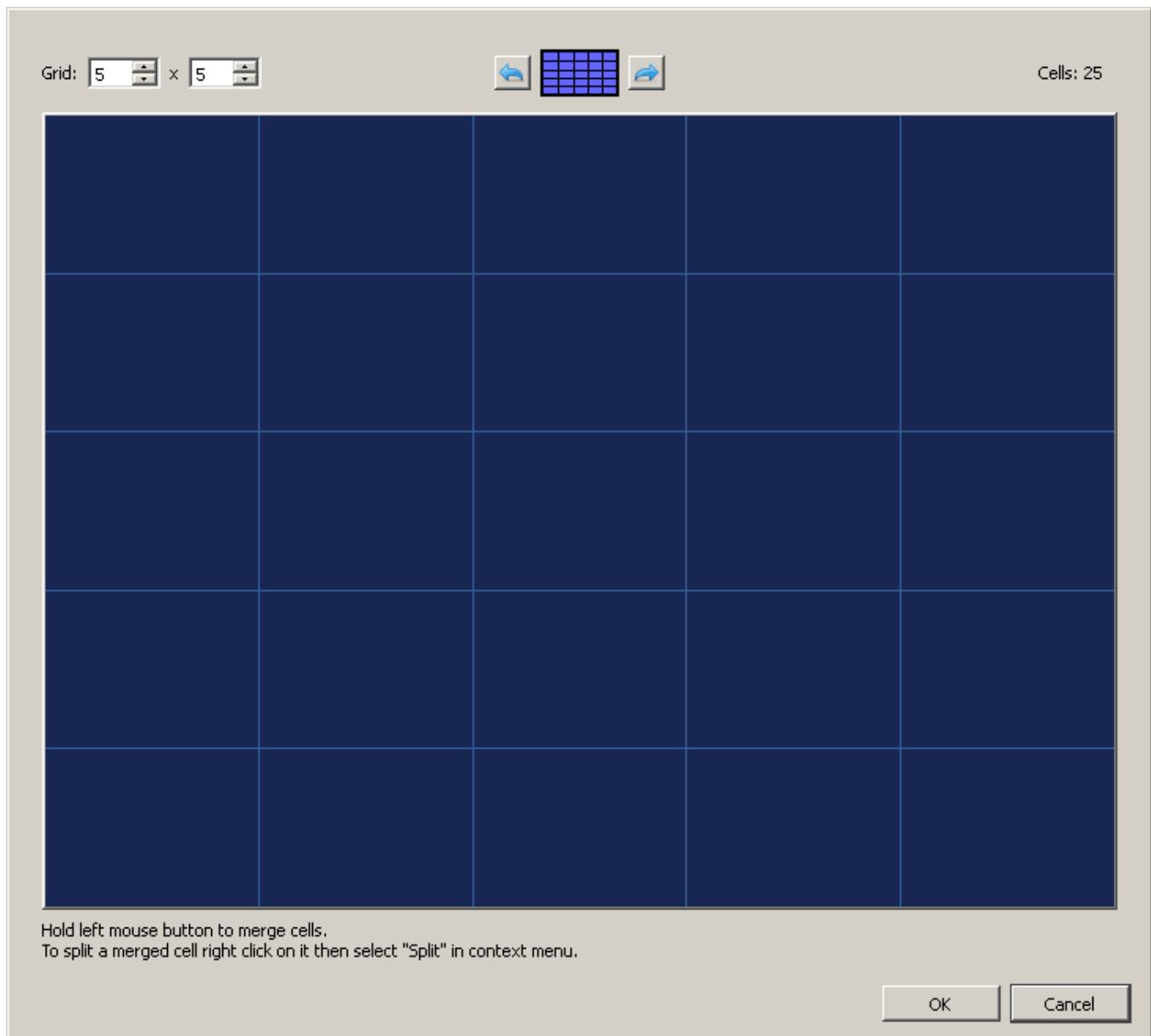


Figure 130. Layout object settings window

Table 39. Layout object settings

Parameter	Description
Grid	A grid defines the basic model of the <i>Media Client's</i> working area (i.e. <i>Layout</i>), which contains a specified number of cells vertically and horizontally, accordingly. When creating/editing a layout, any number of adjacent cells can be merged into one cell of larger size. This large cell can again be split to the appropriate number of basic cells.
Cells	Information string. Displays the total number of cells currently displayed on the layout. Updates automatically when the layout's grid numbers are changed. Max number of cells in a layout is 250.
Buttons	

Parameter	Description
	<p>View buttons (Previous view, Next view) to look at the intermediate versions of the layout's model.</p> <hr/> <p>Note. Intermediate versions of the layout are stored in the SecurOS's RAM and are accessible to the administrator during current session of creating/editing the object.</p>
OK (Cancel)	Saving current layout and closing object settings window (Closing object settings window without saving changes).

7.8.1.5 View

View represents a combination of several *Cameras*, *Microphones* or *Cameras* and *Microphones* simultaneously, grouped into a single object that is controlled by a *Media Client*. Visually *View* includes *Media Client's Working area*, where *Cameras* are displayed, and *Microphone Panel*. Each *View* is a separate object of a *Media Client*, that allows operator quick access to information of interest, which is provided by preliminary specified group of video and audio sources.

Parent object – *Security Zone\Layouts & Views* group.

Object has no settings to configure.

Setting up *Views* to use them on the *Operator Workstation* is performed by system administrator with the help of *Media Client* (see [About Views](#)).

Setting up *Media Client* to work with *Views* is performed in the its [Views](#) tab.

7.8.1.6 Zone

This object represents a single detection zone of the motion detector (see [Working Principles of Motion Detection Zones](#) for detailed information). One default zone called *Main* is created automatically when a *Camera* object is created and covers the whole visible area of the *Camera* cell.

When configuring a *Zone* object, take into account the following parameters:

- **Contrast** slider defines minimal moving object contrast. Top position of the slider means the zone would detect motion only if a moving object differs greatly from the surroundings. Bottom position of the slider means the zone would detect motion even if a moving object slightly differs from the surroundings.
- **Size** slider defines minimal moving object size. Top position of the slider means the *Zone* would detect motion of large objects only. Bottom position of the slider means the *Zone* would detect motion of small objects.

Note. The values of the **Contrast** and **Size** sliders should be set by practical consideration.

- **Alarming** flag should be active to generate an alarm on the camera upon any motion detection

within the zone. If this flag is not checked, the zone is considered informational.

- **Armed always** flag should be active to have the zone always armed, regardless of the armed/disarmed state of other zones on the same camera.
- **Save movement coordinates (enables Smart Search)** checkbox should be activated if it is necessary to save alarm object coordinates into the database.

Note. Several **Zone** objects within the same parent object are combined into the **Motion Detector** logic group in the Object Tree.

Parent object – *Camera\Image zones* group.

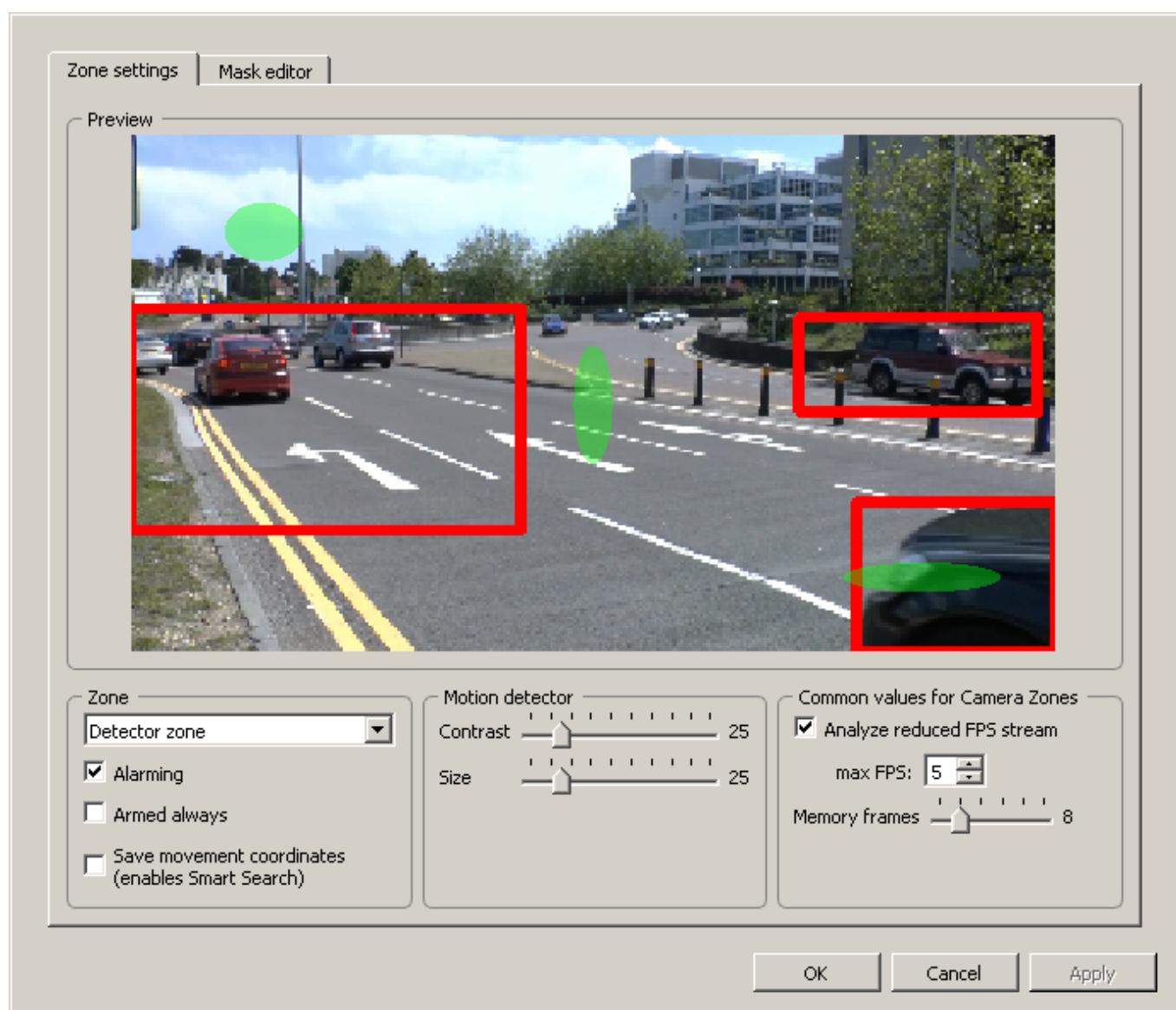


Figure 131. Zone object settings window

Table 40. Zone object settings

Parameter	Description
The Zone settings tab	

Parameter	Description
Zones	A <i>Zone</i> can be represented with one of the following types: <ul style="list-style-type: none"> • Detector zone – intended for motion detection in selected area of the <i>Camera</i> image; • Blackened zone – is used to hide part of the <i>Camera</i> image area (privacy mask); • Generic zone – stores information about zone arrangement. <p>Warning! Alarming, Armed always, and Save movement coordinates (enables Smart Search) parameters are available for editing only if the Zone type parameter is set to Detector zone.</p>
Alarming	Enable this option to treat motion detection within this zone as an alarm (camera will enter alarmed state, recording will be started automatically, etc.). If this option is selected then the Save movement coordinates (enables Smart Search) option will be available. If you clear this option, the zone will be treated as "informational": no predefined actions will be performed, the <i>Zone</i> object will generate events upon detection start and end, thus allowing you to program custom reactions via macros or scripts.
Armed always	Select this option to keep armed mode for camera. Operator won't be able to disarm this zone.
Save movement coordinates (enables Smart Search)	Select this checkbox if it is necessary to save alarm object coordinates into the SecurOS database. If the checkbox is selected, alarm data will be recorded to the <i>fsindex</i> database (detection of <i>Alarms</i> starts after the camera is armed), which in turn, further allows one to search for specific <i>Alarm</i> criteria. Warning! All records that indicate <i>Alarm</i> start and stop (in microseconds) will be registered in the SecurOS database, assuming the default PostgreSQL database is used. In case of other databases, records with <i>Alarm</i> times will not be recorded and searching will be impossible. <hr/> <p>Note. Alarm time intervals are registered regardless of archive existence for that time. It is implied that the camera writes video constantly or on motion detection.</p>
Motion detection	
Contrast	Move slider to specify detected object contrast sensitivity. Boundary values: 10 – even low-contrast objects will be detected; 99 – only objects with high contrast will be detected.

Parameter	Description
Size	Move slider to specify detected object size sensitivity. Boundary values: 10 — even smallest objects will be detected; 99 — only large objects will be detected.

Common values for Camera Zones

Analyze reduced FPS stream, max FPS	Select Analyze reduced FPS stream checkbox if it is allowed to use stream with reduced FPS when detecting motion. Specify, if necessary, maximum frames per second value sufficient to detect motion (max FPS parameter). Note. The stream is reduced by I-frames. If the value specified in the max FPS parameter is less than the result value of the initial frame rate reduction then the I-frames themselves are further reduced. By default the checkbox is not selected, and the max FPS parameter is disabled. After the checkbox is activated, the range of max FPS parameter values is [1; 30].
Memory frames	Set the number of last camera frames used for motion analysis. If there is not enough frames then the motion detection procedure is not started. Possible values from 4 to 128 (frames). Default value — 8.

The Mask editor tab (see figure 132)

Video	Area to display camera zones.
Fill all	Click the button to fill the whole frame by a mask.
Clear all	Click the button to clear the camera mask.
Show all zones	Click the button to display all camera zones.
OK (Cancel)	Exit settings with (without) saving.

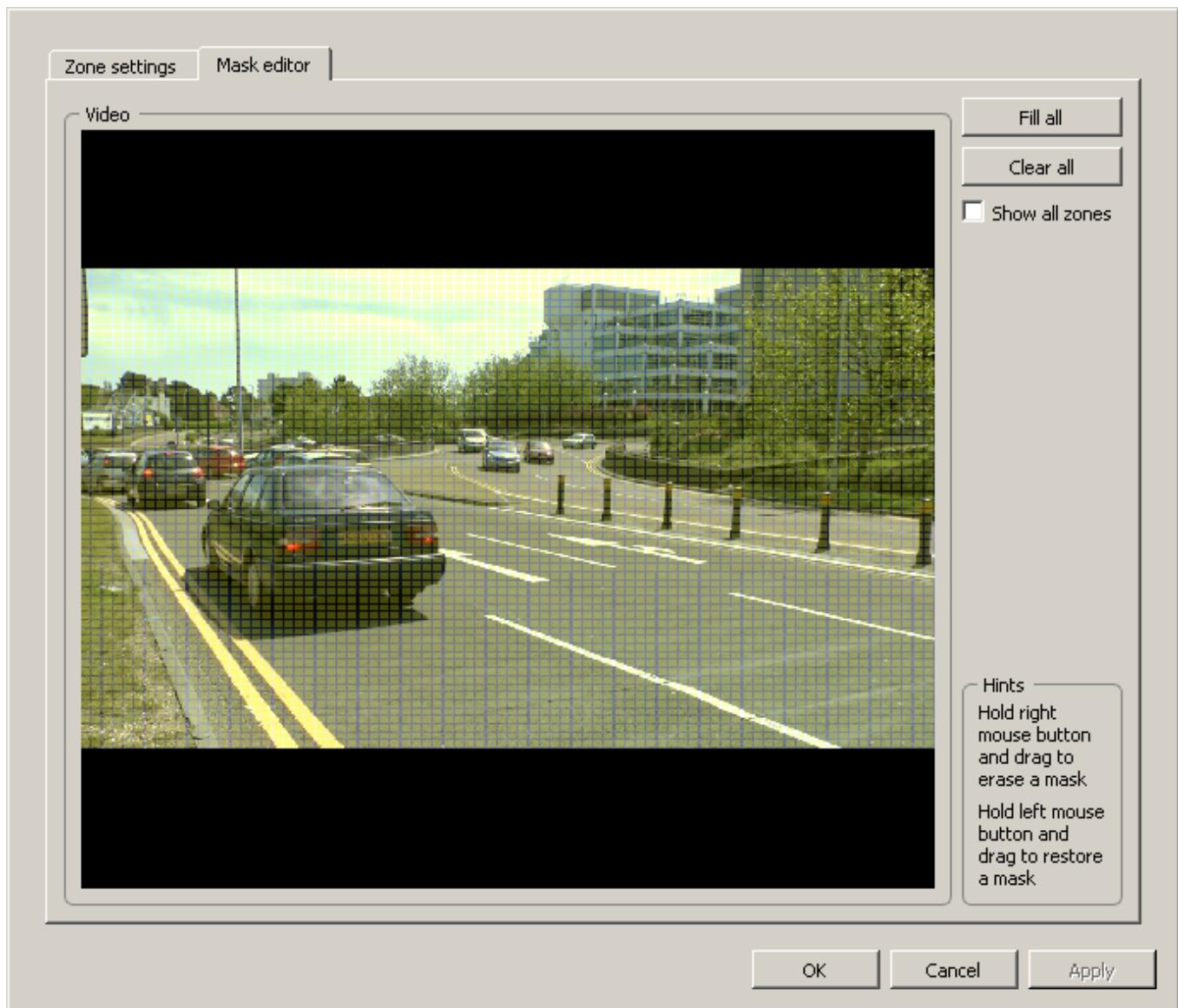


Figure 132. Zone object settings window. Mask editor

To edit zone mask:

1. Click the **Mask editor** tab on the *Zone* object property window.
2. Draw a rectangle inside the camera cell holding the right mouse button, then releasing it. This part of the camera screen would be excluded from the zone.
3. Draw some rectangles inside the camera cell holding the left mouse button, then releasing it. This part of the camera screen would be added to the zone.

7.8.1.7 Light Detector

This object represents the detector of contrast between inner and outer zones.

Parent object – **Camera**.

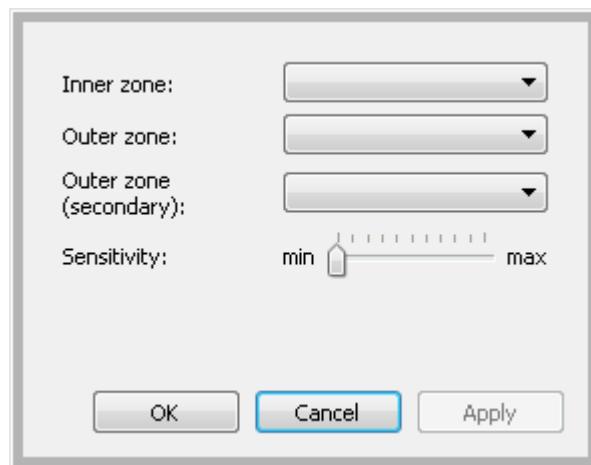


Figure 133. Light Detector object settings window

Table 41. Light Detector object settings

Parameter	Description
Inner zone	Select from the list a <i>Zone</i> object corresponding to the inner zone.
Outer zone	Select from the list a <i>Zone</i> object corresponding to the outer zone.
Outer zone (secondary)	Select from the list a <i>Zone</i> object corresponding to the secondary (additional) outer zone for checking light level by comparison with two independent zones.
Sensitivity	Move slider to specify detection light sensitivity. Boundary values: min – even smallest light difference will be detected; max – only high light difference will be detected.

7.8.1.8 Archive Converter

This object is used to get video/audio archives from all the video servers of the system and convert them to ASF, AVI, Evidence and ISS (obsolete) formats.

Warning!

1. If the export start period does not fit within the i-frame time-stamp (accurate within milliseconds), then the actual export start time will be shifted to the first i-frame time-stamp inside the export period.
2. It is necessary to reserve enough free space on the hard drive of the computer where export will be performed.

Note. To play **quick converted** video It is recommended to use VLC media player.

Parent object – **Computer**.

Settings window appearance may differ depending on selected format (see figure 134 and figure 135).

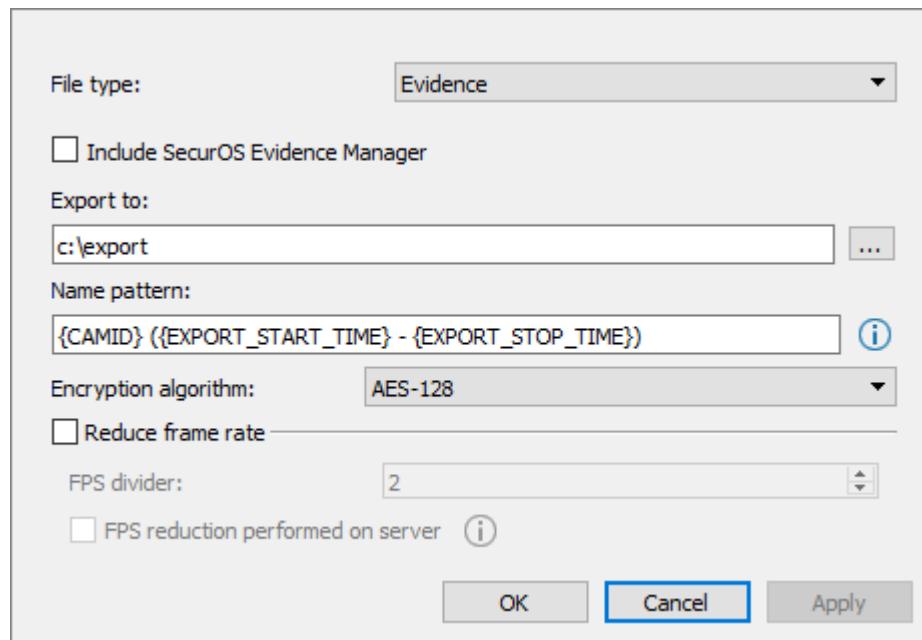


Figure 134. Archive Converter object settings window. File type - Evidence

Note. For the **ISS (obsolete)** format parameter settings window appearance is like for **Evidence** format.

Video Subsystem

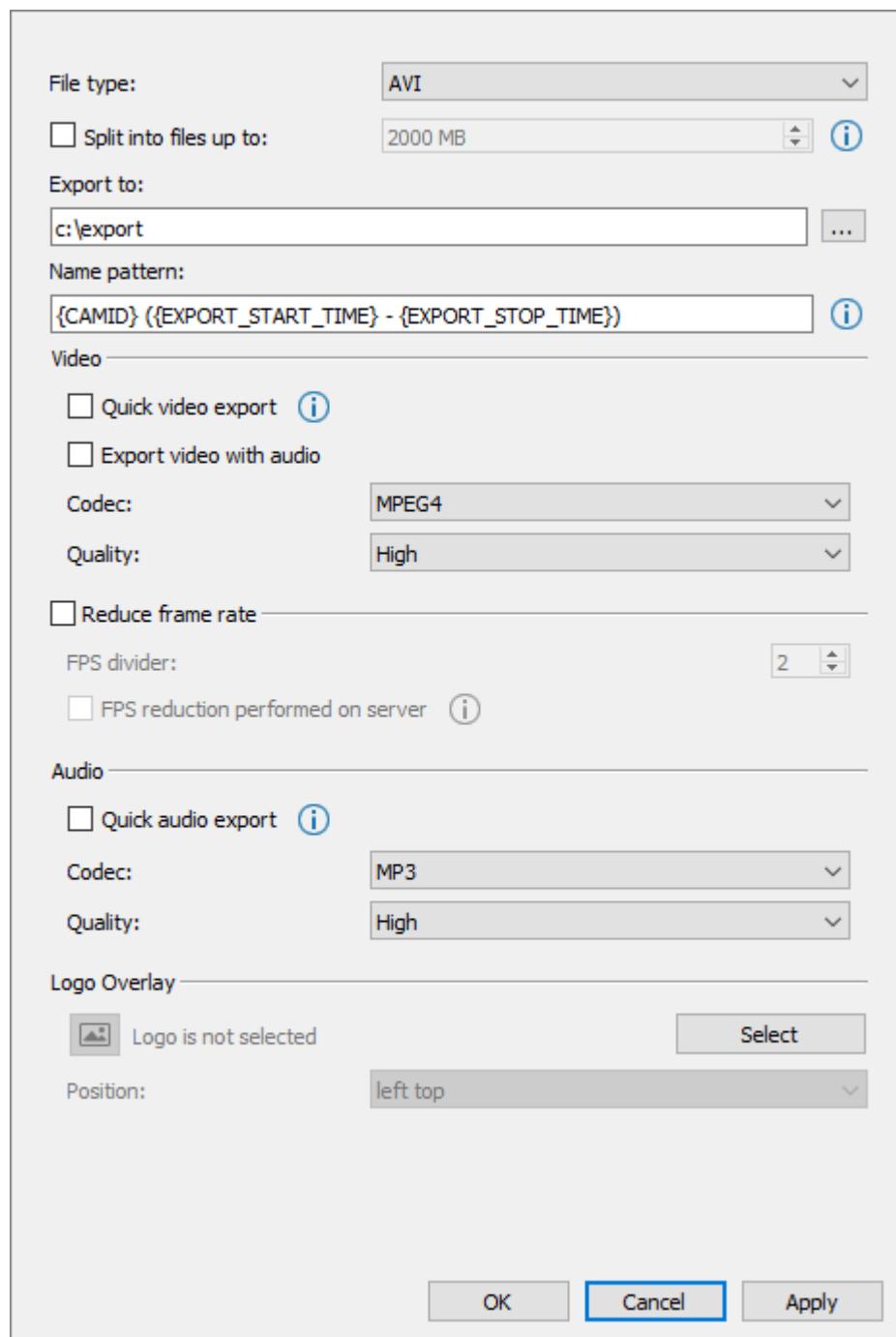


Figure 135. Archive Converter object settings window. File type - AVI (ASF)

Table 42. Archive Converter object settings

Parameter	Description
File type	Select format of converted file: ASF, AVI, Evidence or ISS (obsolete). Default value is - ASF. Notes: <ol style="list-style-type: none"> 1. The Evidence format is used to export files encoded with ISS Native codec. Converted video can be only played with SecurOS Evidence Manager. 2. When exporting to Evidence format video from multiple <i>Cameras</i> can be saved into one file. 3. In Evidence format audio track is not being converted to resulting file.
Add SecurOS Evidence Manager	Tick this checkbox to attach SecurOS Evidence Manager application to the archive that will be created (see SecurOS Evidence Manager User Guide).
Split into files up to	Max size of each file created after the export. Default value is 2000 MB. Max value is 10000 MB. Warning! Some media players do not support AVI-files greater than 2 GB. When exporting to the AVI and ASF file formats archive can be split into several files regardless of the specified value of this parameter. Archive is being split automatically in the following cases: <ul style="list-style-type: none"> • Video archive contains frames with different frame resolution. When resolution is changed the new file will be created; • Quick export of the video/audio archive is performed (see Quick video export) and video/audio codec is changed; • Export is performed both from the <i>Primary</i> and <i>Long-term archive</i>. In this case two separate files will be created: one for all records from the <i>Primary archive</i> and another one for all records from the <i>Long-term archive</i>.
Export to	Specify directory to store converted files. Possible values: any available directory on the hard drives of the local machine. Optional parameter. If not specified, the file is saved into the c:\export directory. Note. When setting the parameter values it is possible to use file name macros (see Name pattern parameter description).

Parameter	Description
	<p>Template for the created file names. Can be formed by any combination of <i>valid characters</i> and <i>macro substitutions</i>.</p> <p>Optional parameter. Default value is {CAMID} ({EXPORT_START_TIME} - {EXPORT_STOP_TIME})</p> <p>Any characters, that are permitted to be used in the file names by used OS.</p> <p>The following macro substitutions are available (curly brackets are necessary):</p> <ul style="list-style-type: none"> • {SID} – export session number. Set to zero when the SecurOS application is started. • {CAMID} – camera identifier when exporting video or microphone identifier when exporting audio file only; • {CAMNAME} – camera name when exporting video or microphone name when exporting audio file only; • {COMPID} – computer (video server) identifier; <p>Warning! When converting archive of multiple <i>Cameras</i> to Evidence format, macro substitutions CAMID, CAMNAME and COMPID are being ignored.</p>
Name pattern	<p>• {SOURCE_TYPE} – type of the object, with the help of which the initial archive file has been created. Possible values:</p> <ul style="list-style-type: none"> – video – archive has been created by a <i>Camera</i> object; – audio – archive has been created by a <i>Microphone</i> object. <p>• {COMMENT} – export initiator comment, used when the conversion is started from a program or a bookmark is exported;</p> <p>• {CUR_YEAR} – current year in "YYYY" format;</p> <p>• {CUR_MONTH} – current month in "MM" format. Non-significant zero is omitted when displaying in the file name;</p> <p>• {CUR_DAY} – current day in "DD" format. Non-significant zero is omitted when displaying in the file name;</p> <p>• {CUR_HOUR} – current hour in "HH" format. Non-significant zero is omitted when displaying in the file name;</p> <p>• {CUR_MINUTE} – current minute in "MM" format. Non-significant zero is omitted when displaying in the file name;</p> <p>• {CUR_SEC} – current second in "SS" format. Non-significant zero is omitted when displaying in the file name;</p>

Parameter	Description
	<ul style="list-style-type: none">• {CUR_FRAC} — current millisecond in "sss" format. Non-significant zero is omitted when displaying in the file name;• {CUR_DATE} — current date in "YYYY-MM-DD" format (for example, "2011-12-31");• {CUR_TIME} — current time in "HH'MM'SS" format (for example, "23'05'06");• {EXPORT_START_TIME} — export period start time in "YYYY-MM-DD HH'MM'SS" format (for example, "2011-12-31 23'02'06");• {EXPORT_START_YEAR} — export period start year;• {EXPORT_START_MONTH} — export period start month number;• {EXPORT_START_MONTH_STR} — export period start month name;• {EXPORT_START_DAY} — export period start day;• {EXPORT_START_HOUR} — export period start hour;• {EXPORT_START_MINUTE} — export period start minute;• {EXPORT_START_SEC} — export period start second;• {EXPORT_START_FRAC} — export period start millisecond;• {EXPORT_STOP_TIME} — export period end time in "YYYY-MM-DD HH'MM'SS" format (for example, "2011-12-31 23'02'06");• {EXPORT_STOP_YEAR} — export period end year;• {EXPORT_STOP_MONTH} — export period end month number;• {EXPORT_STOP_MONTH_STR} — export period end month name;• {EXPORT_STOP_DAY} — export period end day;• {EXPORT_STOP_HOUR} — export period end hour;• {EXPORT_STOP_MINUTE} — export period end minute;• {EXPORT_STOP_SEC} — export period end second;• {EXPORT_STOP_FRAC} — export period end millisecond.

Parameter	Description
Encryption algorithm	Select encryption algorithm that will be used when converting video to the <i>Evidence</i> format. Possible values: <ul style="list-style-type: none"> • AES-128; • AES-192; • AES-256. <p>Warning! File will be encrypted only if password is set in the export task parameters to protect it from unauthorized access (see SecurOS Quick User Guide, Archive Export section).</p>
Video (video conversion parameters)	
Quick video export	Use original video codec and video quality during conversion. Makes it possible to increase conversion rate significantly and to reduce CPU load. Saving original codec and quality can only be applied to H.263, H.264, MJPEG and MPEG-4 formats. Note. When normal export is performed (Quick video export checkbox is not selected) video data is re-coded. Re-coding is performed on a single logic CPU's core.
Export video with audio	Option to convert video with synchronous audio file. By default it is selected. If not selected, then only video will be converted. This option does not affect audio files, recorded with the help of standalone (not linked to the camera) microphones. Note. Audio codec selected in Audio section will be used for conversion (see below)
Codec	Select video codec to convert archive video. Possible values: <ul style="list-style-type: none"> • MJPEG; • MPEG-4.
Quality	Select the quality of the converted video.
Reduce frame rate (use frame rate reduction during conversion). Select this checkbox to set frame rate reduction.	
FPS divider	Set the frame rate reduction factor. Range of values: [2 ; 100].
FPS reduction performed on server	Reducing the frame rate of the original video stream only by I-frames (see Frame Rate Reduction). Frame rate reduction of the archived video will be done on the <i>Video Server</i> where it is stored.
Audio (audio conversion parameters)	
Quick audio export	Use original audio codec and video quality during conversion. Saving original codec and quality can only be used for GSM, PCM and ADPCM formats. ADPCM format will be converted to the PCM format.

Parameter	Description
Codec	Select audio codec to convert archive audio. Possible values: <ul style="list-style-type: none"> • PCM; • WMA (for ASF container); • MP3 (for AVI container).
Quality	Select the quality of the converted video.
Logo Overlay (apply logo on the frame)	
Warning! When quick export is used (see Quick video export) logo is not applied.	
Select (button)	Click this button and use file manager to select logo file. Logo file must meet the following requirements: <ul style="list-style-type: none"> • file format — PNG; • max image dimension — 500x500 pix; • max file size — 500 KB. If the logo file is loaded successfully the appearance of the Logo Overlay block of parameters will be as shown in Figure 136. To view the loaded logo click on the  (Preview logo) button. To change the logo scale use mouse wheel. To remove the loaded logo click on the Delete button.
Position	Position of the logo on the frame. Possible values: <ul style="list-style-type: none"> • left top; • right top; • right bottom; • left bottom.

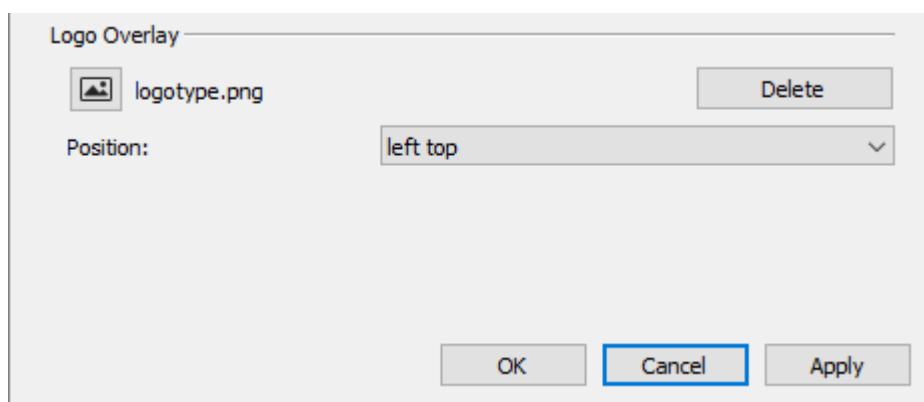


Figure 136. Appearance of the Logo Overlay block after logo is successfully loaded

7.8.1.8.1 Digital Signature

A digital signature with a certificate ensures that the signed file has not been replaced or edited after creation. The **PKCS#7 Signed data detached signature** standard is used for digital signature within SecurOS.

Possibility to sign files with the certificate is available on the *Computers* that have any Role (see [Computer](#)).

- Digital signature on the *Video Server* is available in case, if the *Archive Converter* configured in any [Operator Workstation Profile](#) is selected to perform export task;
- Digital signature on the *Operator Workstation* is available in case, if the *Archive Converter* configured on this [Operator Workstation](#) or in any [Operator Workstation Profile](#) is selected to perform export task.

After enabling the digital signature functionality, the *Archive Converter* will automatically sign audio and video files using the selected certificate.

Functionality is enabled directly on the *Operator Workstation* or the *Video Server*. Certificate, that matches the following requirements, must be installed in advance on operator's computer:

- The **Digital Signature** bit is asserted in the **Key usage** certificate's extension;
- The **Code signing** attribute is set in the **Enhanced key** certificate's extension.

Functionality enabling procedure and **Digital signature verification utility** are described in details in [SecurOS Quick User Guide](#).

Note. To check and demonstrate how the digital signature works one can use self-signed certificate created with the help of [Certificate Generator](#) utility.

7.8.1.8.2 Displaying Subtitles in Exported Video

Subtitles can be added on a live video frame in the following ways:

- when using the *SecurOS POS Module* (see [SecurOS POS User Guide](#));
- from the [VBScript program](#) the with the help of the ADD_SUBTITLES command (see [SecurOS Programming Guide](#)).

Added subtitles are stored both in *Primary* and *Long-term* archives.

When exporting to the AVI/ASF or Evidence file formats added subtitles are stored in archive only in case if initial video stream is being re-coded when export procedure is performed (the **Quick export** option is not selected). If the **Quick export** option is selected subtitles are not saved in the exported file. Subtitles themselves are the part of the exported video and cannot be hidden.

Additionally, the following data is always displayed on the frame:

- Camera ID – imposed in the left bottom corner of the frame;
- Frame Date and Time – imposed in the right bottom corner of the frame.

7.8.1.9 Archive Export Profile

Archive profile export is a special object designed for quick configuring the archive export feature on any *Operator Workstation* within the SecurOS network. Settings of this object are the same as the [Archive Converter](#) object excluding the **Export to** parameter.

When using *Archive export profile* then only *Media Client* is used to create an export task and execute an export procedure.

Just as when using the *Archive converter* an archive file can also be signed with the help of the certificate (see [Digital Signature](#)). In this case the file can be signed on any *Computers* without additional limitations.

Parent object – [Security Zone](#).

7.8.1.10 Archiver

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

This object is used to copy records of specified cameras from *Regular archive* to the *Long-term archive* in SecurOS format (see [SecurOS Archives](#)) and also to view files of the long-term archive in *Media Client*.

Parent object – [Computer](#).

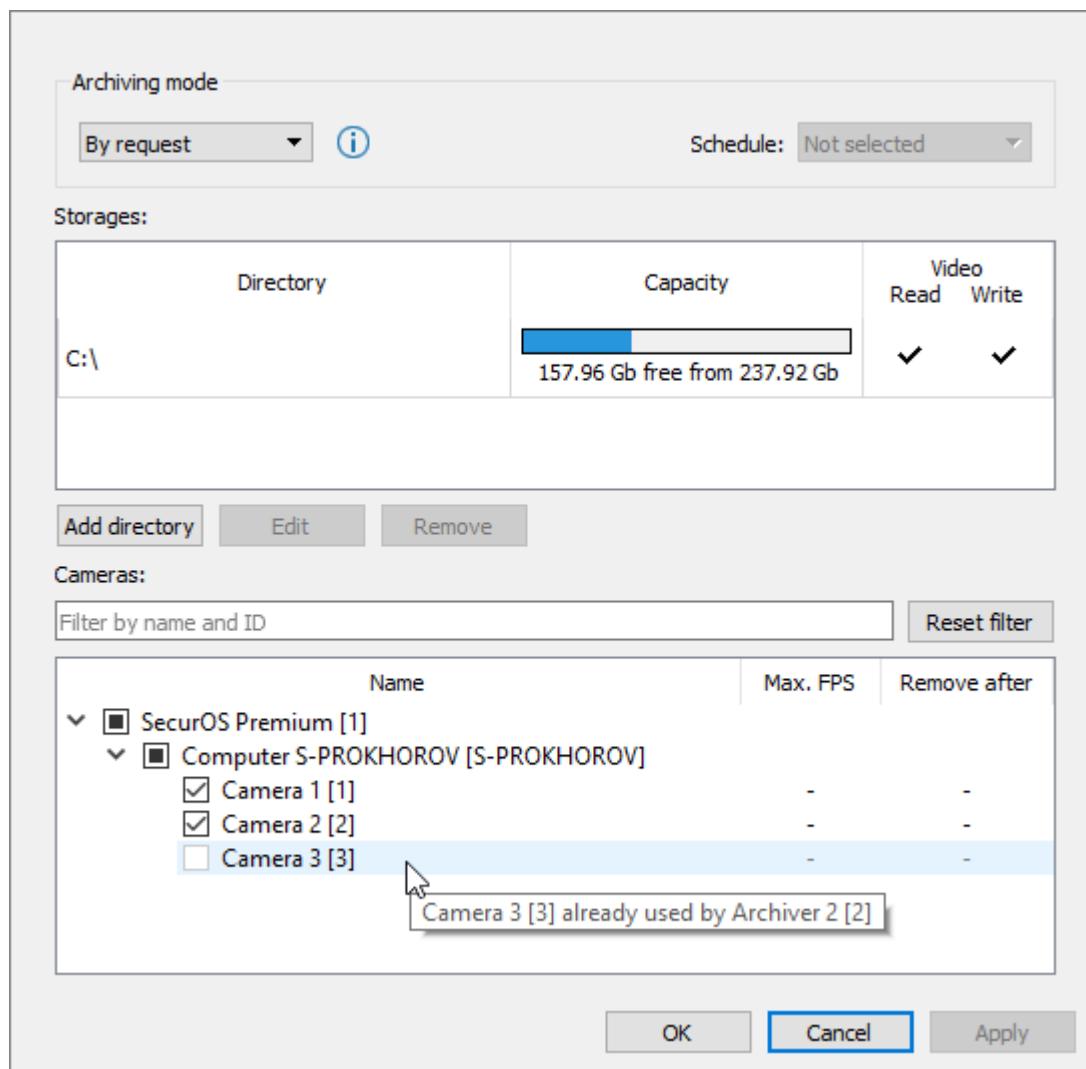


Figure 137. Archiver object settings window

Table 43. Archiver object settings

Parameter	Description
Archiving mode	

Parameter	Description
Archiving mode	<p>Select from the list the mode, that will be used to copy files of the <i>Regular archive</i>:</p> <ul style="list-style-type: none"> • By request – in this mode copying will start only when <i>Macro</i> will be executed or method, specified in the <i>VB/JScript program</i> body will be called. Only those records that match the command parameters will be copied (for the details see SecurOS Programming Guide, ADD_TASK command); <p>Warning! When upgrading SecurOS version 9.5 (and earlier) to 9.6 (and later) it is necessary to edit all used Macros and VB/JScript programs, that are used for <i>Long-term archive</i> creation.</p> <ul style="list-style-type: none"> • Continuous – in this mode all archives, existing at the moment for all <i>Cameras</i>, selected in the object settings, are copied continuously; • Scheduled – like Continuous mode, but copying is performed only during the validity of the selected time interval (see Schedule parameter below). <p>Note. Copying by schedule allows to select such time period for operation execution, when total load of the system is minimal. For example, night.</p>
Schedule	Specifies schedule to perform copying of the regular archive. Is enabled, if the Archiving mode parameter is set to Scheduled.
Storages (table)	
Directory	<p>List of drives available for writing and/or reading archive by given <i>Archiver</i>.</p> <p>Note. This table is empty when starting archiver for the first time.</p>
Capacity	Contains information about free space on the hard drive.
Mode	<p>Available mode of working with the specified directory. Possible values:</p> <ul style="list-style-type: none"> • Read only – directory is available only for reading. • Read and Write – directory is available both for reading and writing.
Buttons	
Add directory	Click on this button to add a new directory to store long-term archive. Details are described in Adding a directory for writing archive .
Edit	Click on this button to change parameters of the selected directory. Details are described in Editing a directory for writing archive .

Parameter	Description
Remove	Click on this button to delete selected directory. Details are described in Deleting a directory for writing archive .
Cameras	
Filter	To search <i>Camera</i> by name (part of its name) or by ID, type required characters in the field; only those <i>Cameras</i> , that meet the search condition will automatically be displayed in the tree. To clear the field click the Reset filter button.
Camera list (table)	
Name	<p>To add a camera to the <i>Camera list</i>, with which given <i>Archiver</i> will work, tick appropriate checkbox on the left of the <i>Camera</i> object.</p> <hr/> <p>Notes:</p> <ol style="list-style-type: none"> 1. Cameras, selected to work with another <i>Archiver</i>, can not be added to the list of the given <i>Archiver</i>. Checkboxes of such cameras are disabled. Place the mouse pointer over such Camera and system will display a name of the <i>Archiver</i> object, in the settings of which given <i>Camera</i> is selected. 2. Cameras, children to the <i>Video Capture Device</i> that having <i>ISS Video Concentrator</i> type and cameras, that work with remote archives with the help of <i>EdgeStorage Gate</i> object, are not displayed in the list of the <i>Cameras</i>.
Max. FPS	Specify max frame rate (from 1 to 60) to record <i>Long-term archive</i> with (see Frame Rate Reduction). If value is not specified, video frame rate in the <i>Long-term archive</i> will be equal to frame rate of the <i>Regular archive</i> .
Remove after	<p>Specify max period for storing fragment in the <i>Long-term archive</i> (in days).</p> <p>Warning! Storage period is calculated not from the date when fragment has been copied to the <i>Long-term archive</i>, but from the moment when this fragment has been recorded to the <i>Regular archive</i>. For example: fragment has been recorded in the <i>Regular archive</i> on April, 10, and has been copied in the <i>Long-term archive</i> on April, 15. If Remove after parameter is set to 15, then fragment will be removed from the <i>Long-term archive</i> on April, 25 (i.e. in 10 days after it was copied).</p> <hr/> <p>Note. If there is not enough free disk space to write a long-term archive, the archive will be deleted earlier than the specified storage period to free space for new files.</p> <hr/> <p>If value is not specified, long-term archive wil be rewritten in "ring mode" (old files are deleted, new ones are written in their place).</p>

Adding a directory for writing archive

To add a directory to write a long-term archive follow these steps:

1. In the object settings window (see Figure 137) click on the **Add directory** button.

2. The Add new directory window will appear (see Figure 138).

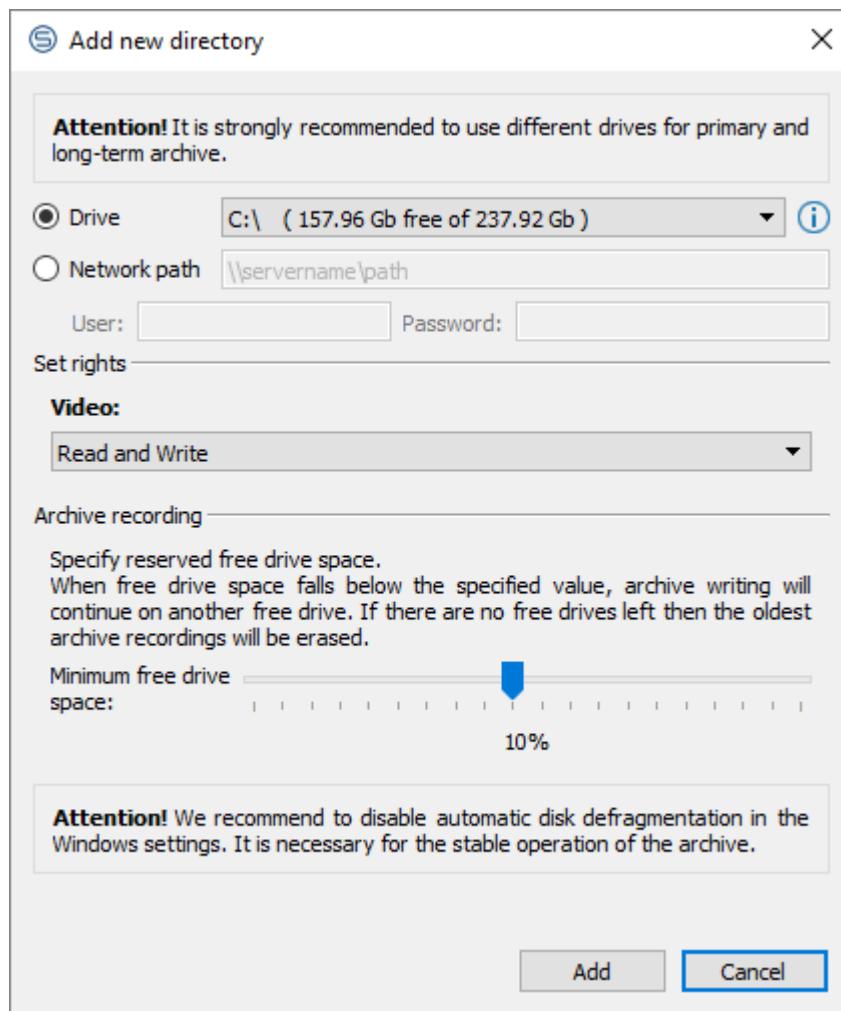


Figure 138. Add new directory window

3. Select option to record archive (**Drive/Network path**) and select hard drive or specify path to the network folder (user name and password are specified optionally).

Notes:

1. The Drive list is automatically populated with all hard drives, available on given *Video Server*.
 2. If *Video Server* is disconnected, then list will be populated with all drives from A to Z.
-

Warning! It is not recommended use the same **Directory** for recording *Regular* (see **Archive** in the *Computer* object settings) and *Long-term* archives.

4. In **Video** field (section **Set rights**) set the rights of directory access. Possible values:

- Read – directory will be available only for reading.
- Read and Write – directory will be available both for reading and writing.

5. In **Archive recording** check and, if necessary, modify the **Minimum free drive space** value.

Notes:

1. Parameter value is calculated and applied automatically when adding new directory.
-

-
2. It is recommended to allocate not less than 10% of full drive space. This value allows to record archive as efficiently as possible.

6. Click on the **OK** button to save the changes.

Editing a directory for writing archive

To edit parameters of a directory to write a long-term archive follow these steps:

1. Select required entry in the **Storages** table (see Figure 137), click on the **Edit** button.
2. The **Edit existing directory** window will appear (see Figure 139).

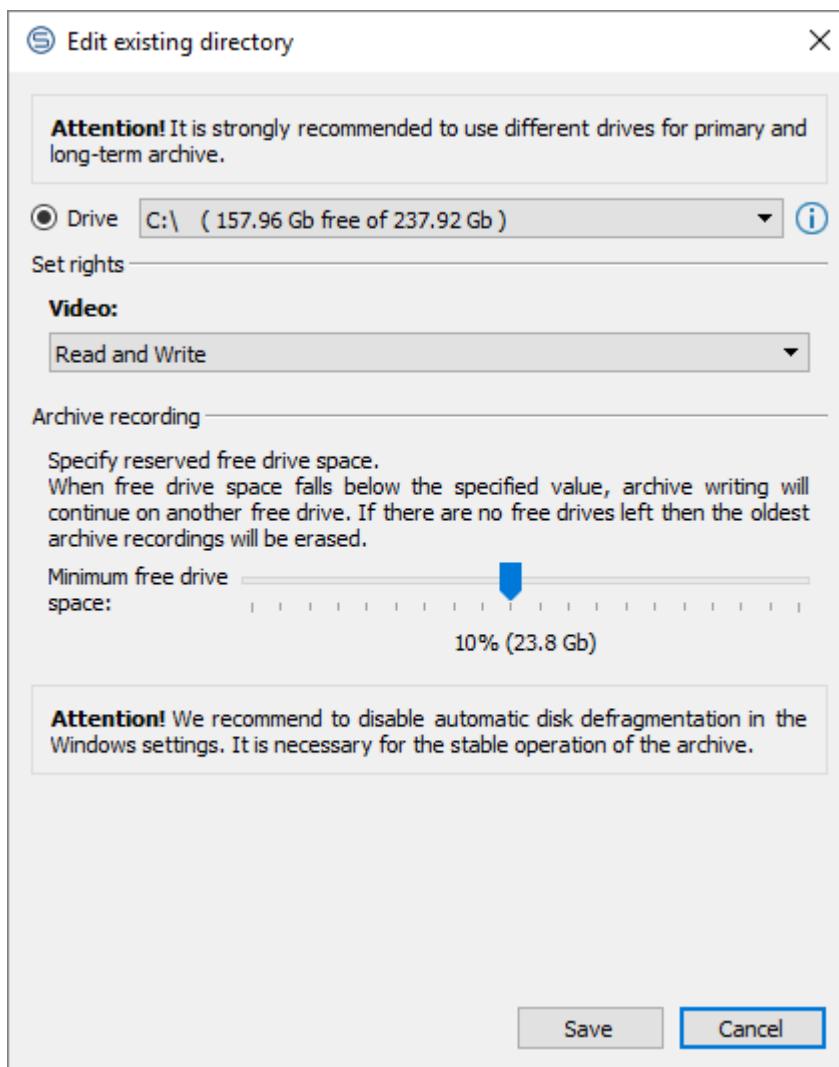


Figure 139. Edit existing directory window

3. Change the current parameters of the directory.

Warning! It is not recommended use the same **Directory** for recording *Regular* (see **Archive** in the *Computer* object settings) and *Long-term* archives.

4. In **Video** field (section **Set rights**) change the rights of directory access. Possible values:

- **Read Only** – archive is available only for reading.
- **Read and Write** – archive is available both for reading and writing.

5. In **Archive recording** check and, if necessary, modify the **Minimum free drive space** value.

Notes:

1. Parameter value is calculated and applied automatically when adding new directory.
 2. It is recommended to allocate not less than 10% of full drive space. This value allows to record archive as efficiently as possible.
-

6. Click on the **Save** button to save the changes.

Deleting a directory for writing archive

To delete a directory, select required entry in the **Storages** table (see Figure 137), click on the **Remove** button.

7.8.1.11 Image Processor

This object is used for image (frame) processing and to subsequently export the image(s) to a file or database.

Parent object – **Computer**.

Object has no settings to configure.

Processing images assumes the following operations:

- cropping initial image to the specified size and position relative to the source values;
- drawing unfilled rectangles with specified color, line width, and position.

When exporting an image to a file it is saved on the hard drive of the parent *Computer* or can be stored in any *Database* configured in the SecurOS object tree when exporting to the database.

To process and export processed frames the **VB/JScript program** object can be used with the help of the **EXPORT** command. For the complete export program syntax see **SecurOS Programming Guide**.

Additional Information

In addition to the parameters specified directly in the command string, the export procedure is controlled with the additional parameters stored in the `HKEY_LOCAL_MACHINE\SOFTWARE\ISS\SecurOS\Niss400\Image Processor` system registry key:

- `deltaArchive` – time shift (in seconds), counted out of the export time value (T) specified in the command string. Is used to specify frame search range in archive records which is calculated as follows: `[T - deltaArchive; T + deltaArchive]`. Default value is 600.
- `downloadTimeout` – timeout to download frame to the archive, in seconds. Is used when exporting frames in real-time. Default value is 20.

7.8.1.12 RTSP Server

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

This module is designed to transmit live or archive H.264 video from SecurOS's *Video Servers* to remote external systems via RTSP/RTP. Video streams can be transmitted both via UDP, which is used by the *RTSP Server* by default, and TCP. The type of transport protocol used is specified by the settings of the external system.

There are the following restrictions when transmitting video from *RTSP Server*:

- total number of *Cameras* connected to a single *RTSP Server* object – not more than 1000;
- total number of clients to receive live or archive video from one *Camera* – not more than 800.

Warning!

1. Any stream of the multi-streaming camera can be transmitted.
2. Transmission of the synchronized audio is not supported.

Parent object – *Computer\Integration and Automation* group.

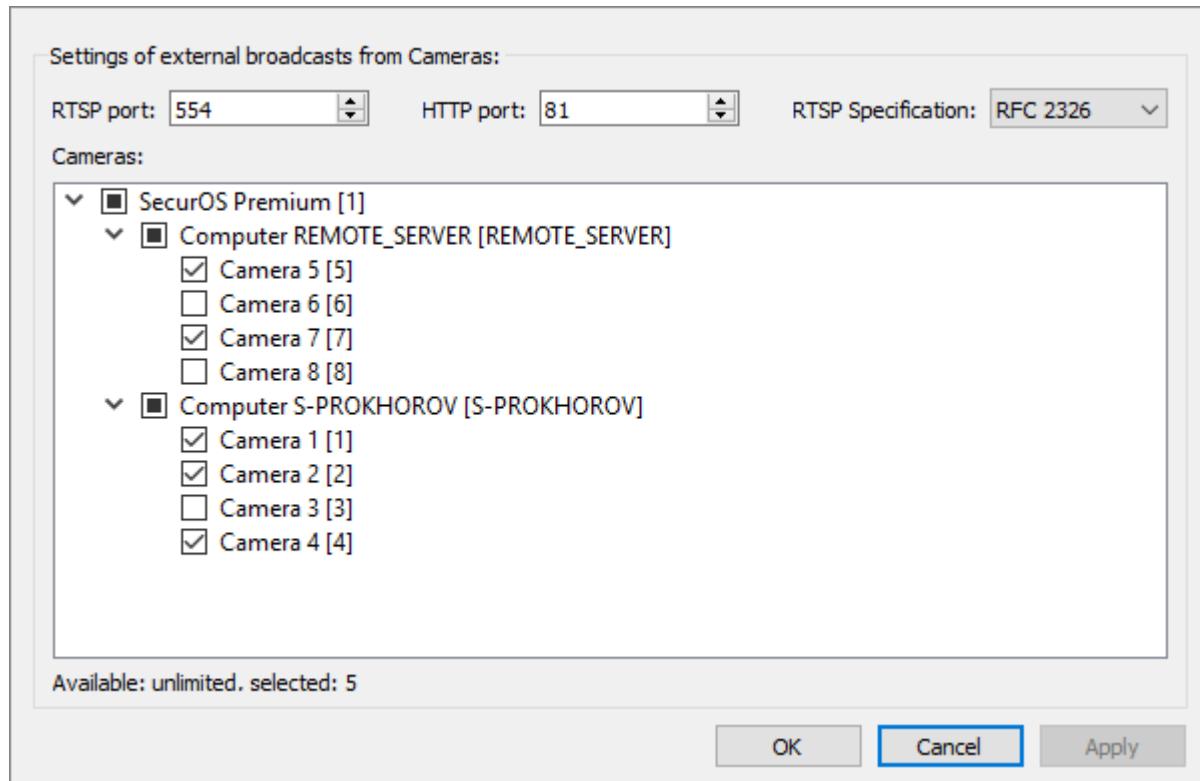


Figure 140. RTSP Server object settings window

Table 44. RTSP Server object settings

Parameter	Description
RTSP port	SecurOS's port for interaction with external system via RTSP. Is used to receive live and archive video with the help of an external application (e.g. media player). Range of values: [1; 32768]. Default value is 554.
HTTP port	SecurOS's port for interaction with external system via HTTP. Is used to receive a list of archive records via web-browser. Range of values: [1; 32768]. Default value is 81. Warning! When changing the default port value it is recommended to use netstat -aon more query in the command prompt to determine the free port.

Parameter	Description
RTSP Specification	Select archive video transfer protocol. Possible values: <ul style="list-style-type: none"> • RFC 2326 – default value. Is recommended for use in most cases; • UDC – select this value, if reverse playback of the archive video requested via RFC 2326 causes errors.
Cameras	
Object tree	<p>List of SecurOS's cameras, that can be used as a signal source to transmit live and archive video to an external system via RTSP. Structure of the tree is similar to SecurOS's <i>Object Tree</i>. To use a <i>Camera</i>, select appropriate checkbox on the left of the object. To use all <i>Cameras</i> of the computer select checkbox on the left of the appropriate <i>Computer</i>. To use all <i>Cameras</i> of all the <i>Computers</i> of the system, select checkbox on the left of the <i>System</i> object.</p> <hr/> <p>Note. Temporarily disabled <i>Cameras</i> (see Disabling Objects) are marked in the Object Tree in gray (see Figure 140, Camera 1).</p> <hr/> <p>Warning! The number of cameras, which can be simultaneously used for video transmission, is a licensed value. When the value, specified in the license key file is exceeded, the OK button is disabled.</p>
Buttons	
OK (Cancel)	Save specified values and close object settings window (Close object settings window without saving changes).

For more information about using *RTSP Server*, please contact your regional Intelligent Security Systems representative.

7.8.1.13 ONVIF Server

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

This object is designed to transmit live H.264 video from the SecurOS *Video Servers* to external systems via RTSP protocol and to control SecurOS PTZ cameras from external system via ONVIF protocol.

Parent object – *Computer\Integration and Automation* group.

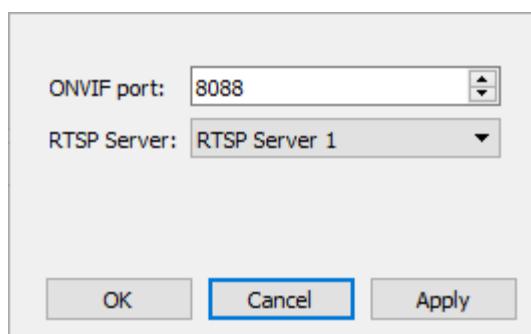


Figure 141. ONVIF Server object settings window

Table 45. ONVIF Server object settings

Parameter	Description
ONVIF port	SecurOS's port for interaction with external system via ONVIF. Is used to control SecurOS PTZ cameras from external system. Range of values: [1; 65535]. Default value is 8088.
RTSP Server	Select RTSP Server, parameters of which will be used for generating request for transmit video from the SecurOS.

For more information about using *ONVIF Server*, please contact your regional Intelligent Security Systems representative.

7.8.1.14 EdgeStorage Sync

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

This object is designed to fill the gaps in the operational archives of the *Video Servers* with the corresponding fragments of the local archives of the *Cameras* (see [Camera Local Storage \(Edge Storage\)](#)).

Parent object – [Computer](#).

This object has no settings to configure.

7.8.1.15 EdgeStorage Gate

This object is designed for working with video archive stored on the external device. One can playback such archive in the *Media Client* window with different playback speed.

Parent object – [Computer](#).

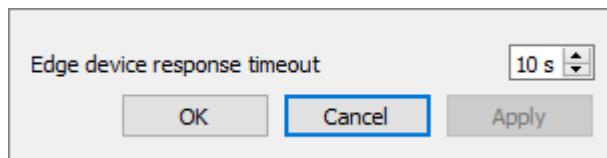


Figure 142. EdgeStorage Gate object settings window

Table 46. EdgeStorage Gate object settings

Parameter	Description
Edge device response timeout	Set timeout for receiving frame from Edge device. Range of values: [1; 60]. Default value is 10.

To configure SecurOS for working with the external archive do the following:

1. In the *Object Tree* create a *Video Capture Device* which **Type** and **Model** corresponds with the Edge device.

2. In the **IP address** field specify IP address of the Edge device where archive you want to work is located.
3. Create the *Camera* object child to the created *Video Capture Device*.
4. In the *Camera* object settings window select the **Playback archive from the edge device** checkbox (see [Recording Tab](#)).
5. Create the *EdgeStorage Gate* object on each *Video Server*, where such *Camera* is created.

7.8.2 User Interface Objects

Media Client is the user interface object intended to work with Video Subsystem.

7.8.2.1 Media Client

This object represents the operator GUI that allows to work with the system *Cameras* and *Microphones*. *Media Client* provides the system with the ability to process each stream generated by a multi-streaming camera in real-time (see [Multi-streaming](#)) and allows to assign a type of stream to display depending on the camera cell size (see Figure 144 and Table 48).

When using the digital zoom feature in the *Media Client*, if it is possible, the stream with the better quality is automatically switched to (for the multi-streaming cameras).

Media Client can operate in two modes: with selected *Camera* list or with all *Cameras* within the system. By default the *Media Client* operates with all *Cameras* connected to the system, which are added to the *Camera list* automatically when creating the *Media Client* object. When creating a new *Camera* object, it is automatically added to the list (only when "working with all *Cameras* mode" is on).

Parent object – [Desktop](#).

Parameter settings windows contains the following tabs:

- [Display options](#) Tab.
- [Layouts](#) Tab.
- [Views](#) Tab.
- [Cameras](#) Tab.
- [Archive export](#) Tab.
- [Audio](#) Tab.

7.8.2.1.1 Display options Tab

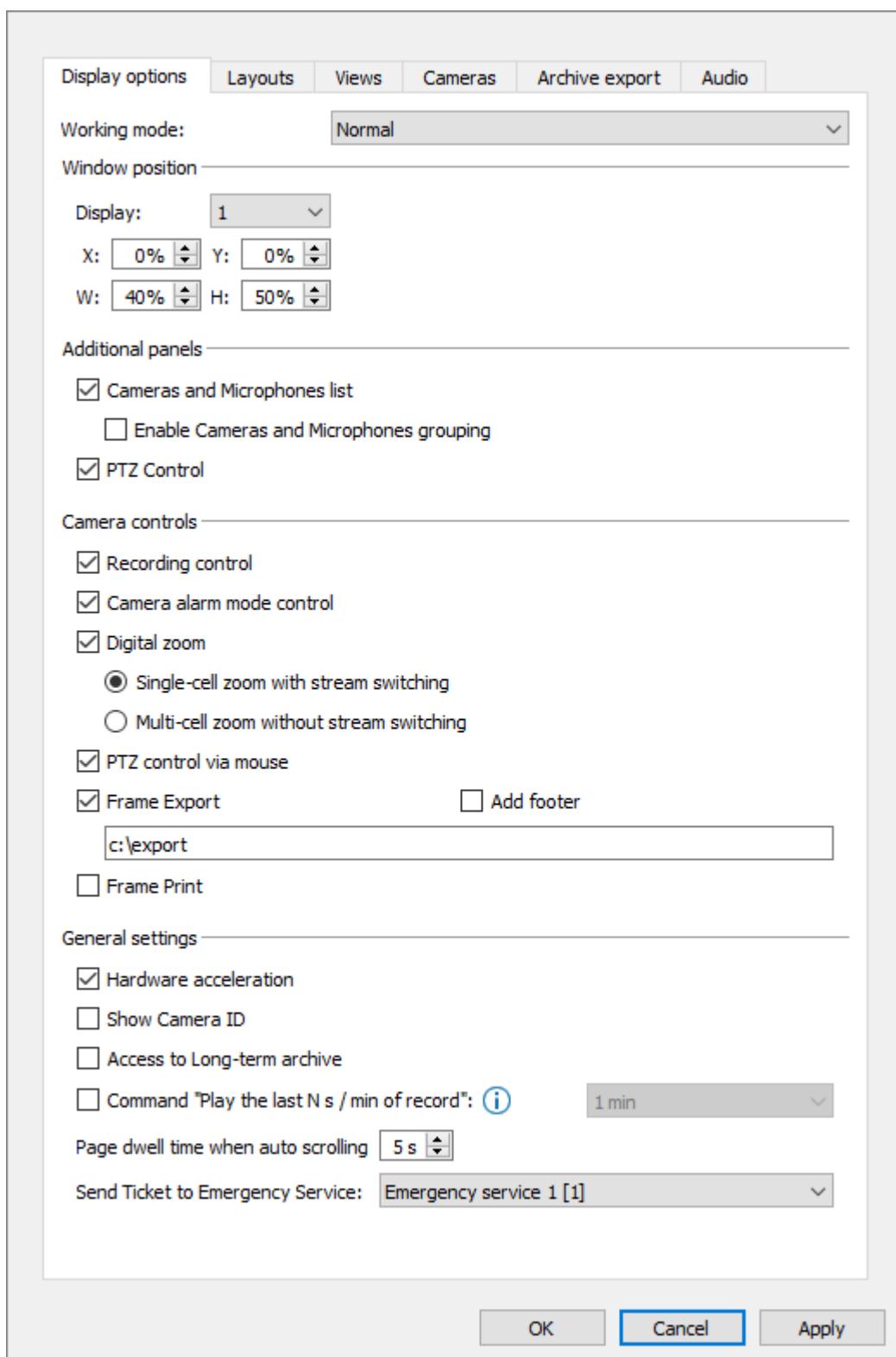


Figure 143. Media Client object settings window. Display options Tab

Table 47. Media Client object settings. Display options Tab

Parameter	Description
Working mode (select <i>Media Client</i> working mode)	
Normal	<p>Normal working mode. Availability of standard controls and miscellaneous elements of the <i>Media Client</i> is defined by current settings. Camera cell controls and cell border are displayed.</p> <p>This mode is specified by default.</p>
Live only	<p>Working only with live video or sound – operator can not switch objects to the archive mode. In this mode all archive controls, that are normally available to the operator, are hidden (for example, the Export panel, the Live/Archive button in the <i>Camera</i> cell or in the <i>Microphone Panel</i>, archive control commands of the context menu).</p>
Alarming	<p>In this mode only alarmed cameras (i.e. where motion is detected) are displayed.</p> <p>In this mode a standard (<i>Layout Bar</i>, <i>Camera Control Bar</i>) and additional (<i>Microphone and Camera List</i>, <i>PTZ Control Panel</i> etc.) <i>Media Client</i>'s controls are not available. <i>Zoom</i> and <i>Export frame</i> buttons are available in the camera cell.</p> <p>Camera is displayed in the <i>Media Client</i> working area only when motion is detected in camera's Zone. When alarm ends, camera is removed from working area in accordance with Time to display Camera after alarm ends parameter (see below).</p>
Active	<p>Working with active camera only in 1×1 layout. Standard <i>Media Client</i> tools and <i>Camera list</i> and <i>Microphone list</i> are hidden. Camera cell controls and cell border are displayed.</p>
View only	<p>In this mode, the standard <i>Media Client</i>'s controls are not available to the operator.</p> <p>When turning this mode on, all additional <i>Media Client</i> controls (i.e. <i>Camera Panel</i>, <i>Layout Panel</i> etc.), and also <i>Camera</i> cell controls and <i>Camera</i> cell border, that are normally displayed, are hidden.</p> <p>If this mode is applied to the existing <i>Media Client</i> object, then all cameras are switched to the live video mode. Layout of the working area and displayed video page are not changed.</p> <p>When view mode is on, the <i>Media Client</i> is controlled only externally, for example, with the help of VB/JavaScript programs. The following types of commands are supported:</p> <ul style="list-style-type: none"> • layout switching; • moving <i>Camera</i> to the specified cell; • switching between live/archive modes; • archive control commands.

Parameter	Description
Settings for alarm mode	
Time to display Camera after alarm ends	Specify time interval to display <i>Camera</i> on the <i>Media Client</i> after alarm ends (in seconds).
Window position	
Display	Choose the number of the physical display this <i>Media Client</i> belongs to. Possible values: [1; 16]. Default value is 1.
X, Y	Specify top-left coordinates (X, Y), relative to the top-left corner of the computer's monitor. Possible values: [0; 70], in percent of screen size.
W, H	Specify width and height (W, H) of the window. Possible values: [30; 100], in percent of screen size. Notes: 1. If the specified parameters result in $(X+W) > 100$ or $(Y+H) > 100$ and the View mode option is disabled, then the system automatically reduces the specified values down to $(X+W) = 100$ or $(Y+H) = 100$ respectively. 2. If the specified parameters result in $(X+W) > 100$ or $(Y+H) > 100$ and the View mode option is enabled, then the system displays <i>Media Client</i> window on several physical monitors, considering their mutual alignment (system setting).
Additional panels	
Cameras and Microphones list	Deselect checkbox to hide <i>Camera list</i> and <i>Microphone list</i> for the given <i>Media Client</i> . By default it is selected.
Enable Cameras and Microphones grouping	Select checkbox to enable <i>Camera</i> and <i>Microphone</i> grouping by name if camera's/microphone's Name (see Adding Camera to System) contains ":" separator (-s). Separators can be used, for example, to specify actual camera/microphone position within a segment of the security network ("Factory:Shop:Area:Camera"). Up to 3 nesting levels for the camera name are supported ("Factory:Shop:Area"). Groups (nested levels) are displayed in the <i>Camera and Microphone list</i> in alphabetical order; <i>Cameras/Microphones</i> are also sorted in alphabetical order inside level. <i>Cameras/Microphones</i> that do not have a ":" separator in the Name , do not belong to any level and are united under the Ungrouped system group at the top of the list.
PTZ Control	Deselect checkbox to hide the PTZ Control Panel . By default it is selected.
Camera controls	
Recording control	Deselect checkbox to forbid operator to control the recording mode. By default it is selected.

Parameter	Description
Camera alarm mode control	Deselect checkbox to forbid operator to control the alarm mode. By default it is selected.
Digital Zoom	Deselect checkbox to forbid operator to use the digital zoom feature. By default it is selected.
Single-cell zoom with stream switching	<p>If this option is selected, then only one <i>Camera</i> can be in digital zoom mode at the same time. When turning digital zoom mode on, the system automatically switches camera to display the best quality stream.</p> <p>It is recommended to use this feature if cameras support multi-streaming and are configured to be operated in such mode.</p> <p>Option is enabled if Digital zoom parameter is selected and is the default value.</p>
Multi-cell zoom without stream switching	<p>If this option is selected, then several <i>Cameras</i> can be in digital zoom mode at the same time. When turning digital zoom mode on, no switching to the best quality stream occurs.</p> <p>Option is available if the Digital zoom parameter is selected.</p>
PTZ control via mouse	Deselect checkbox to disable PTZ control via mouse (see SecurOS Quick User Guide). By default it is selected.
Frame Export	Deselect checkbox to forbid operator use of the frame export feature from the <i>Media Client</i> . By default it is selected. If this option is selected, then a frame can be saved to the specified directory.
Add footer	<p>Tick this checkbox to place additional information on the saved frame. This additional information will be displayed in the frame footer in the following format:</p> <pre><Frame date in OS format> <Frame time in OS format, including milliseconds> [< Camera ID>] <Camera Name></pre>
Frame Print	Select this checkbox to allow operator to print frame from the <i>Media Client</i> .
General settings	
Hardware acceleration	<p>Select checkbox to use Direct3D for displaying video.</p> <hr/> <p>Note. If this checkbox is selected, operator will be able to adjust image settings in the camera cell on the <i>Media Client</i> (see SecurOS Quick User Guide).</p> <hr/> <p>If the checkbox is not selected, then software rendering is used.</p>
Show Camera ID	Select checkbox to display <i>Camera</i> ID in the camera cell title. If selected, <i>Camera</i> name in the cell title will be displayed in the [<Camera ID>] <Camera Name> format. By default is not selected.

Parameter	Description
Access to Long-term archive	<p>Tick this checkbox to allow the operator to work both with <i>Primary</i> and <i>Long-term archive</i>. If selected, then additional controls are displayed in the <i>Media Client</i>'s camera cell (see SecurOS Quick User Guide).</p> <p>Warning! Option is available only in Normal and Active working modes (see Working mode parameter description).</p>
Command "Play the last N s/min of record"	<p>Select this checkbox to add the Play the last N s/min of record command to the <i>Camera</i> cell context menu on the <i>Media Client</i> and specify the parameter value. To learn more about command usage and playback features see SecurOS Quick User Guide.</p> <p>Warning! Option is available only in Normal and Active working modes (see Working mode parameter description).</p>
Page dwell time when auto scrolling	Video page dwell time in auto scrolling mode (in seconds).
Send Ticket to Emergency Service	Choose from the list an <i>Emergency service</i> object that will be used to create and send <i>Emergency ticket</i> (see Emergency service and Interaction with External Emergency Service).

7.8.2.1.2 Layouts Tab

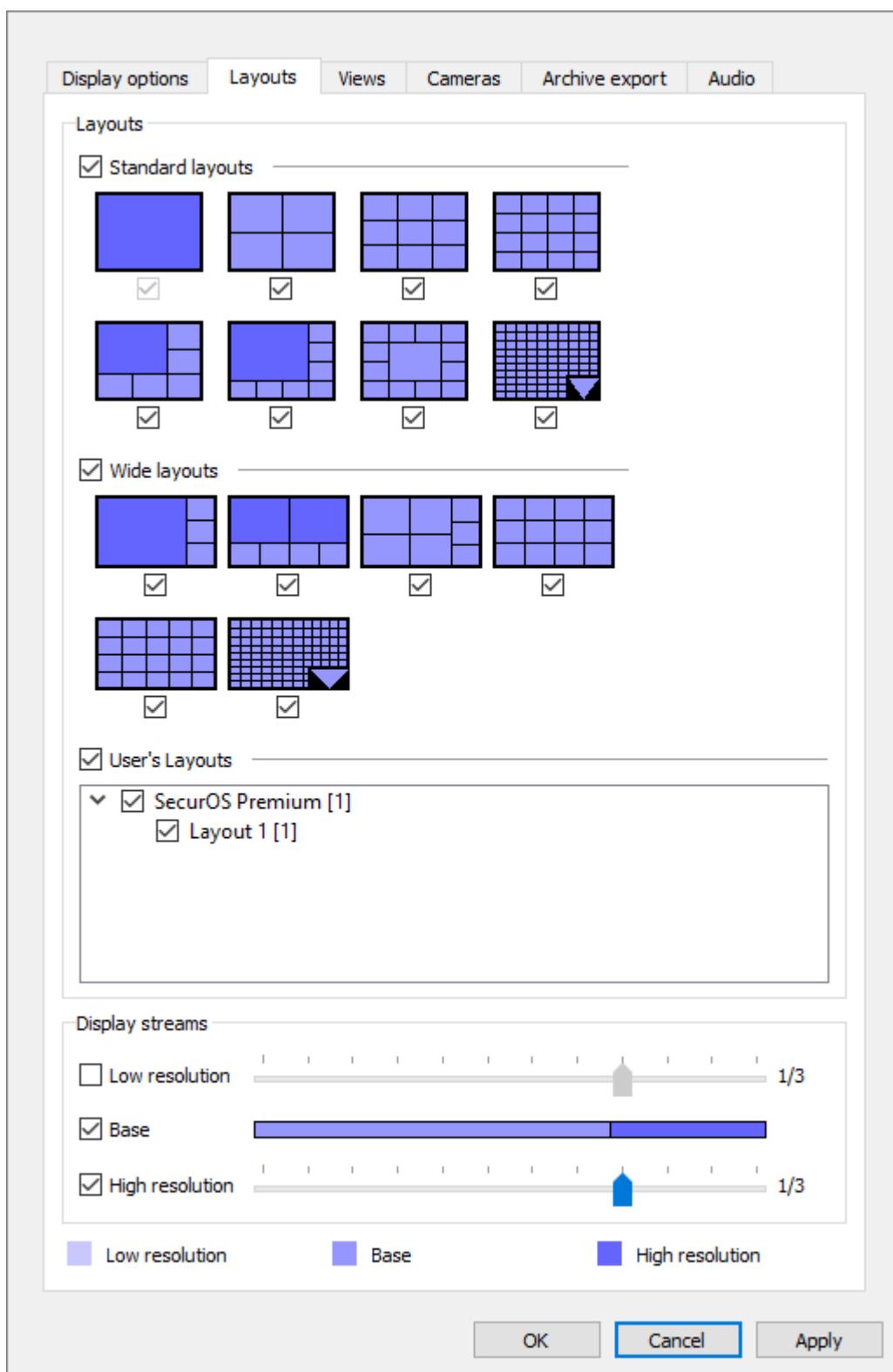


Figure 144. Media Client object settings window. Layouts Tab

Table 48. Media Client object settings. Layouts Tab

Parameter	Description
Number of cells to determine layouts	
Minimum/Maximum	<p>Warning! Parameters are displayed only when Alarming mode is selected.</p> <p>Specify a Minimum and Maximum cells in the layout that can be used for this mode. Only layouts that have predefined types (see Layouts) and cells of which have the same size will be automatically selected.</p> <p>If maximal available number of cameras are displayed, then other alarmed cameras are placed into the queue. Cameras from the queue will be displayed in sequence, when an alarm ends in some currently displayed camera. If alarm ends, camera is removed from the queue.</p> <hr/> <p>Example. When working in the Alarming mode selected layouts are changed automatically depending on number of alarmed cameras. For example, the Minimum parameter is set to 4, and the Maximum parameter – to 9. This means that the 2x2 and 3x3 layouts can be used. If number of alarmed cameras is less or equal to 4, the 2x2 layout will be used, and if number of alarmed cameras is greater than 4, then <i>Media Client</i> will automatically use the 3x3 layout. The 1x1 layout is always available.</p>
Layouts (to select/deactivate all layouts of the group select/deactivate appropriate checkbox on the left of the group name)	
Standard layouts	<p>Select checkbox of the appropriate standard layouts, which will be enabled to the operator in the layout panel of the <i>Media Client</i>.</p> <p>Warning! 1*1 layout is mandatory. It is selected by default and cannot be disabled.</p>
Wide layouts	Select checkbox of the appropriate wide layouts, which will be enabled to the operator in the layout panel of the <i>Media Client</i> .
User's Layouts	Select checkbox of the appropriate User's custom layouts (see Layout), which will be enabled to the operator in the layout panel of the <i>Media Client</i> .
Display streams	
Low resolution, Base, High resolution	<p>Select appropriate checkbox to use the stream. Use the appropriate slider to specify the size of the cell (in parts of <i>Media Client</i>'s window working area), where selected stream should be displayed. When specifying cell size for several used streams, a stream/cell size relation will be represented in the tab (see Figure 144).</p> <p>Warning! By default the Base stream, will be displayed in cells of size less than 1/3 of the <i>Media Client</i> working area. The High resolution stream will be displayed in cells of size 1/3 and greater.</p>

For example, as it is illustrated in Figure 144, if all three camera streams are selected to be displayed, then for the specified settings, the **High resolution** stream will be displayed in any cells whose size is not less than 1/2 of the working area. The **Low resolution** stream will be displayed in any cells whose size is not greater than 1/4 of the working area. At the same time, the **Base** stream will be displayed in the cells of intermediate size.

7.8.2.1.3 Views Tab

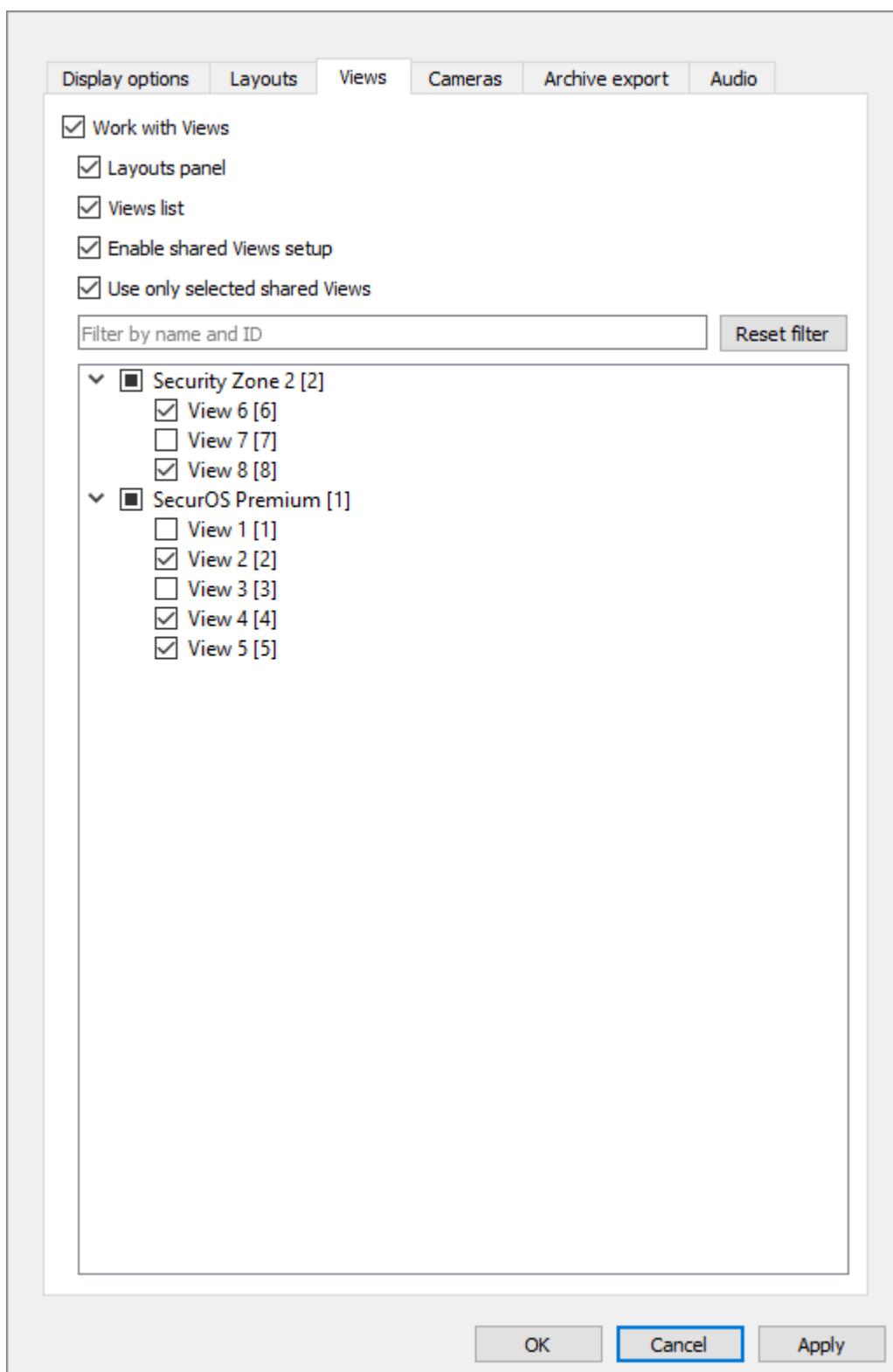


Figure 145. Media Client object settings window. Views Tab

Table 49. Media Client object settings. Views Tab

Parameter	Description
Work with Views	<p>Select this checkbox to work with <i>Views</i>. By default is not selected.</p> <p>Note. Listed below parameters are available only if this checkbox is selected.</p> <p>Operations with <i>Views</i> are described in Working with Views section.</p>
Layouts panel	Deselect checkbox to hide <i>Layouts panel</i> . By default it is selected.
Views list	Deselect checkbox to hide <i>Views list</i> . By default it is selected.
Enable shared Views setup	Select checkbox to allow operator to edit shared <i>Views</i> . By default is not selected.
Use only selected shared Views	<p>Select checkbox to activate manual control mode of the <i>Views list</i> for the given <i>Media Client</i>.</p> <p>If not selected, the <i>Views list</i> is populated automatically and contains all <i>Views</i> created within system. By default is not selected.</p> <p>Note. Listed below parameters are available only if this checkbox is selected.</p>
Filter	To search object by name (part of its name) or by ID, type required characters in the field; only those objects that meet the search condition will automatically be displayed in the tree. To clear the field click the Reset filter button.
Object tree	<p>Tree of the <i>Security Zones</i> within SecurOS network including all children shared <i>Views</i> that are grouped by these <i>Security Zones</i>.</p> <p>To add a <i>View</i> to the <i>Media Client's Views list</i> select appropriate checkbox to the left of the <i>View</i> object.</p> <p>Note. By default objects in the tree are sorted ascending by name and ID.</p>

7.8.2.1.4 Cameras Tab

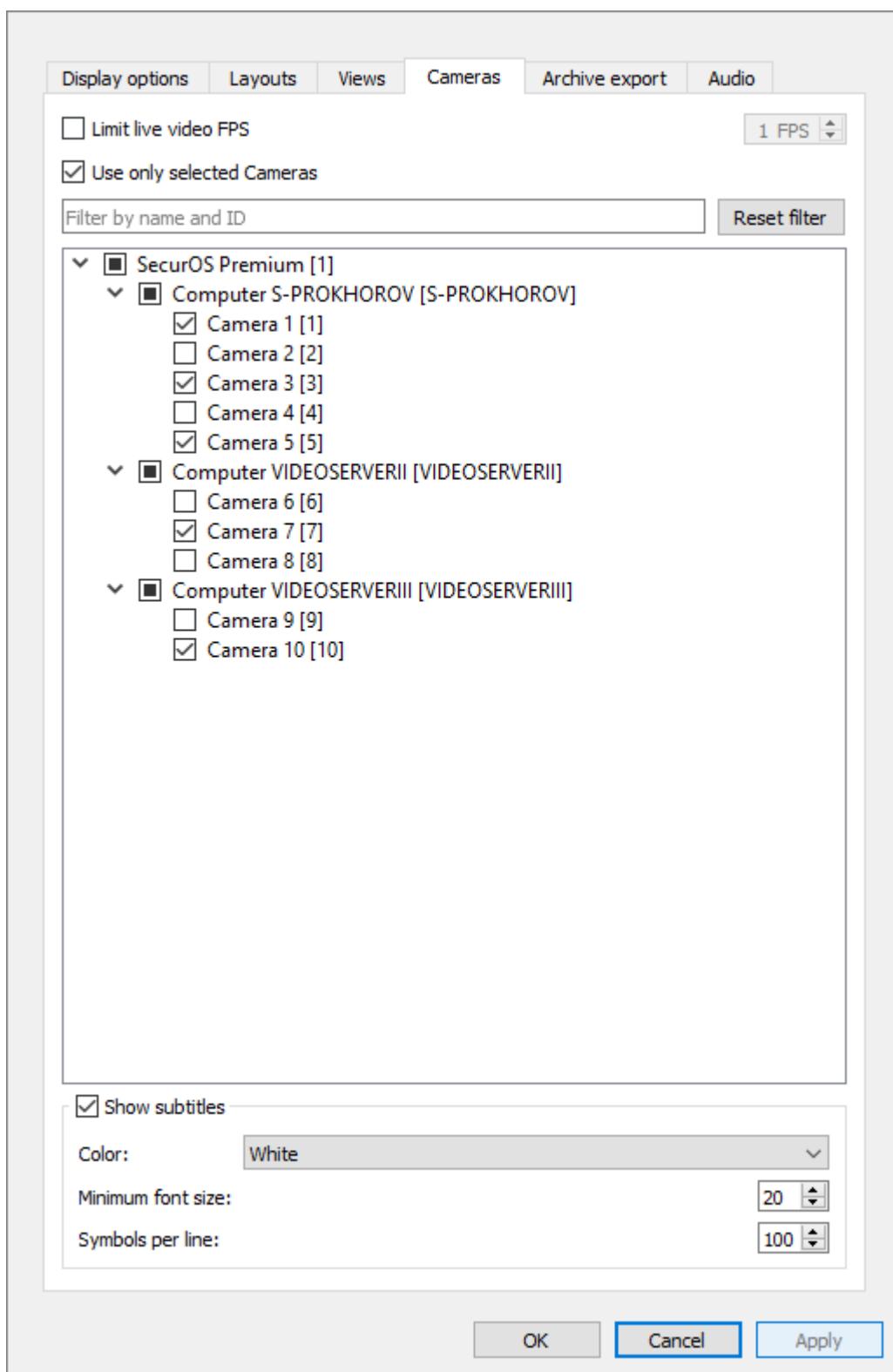


Figure 146. Media Client object settings window. Cameras Tab

Table 50. Media Client object settings. Cameras Tab

Parameter	Description
Limit live video FPS	Select this checkbox if it is necessary to limit live video FPS and specify required value. If value is specified then algorithm described in the Frame Rate Reduction will be used. Notes: <ol style="list-style-type: none"> Specified value is applied to all <i>Cameras</i> selected to work with the given <i>Media Client</i>. If there are more than one <i>Media Client</i> created and configured on one <i>Desktop</i> and each of them works with the given <i>Camera</i>, then FPS of this <i>Camera</i> is equal to the maximal value of the specified on all <i>Media Clients</i>.
Use only selected Cameras	Select checkbox to activate manual control mode of the <i>Camera list</i> for the given <i>Media Client</i> . If not selected, the <i>Camera list</i> is populated automatically, cannot be changed, and contains all <i>Cameras</i> connected to the system. By default is not selected.
Filter	To search object by name (part of its name) or by ID, type required characters in the field; only those objects that meet the search condition will automatically be displayed in the tree. To clear the field click the Reset filter button.
Object tree	<p>Object Tree of the <i>Computers</i> having role <i>Video Server</i> existing within the SecurOS network. When expanding the <i>Video Server</i> node all <i>Camera</i> children objects are displayed.</p> <p>To add a camera to the <i>Media Client's Camera list</i> select appropriate checkbox to the left of the object.</p> <p>Note. The state, when not all <i>Cameras</i> of the appropriate <i>Video Server</i> are added to the <i>Media Client's Camera list</i>, is called "partial usage". In this state, the field located on the left of such <i>Video Server</i>, is marked with a gray background in the Object tree (☒) or, in Windows 7, with the ☐ icon.</p>
Show subtitles (select checkbox to display subtitles with soecified parameters). If selected subtitles will be displayed both in the Live and Archive mode. Subtitles are added externally, wit hthe help of the ADD_SUBTITLES command (see SecurOS Programming Guide)).	
Warning! If subtitle parameters are specified in the ADD_SUBTITLES command, the following values are ignored.	
Color	Choose a subtitles color.

Parameter	Description
Minimum font size	<p>This parameter specifies minimal possible size of the subtitles font. Range of values: [1; 50].</p> <p>Actual font size is calculated automatically depending on the current frame size and the Symbols per line parameter value. Calculated font size Y will always obey $X_{min} \leq Y \leq 50$, where X_{min} – specified parameter value. Calculated font size value is changed proportionally to the frame size change.</p>
Symbols per line	<p>This parameter specifies such minimal font size, which guaranteed that specified above provide number of characters will be displayed in one output line in the <i>Camera</i> cell without forced line breaking. Range of values: [1; 200].</p> <p>Number of characters in the line for the given frame size will be kept constant until calculated font size value is greater than specified Minimum font size. If calculated font size is less than Minimum font size, then the size of the displayed characters will be equal to Minimum font size. At the same time output line may include less characters, than is specified by the Symbols per line parameter.</p> <p>If length of the subtitle text string exceeds frame horizontal size, it wraps to the next line "by words".</p> <p>For the details of how to control subtitles see SecurOS Programming Guide, the Working with Subtitles section.</p>

7.8.2.1.5 Archive export Tab

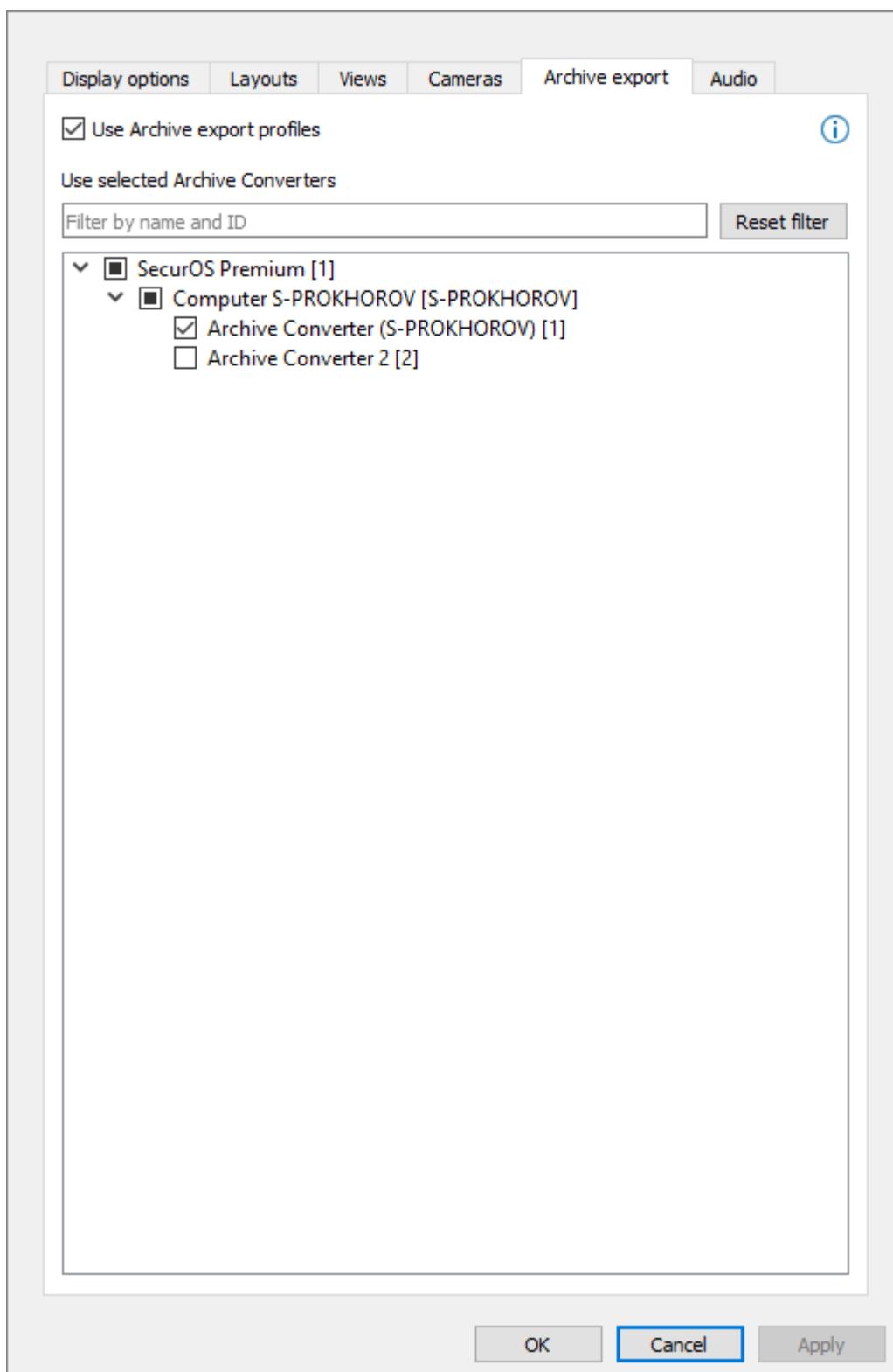


Figure 147. Media Client object settings window. Archive export Tab

Table 51. Media Client object settings. Archive export Tab

Parameter	Description
Use Archive export profiles	Select this checkbox to use <i>Archive export profiles</i> when exporting archive with the help of the configured <i>Media Client</i> (for the details see Export Using Archive Export Profile).
Use selected Archive Converters	
Filter	To search object by name (part of its name) or by ID, type required characters in the field; only those objects that meet the search condition will automatically be displayed in the tree. To clear the field click the Reset filter button.
Object tree	<p>Tree of the <i>Video Servers</i>, <i>Operator Workstations</i> or <i>Operator Workstation Profiles</i> existing within the SecurOS network and having the <i>Archive Converters</i> children objects. When expanding the node of each object the list of <i>Archive Converters</i> children objects is displayed.</p> <p>To choose an <i>Archive Converter</i>, which will be used by the given <i>Media Client</i>, select the appropriate checkbox to the left of the <i>Archive Converter</i> object (for the details see Export Using Archive Export Profile).</p> <p>Warning! <i>Archive Converters</i> created on the <i>Video servers</i> are available on any <i>Computer</i>. <i>Archive Converters</i> created on the <i>Operator Workstations</i> or <i>Operator Workstation Profiles</i> are available only on these <i>Computers</i>.</p>

Warning! To perform export operations user access rights to the *Archive export profile* and *Archive Converter* objects must be not less than  ([View](#)), see [User Rights](#). If operator has an access to the pointed objects, then possibility of use these objects is being specified in this tab.

Export Using Archive Export Profile

When using *Archive export profile*:

- **Export task** is being created by *Media Client*;
- **Export** is being performed also by *Media Client*.

Export Using Archive Converter

When using *Archive Converter*:

- **Export task** is being created by *Media Client*;
- **Export** is being performed by *Archive Converter*.

7.8.2.1.6 Audio Tab

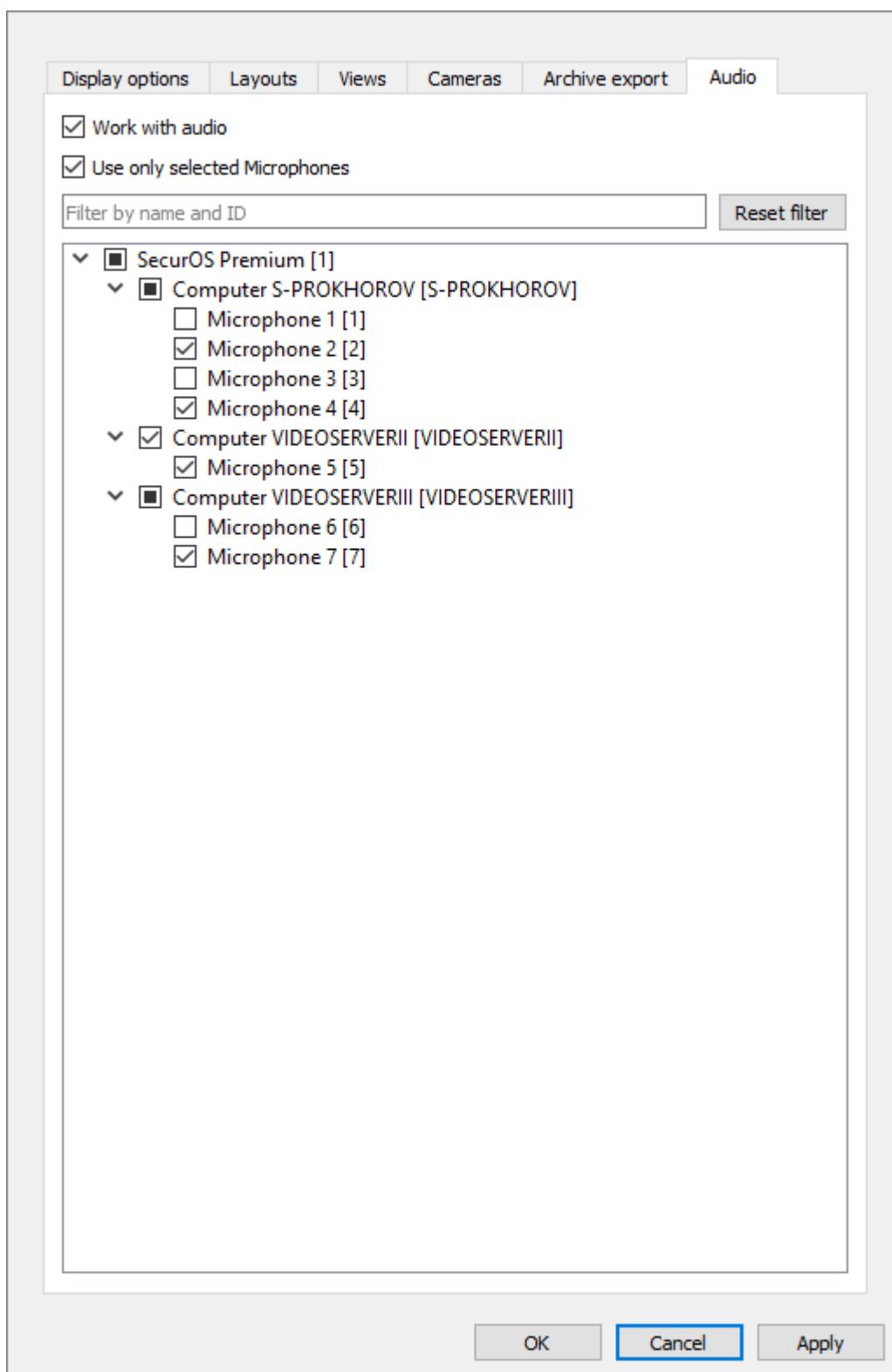


Figure 148. Media Client object settings window. Audio Tab

Table 52. Media Client object settings. Audio Tab

Parameter	Description
Work with audio	Select checkbox to listen to the live or archived audio.
Use only selected microphones	Select checkbox to activate manual control mode of the <i>Standalone microphone list</i> for the given <i>Media Client</i> . Notes: <ul style="list-style-type: none"> 1. A <i>Standalone microphone</i> means one that is not associated with any <i>Camera</i>. 2. This option does not affect operation with the <i>Microphones</i> associated to <i>Cameras</i>.
	If not selected, the <i>Standalone microphone list</i> is populated automatically, cannot be changed, and contains all standalone <i>Microphones</i> connected to the system. By default is not selected. Option is disabled if the Work with audio option is disabled.
Filter	To search object by name (part of its name) or by ID, type required characters in the field; only those objects that meet the search condition will automatically be displayed in the tree. To clear the field click the Reset filter button.
Microphone Tree	Object Tree of the standalone <i>Microphones</i> existing within the SecurOS network. When expanding the <i>Video Server</i> node all standalone <i>Microphone</i> children objects are displayed. To add a standalone <i>Microphone</i> to the <i>Media Client's Standalone Microphone list</i> , select the appropriate checkbox to the left of the <i>Microphone</i> object.

7.8.2.1.7 About Views

View is an object, that allows to group *Cameras* and *Microphones* and place them in *Media Client* as required.

Figure 149 illustrates an example of *View*.

Video Subsystem

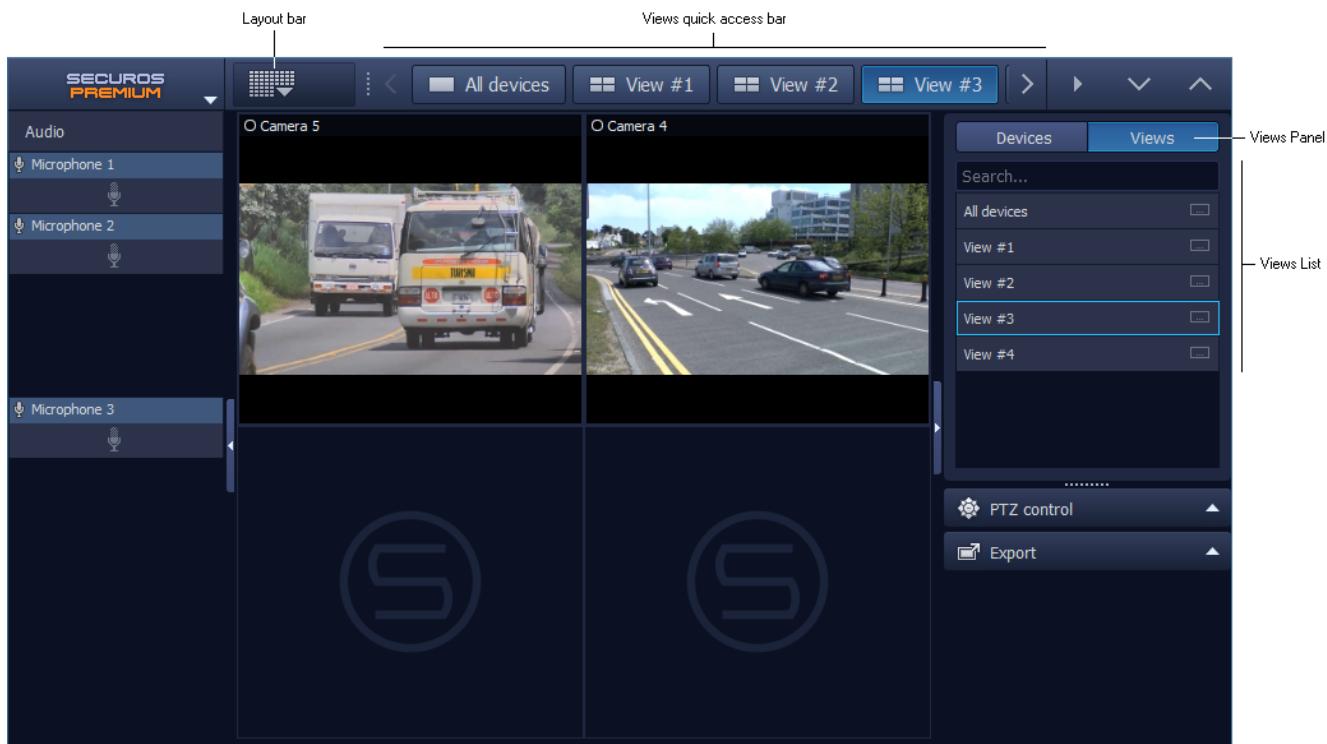


Figure 149. Example of View

All *Views*, exclude *View*, name of which is **All devices**, are single-page, i.e. *Cameras* of these *Views* can not be listed. The **All devices** multi-page *View* always exists and includes all available *Cameras* and *Microphones*.

The following objects are shown on Figure 149:

- *Layout bar* – (is collapsed in Figure 149) contains all *Layouts* that can be used when working with *Views*;
- *Views quick access bar*, where you can drag-and-drop frequently used *Views*. An active *View* is highlighted on this bar in light-blue;
- *Views Panel* – contains *Views List* and *View search field*;
- *Views List* contains all available *Views*. An active *View* is highlighted in this list in light-blue frame.

Using the settings of the **Views** tab administrator can hide *Views List*, *Layout bar* and also select a *Views*, that you can work with in the *Media Client*.

Note. If *Views List* is hidden, then *Views* are displayed in the *Views quick access bar*.

For the details of how to switch *Views*, work with *Views quick access bar*, temporarily change *Views*, refer to the [SecurOS Quick User Guide](#).

7.8.2.1.8 Working with Views

To get a possibility to create, edit and remove *Views*, tick the **Enable shared Views setup** checkbox in the **Views** tab of the *Media Client*.

To open the *Views Editor* edit mode click on the button in upper left corner of the *Media Client* (see Figure 150) and select the **Enter Views Setup** command.

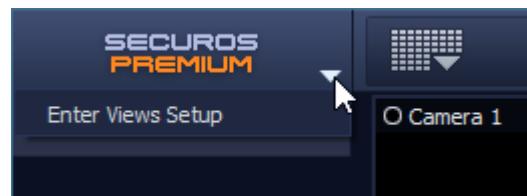


Figure 150. Switching to Views Editor

You can perform the following operations in the *Views Editor*:

- [Creating View](#).
- [Editing View](#).
- [Renaming View](#).
- [Deleting View](#).

These operations are performed with the help of buttons, located in the *View Edit Bar* (see Figure 151).

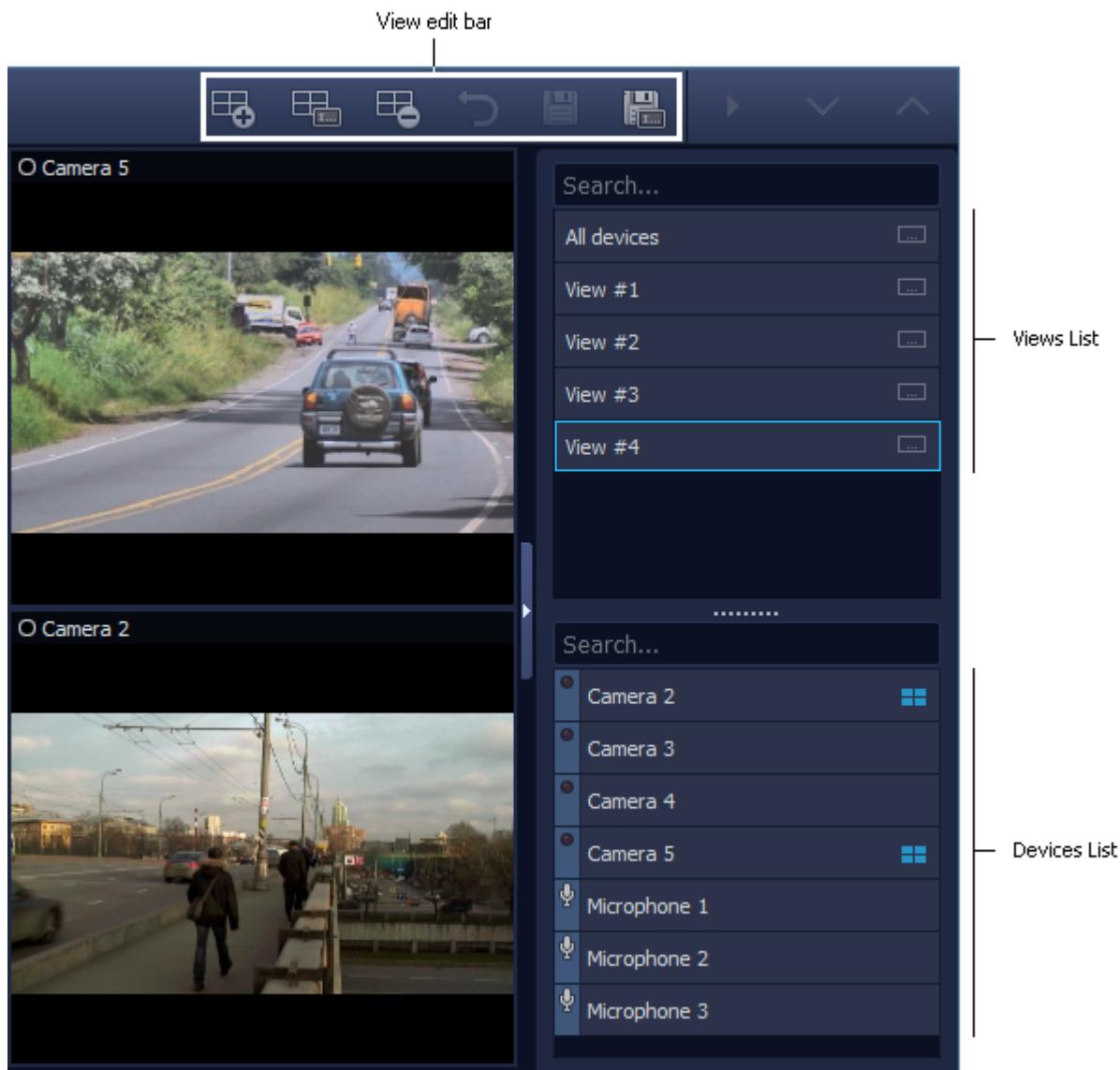


Figure 151. Views Editor

Note, that *Device List* is located under the *Views List* in the *Views Editor*. *Views*, that don't contain devices, are presented in gray background in the *Views List*, for example, **View 5** (see Figure 151).

To close the *Views Editor* click on the  button in upper left corner of the *Media Client* (see Figure 152) and select the **Exit Views Setup** command.

7.8.2.1.8.1 Creating View

Note. This section provides information on creating a *View* with a *Cameras*. You can create a *View*, containing *Microphones*, in the same way.

To create a View in *View Editor* do the following:



1. Click on the  (**Create new**) button on the *View Edit Bar*. System will display the *View creation window* (see figure 152).

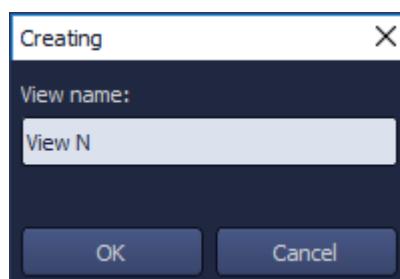


Figure 152. View create window

2. Type new name of a *View* in the **View name** field and click on the **OK** button.
3. The *2x2 Layout* is selected by default for the *Media Client Working Area*. **To change layout** choose another one in the *Layout bar*.
4. **To add a Camera** choose it in the *Device List* and drag-and-drop it to the required cell of the *Media Client*.
5. **To delete a Camera** choose it in the *Media Client's* cell and drag-and-drop it to the *Device List*.
6. **To change Camera's position** choose it and drag-and-drop it to the required cell of the *Layout*.



7. To save changes click on the  (**Save**) button on the *View Edit Bar*. To discard changes click on the  (**Discard current changes**) button on the *View Edit Bar*.

Note. To mark *Views* with unsaved changes, an Italic font is used in the *Views List*.

7.8.2.1.8.2 Editing View

When editing a View, you can add or delete *Cameras* and/or *Microphones*, change *Camera's* and/or *Microphones* position in the *Media Client's* cells, change *Layout* of the *Media Client Working Area*. How to do this see [Creating View](#) section.



To save *View* with the same name, click on the  (**Save**) button, with a new name – the  (**Save as**) button.



Notes:

1. When saving *View* its changes are applied for all *Media Clients*, that use this *View*.
2. *View*, that contains devices, access for which is denied (*View* that marked with an  icon in the *Views List*), can not be saved with previous name. If *View* is saved with a new name, then *Media Client's* cells, that correspond to such devices, are empty.

7.8.2.1.8.3 Renaming View

To rename a *View* in *View Editor* do the following:

1. Choose required *View* in the *Views List*.



2. Click on the  (**Rename**) button on the *View Edit Bar*. System will display the **View renaming** window (see figure 153).

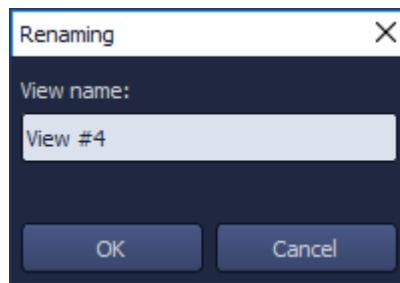


Figure 153. Renaming window

3. Type new name of a *View* in the **View name** field and click on the **OK** button.

Additional Information

View can also be renamed in SecurOS *Object tree* (see [Working with Objects](#)).

Note. *View*, that contains devices, access for which is denied (*View* that marked with an  icon in the *Views List*), can not be renamed.

7.8.2.1.8.4 Deleting View

To delete a *View* in *View Editor* do the following:

1. Choose required *View* in the *Views List*.



2. Click on the  (**Remove**) button on the *View Edit Bar*.

Additional Information

View can also be deleted in SecurOS *Object tree* (see [Working with Objects](#)).

Note. *View*, that contains devices, access for which is denied (*View* that marked with an  icon in the *Views List*), can not be deleted.

7.9 Configuration Examples

This section includes examples of how to setup typical configurations.

7.9.1 Standalone Configuration

Original objective: one computer and two cameras connected to local area network. Computer should be used not only to capture and record video, but to monitor cameras also.

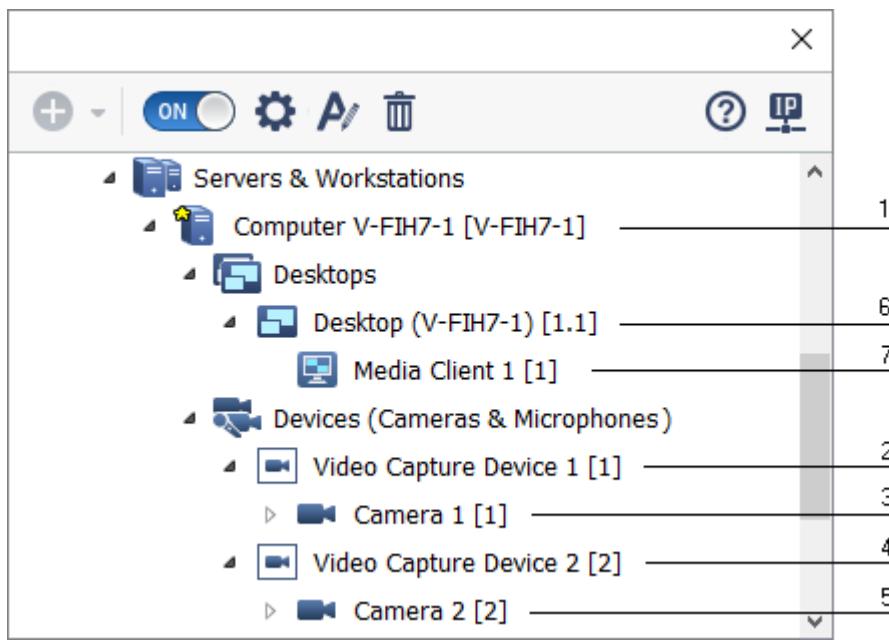


Figure 154. Object tree for standalone configuration

Solution: (see figure 154):

Go to administration mode (see [SecurOS Administration Overview](#)) and to the following:

1. Open *Computer* object settings window (see [Editing Object Settings](#)). In **Archive** section set **Read** and **Write** value for **Video** parameter at least for one directory (for example drive C:\).
2. Go to *Computer* → *Devices (Cameras & Microphones)* branch in the object tree and create *Video Capture Device* object.

Enter values for following parameters of the objects:

- **Type:** camera vendor;
 - **Model:** model of the camera of selected vendor. In some cases parameter stands for the communication protocol between server and camera;
 - **Protocol:** version of communication protocol between server and camera. For some models this field may be disabled;
 - **IP address:** address of the camera in the TCP/IP network;
 - **User and Password:** login and password of the user that has an access to camera's video stream (can be set in the camera's web interface).
3. Create the *Camera* object (child object of the *Video Capture Device* object).
 4. Create second *Video Capture Device* and configure it the same way.
 5. Create the *Camera* object (child object of the second *Video Capture Device* object).
 6. Go to *Computer* → *Desktops* branch in the object tree and create *Desktop* object.

7. Create *Media Client* object child to recently created *Desktop* object.
8. Exit administration mode.

Now you will see a full-screen *Media Client* with live video from two cameras.

7.9.2 Video Server and Operator Workstations

Original objective: video server and two cameras connected to local area network. Monitoring can be performed from one or more Operator Workstations. For them the *Operator Workstation Profile* user interface will be created (see [Operator Workstation Profiles](#)), that can be used on all computers.

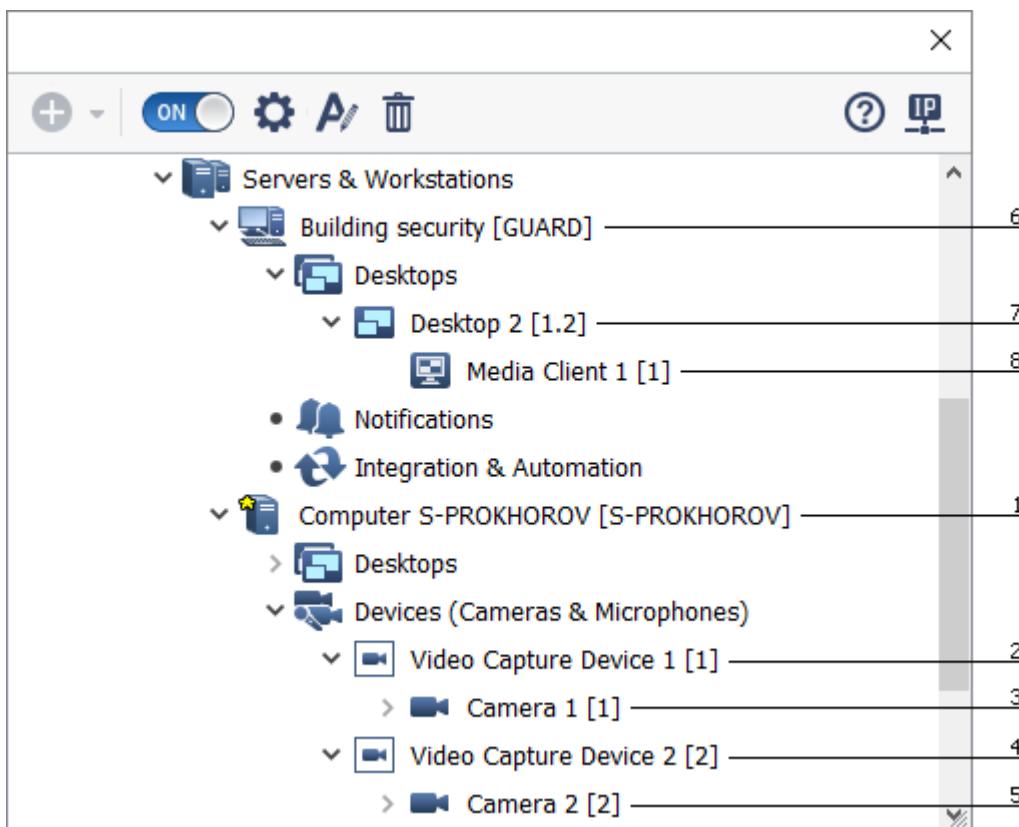


Figure 155. Object tree for server-workstation configuration

Solution: (see figure 155):

Go to administration mode (see [SecurOS Administration Overview](#)) and to the following:

1. Find *Computer* object that corresponds to video server and open its settings window (see [Editing Object Settings](#)). In **Archive** section set **Read** and **Write** value for **Video** parameter at least for one directory (for example drive C:\).
2. Go to *Computer* → *Devices (Cameras & Microphones)* branch in the object tree and create *Video Capture Device* object.

Enter values for following parameters of the objects:

- **Type:** camera vendor;
- **Model:** model of the camera of selected vendor. In some cases parameter stands for the communication protocol between server and camera;
- **Protocol:** version of communication protocol between server and camera. For some models this field may be disabled;
- **IP address:** address of the camera in the TCP/IP network;

- **User and Password:** login and password of the user that has an access to camera's video stream (can be set in the camera's web interface).
3. Create the *Camera* object (child object of the *Video Capture Device* object).
 4. Create second *Video Capture Device* and configure it the same way.
 5. Create the *Camera* object (child object of the second *Video Capture Device* object).
 6. Create *Computer* object with *Operator Workstation* role, which ID and Name corresponds to its destination.
 7. Tick the **Use as Operator Workstation Profile** checkbox in the created *Computer* object settings.
 8. Create *Desktop* child object in the *Desktops* group of objects.
 9. Create *Media Client* object child to recently created *Desktop* object.
 10. Launch SecurOS operator interface on the computer, that will be used as *Operator Workstation*. Specify IP address or DNS/WINS name of the Video Server.

Operator interface containing *Operator Workspace* that corresponds created profile, will be loaded. When client has started, you will see on its display a full-screen *Media Client* with live video from two server-side cameras.

7.9.3 Setting Up Camera

Setting up a camera includes the following operations:

1. [Adding Video Capture Device](#).
2. [Adding Camera to System](#).
3. [Selecting Camera to Work with Media Client](#).
4. [Adding User Rights](#).
5. [Setting up telemetry](#).

7.9.3.1 Adding Video Capture Device

To add a *Video Capture Device* do the following:

1. Enter the Administration Mode.
2. In the *Object Tree* select the *Computer* object to which the added device will be connected.
3. Create child *Video Capture Device* object in the *Devices (Cameras & Microphones)* group.
4. In the **Parameters of created object** window set the required values.
5. In the object properties window (see figure156) set the required values.

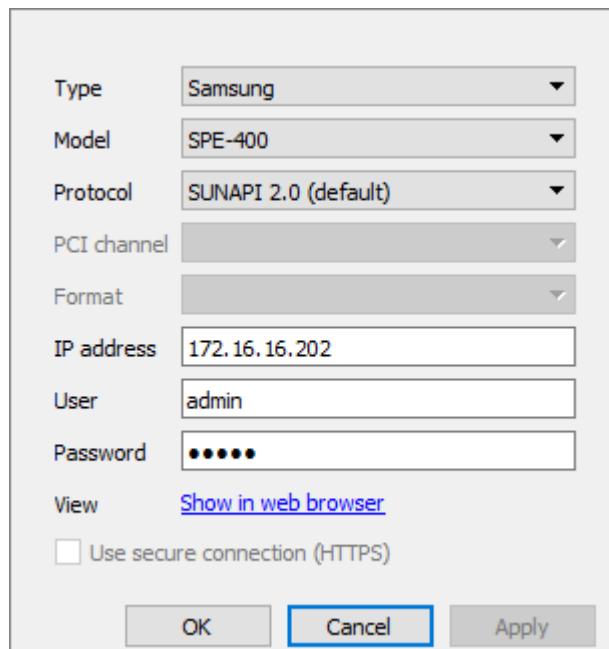


Figure 156. The Video Capture Device object properties window

6. Apply new settings.

7.9.3.2 Adding Camera to System

To add a *Camera* do the following:

1. Enter the Administration Mode.
2. In the *Object Tree* select the created *Video Capture Device* object.
3. Create a *Camera* child object.
4. In the **Parameters of created object** window set the required values.
5. In the object properties window (see figure 157) set the required values.

Note. At this step it is possible to set the PTZ-control. The configuration sequence is described in the [Setting up Telemetry](#) section. This step can also be done later.

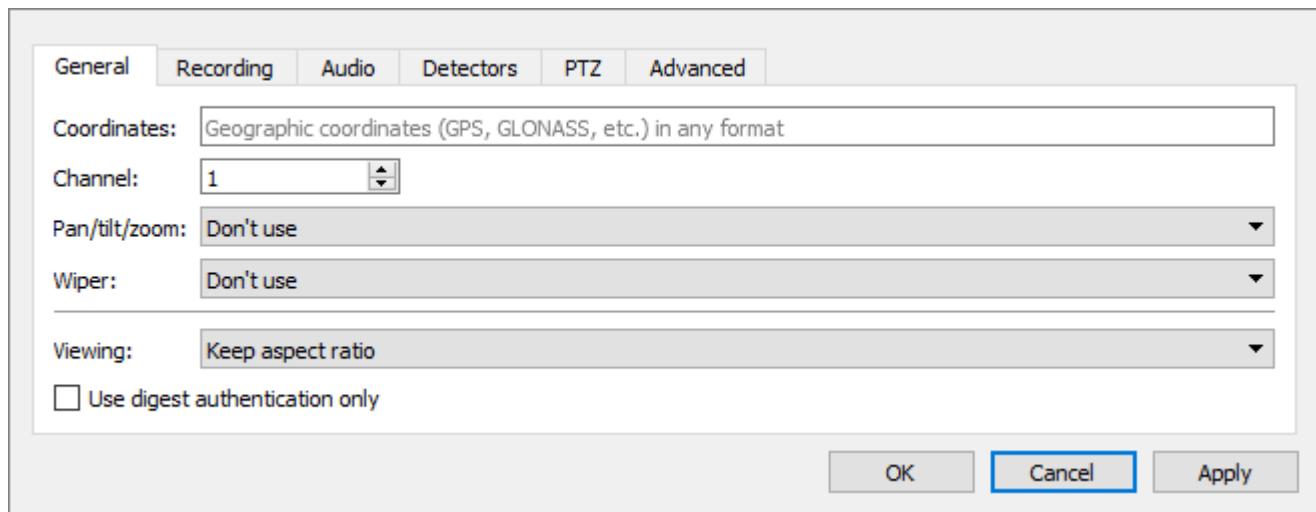


Figure 157. The Camera object properties window

6. Apply new settings.

7.9.3.3 Selecting Camera to Work with Media Client

By default, video streams from all cameras connected to the system will be displayed on each newly created *Media Client*.

To display video streams only from required *Cameras* on the *Media Client* do the following:

1. Enter the Administration Mode.
2. In the *Object Tree* select the *Media Client* on which it is necessary to configure the *Camera* list (**Security Zone** → **Servers & Workstations group** → **Computer** → **Desktops group** → **Desktop** → **Media Client**).
3. Enter *Media Client* object parameter settings mode. In the **Cameras** tab (see Figure 158) do the following:

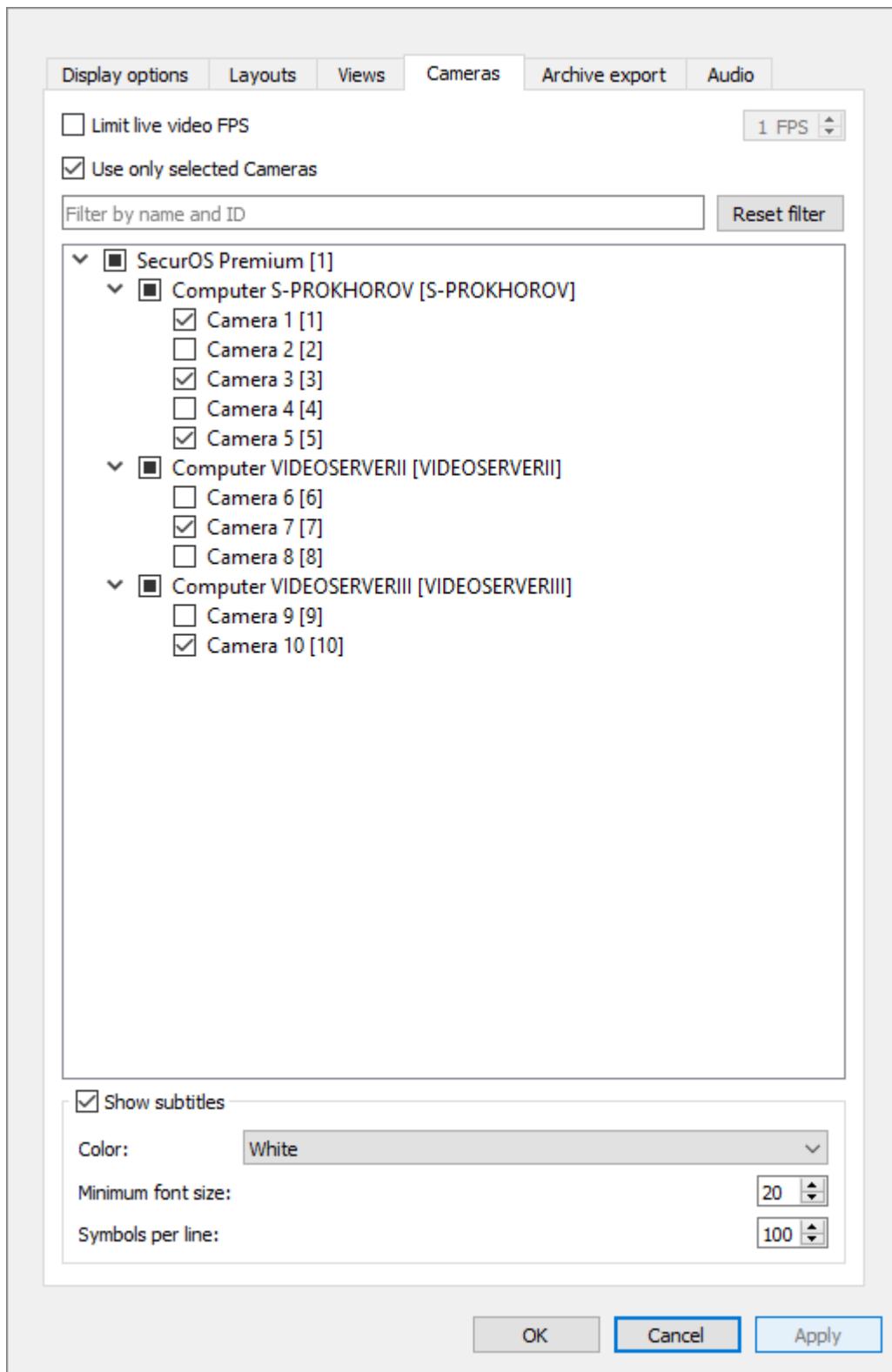


Figure 158. Select Cameras to work with Media Client

- select the **Use only selected Cameras** checkbox.
 - in the *Object tree* select checkboxes on the left of that *Cameras*, image from which must be displayed on the *Media Client*.
4. Apply new settings.

7.9.3.4 Adding User Rights

For the users created by the system by default, the rights to child objects are inherited from the parent objects. In case it is not enough rights inherited by default to control a recently created object, such rights can be assigned manually. For adding user rights to control a recently created object, do the following:

1. Enter the Administration Mode.
2. In the SecurOS *Object Tree* select a *User Rights* object where user or user group, to which a right to control created *Camera* must be granted, is defined.
3. In the User Rights settings window (see figure 159) select the *Camera* object you need, and set the required access level (using the icon on the left side of the object name).

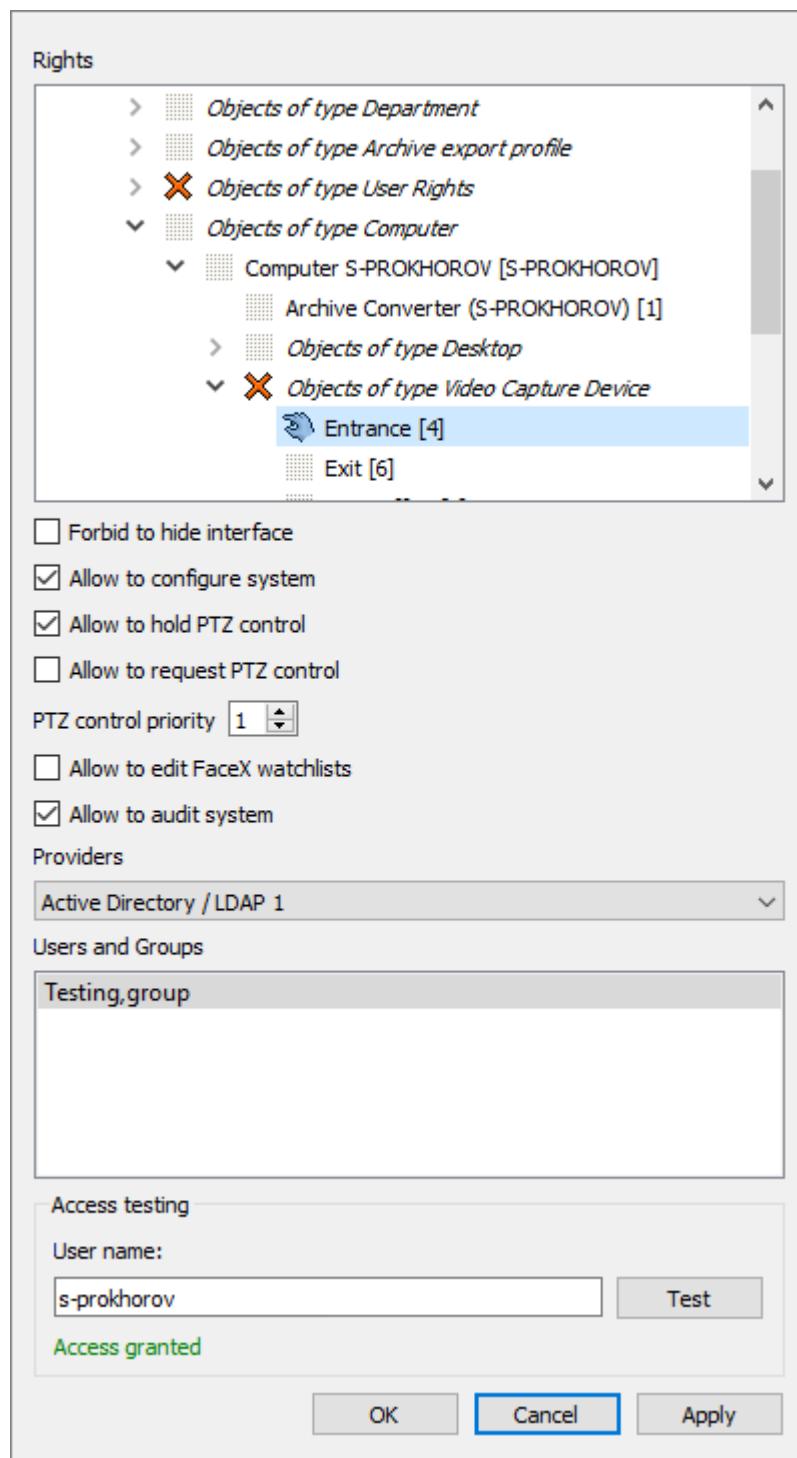


Figure 159. The User Rights object properties window

Note. Detailed information about access levels and its corresponding icons is available in the [User Rights](#) section.

4. If you want to provide an operator with a possibility to hold PTZ control for an unlimited time, tick the **Allow to hold PTZ control** checkbox (see [Holding PTZ Control for a Long Time](#)).
5. If it is necessary to restrict the order of user access to PTZ control (see [Shared Telemetry Control](#) and [Exclusive Telemetry Control](#)) specify required value in the **PTZ Control Priority** field.

Note. Specified priority value is applied to all *Cameras* that can be controlled by the given user.

6. Apply new settings.

7.9.3.5 Setting up telemetry

Telemetry is configured in the **Common** and **PTZ** tabs of the *Camera* object settings.

After PTZ Device configuration, at the activation of a cell of any camera placed on the *Media Client*, the **PTZ** button will be displayed.

When controlled camera is activated, then the *PTZ Control Panel* will be activated on the *Media Client*.

7.9.3.5.1 Setting up telemetry for IP devices

To configure PTZ control for IP devices follow the next steps:

1. Enter the Administration Mode.
2. In the SecurOS *Object Tree* select the *Camera* object (see [Setting Up Camera](#) section) for which it is necessary to configure PTZ control.
3. In the **General** tab, (see fig. 160) from the **Pan/tilt/zoom** drop-down menu select the **Use** option.

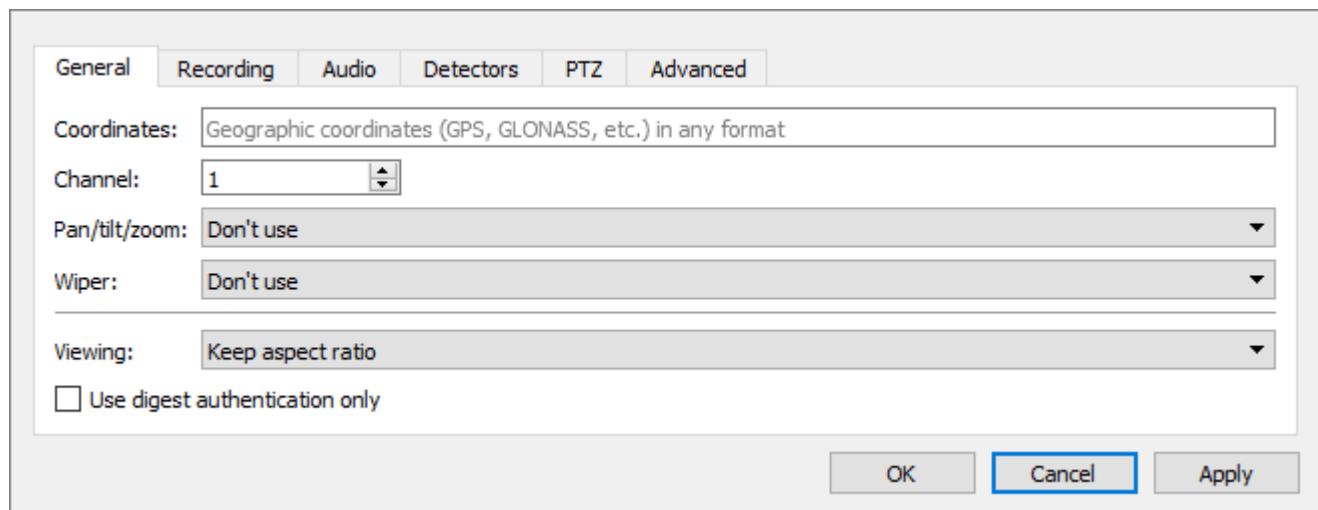


Figure 160. General tab of Camera object settings window

4. In the **PTZ** tab (see Figure 161) configure the corresponding parameters.

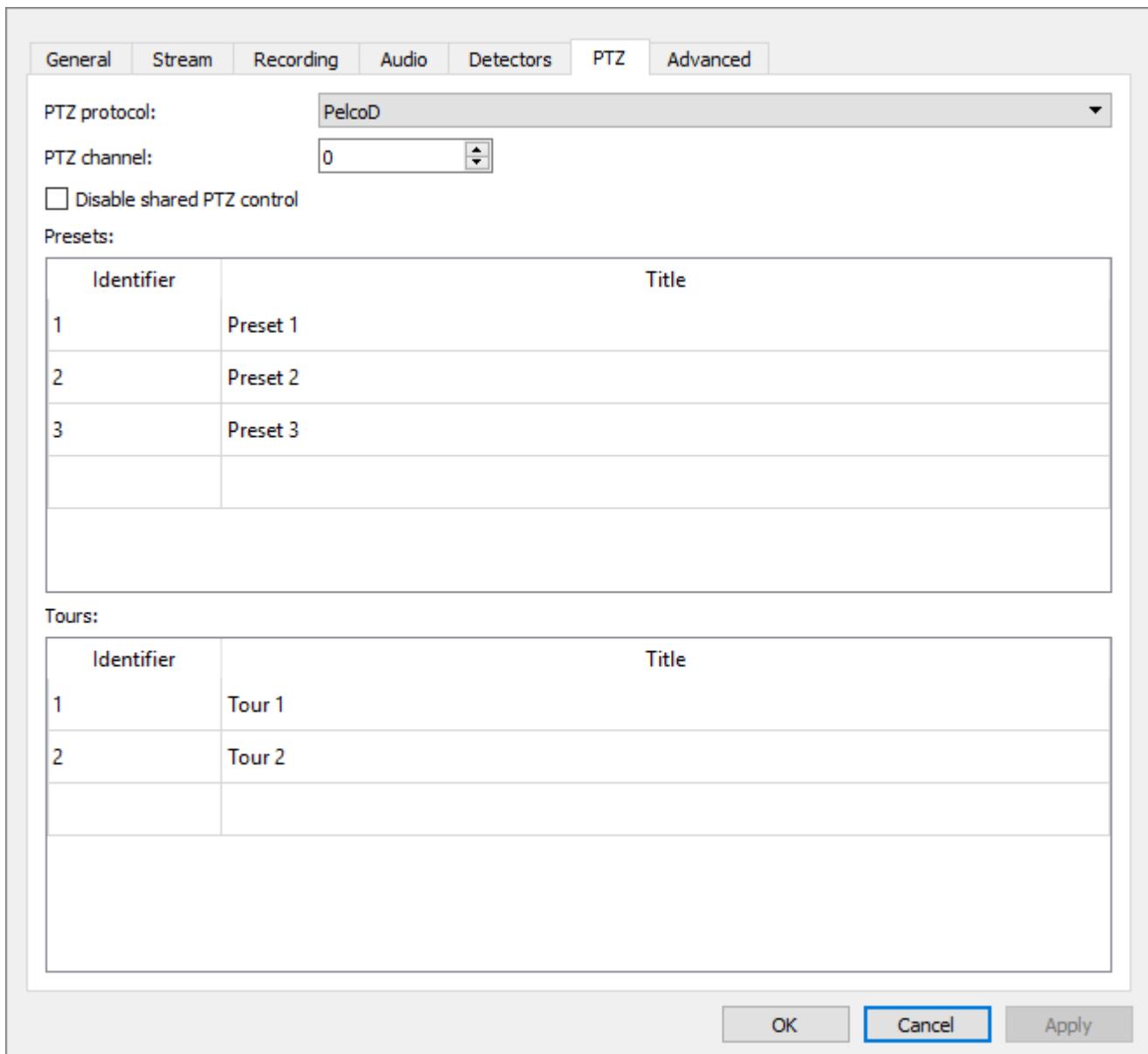


Figure 161. PTZ tab of Camera object settings window

5. Select the PTZ control mode:

- Shared telemetry control – to activate this mode use default value (the **Disable shared PTZ control** checkbox is not selected). Read more about shared PTZ control mode in the [Shared Telemetry Control](#);
- Exclusive telemetry control – select the **Disable shared PTZ control** to activate this mode. Read more about exclusive PTZ control mode in the [Exclusive Telemetry Control](#).

6. If the Exclusive telemetry control mode is selected specify telemetry control priority for each system user (see [User Rights](#)).

7. To activate for operator a possibility to hold PTZ control for a long time, tick the **Allow to hold PTZ control** checkbox in the [User Rights](#) object settings.

8. To display *PTZ Control Panel* on the *Media Client* select the **PTZ Control** checkbox in the [Display options](#) tab of the [Media Client](#) object settings window.

9. To display the **PTZ** button in the *Camera* cell select the **PTZ control via mouse** checkbox in the [Display options](#) tab of the [Media Client](#) object settings window.

10. Apply new settings.

7.9.3.5.1.1 Shared Telemetry Control

In the shared telemetry control mode, all incoming commands are executed. The commands are executed in order they were sent by the operators. Each new command starts executing immediately after it is received. For example, the first operator started patrolling, and the second, after a short period of time, began to rotate the camera with the joystick. In this case, the patrol will be interrupted, the camera will turn.

When working in shared PTZ control mode, then:

- priority of the command sender is not analyzed;
- PTZ control is not blocked;
- commands initiated by *Macros* or *VB/JScript programs* are executed in common turn.

7.9.3.5.1.2 Exclusive Telemetry Control

Warning! Exclusive telemetry control mode is available only for cameras equipped with built-in PTZ device.

When working in exclusive telemetry control mode, there are two options of the operator work:

1. **Capture of PTZ control with automatic control release.**
2. **Capture of PTZ control for a long time with release by operator's command (long-term PTZ hold).**

Capture of PTZ control with automatic release mode is available by default. Option to capture and long-term PTZ hold is configured by system administrator additionally (see **User Rights**, the **Allow to hold PTZ control** parameter). If this option is adjusted, then operator will be able to choose one of two way of work.

For each PTZ control options:

- system analyses priority of the command sender;
- if PTZ control is captured by user, then access to PTZ control is locked for all user with the same or lower PTZ control priority;
- commands initiated by *Macros* or *VB/JScript programs* are executed depending on their priority.

Capture of PTZ control with automatic control release

In this PTZ control mode system works in the following way:

1. Operator sends a PTZ control command.
2. System transfers PTZ control to this operator and analyses all other incoming commands. At the same time:
 - if command was sent by user, whose PTZ control priority is equal to PTZ control priority of the current user or lower, then command is ignored.
 - if command was sent by user, whose PTZ control priority is higher than PTZ control priority of the current operator, then execution of current command is terminated, and new command is started.
3. After command execution is finished, system awaits new command from the same operator during 5 seconds.
4. If such a command was not sent, then system automatically releases PTZ control for any operator within network.

Capture of PTZ control for a long time with release by operator's command (long-term PTZ hold)

In this PTZ control mode system works in the following way:

Note. If possibility to long-term PTZ hold is configured by system administrator, then additional controls are displayed in the camera cell (see [SecurOS Quick User Guide](#)).

1. Operator turns on long-term PTZ hold mode and sends a PTZ control command.
2. System transfers PTZ control to that operator for unlimited period of time and analyses all other incoming commands. At the same time:
 - if command was sent by user, whose PTZ control priority is equal to PTZ control priority of the current user or lower, then command is ignored.
 - if command was sent by user, whose PTZ control priority is higher than PTZ control priority of the current operator, then PTZ control is transferred to this user. In this case system can operate in one of two ways:
 - command was sent in "capture control with automatic release" mode (long-term PTZ hold mode is not turned on) – after executing the command, the system expects a new command from the same operator within 5 seconds. If such a command was not sent, then system automatically releases PTZ control for any operator within network.
 - command was sent after long-term PTZ hold mode was turned on – see paragraph [2](#). When work is finished, PTZ control is released by operator in manual mode or can be released by operator, that has a higher PTZ control priority. The superuser (see [SecurOS Users](#)) can release blocking of any other user, including his own blocking on the different *Computer*.

At the same time, the own priority can be assigned to the telemetry control commands sent by *Macro* and *VB/JScript programs* (priority parameter, see [SecurOS Programming Guide](#)). If this priority value is higher than priority of the *User* that captured telemetry control, then PTZ will be controlled by the command sent from *Macro* or *VB/JScript program*.

When working in the exclusive control mode, the PTZ control panel of the *Media Client* and PTZ control button in the *Camera* cell are disabled for all users except for the user who captured the control and users with higher priority (refer to [SecurOS Quick User Guide](#) for the details).

7.9.4 Joystick Configuration

To use a joystick for control PTZ *Cameras* with the help of the *Media Client* (see [SecurOS Quick User Guide](#)) it is necessary to install and configure it first.

To install and configure a joystick do the following:

1. Connect the joystick to an operator workstation. The device will be detected automatically or drivers should be installed.
2. Find the installed joystick in the devices list (**Control Panel → Game Controllers**) and write down its name exactly as in the list (for example, *Joystick_Name*).
3. Locate the joystick configuration file called *default.xml* in the *\Joy_config* subfolder of the SecurOS root directory. Save this file as the *Joystick_Name.xml* file, into the same subfolder (or alternatively make a copy of the *default.xml* file and rename it accordingly).

4. Click the **Properties** button in the game controllers list, then the **Calibration** tab in the appeared window. Calibrate installed joystick buttons and controls.

Warning! The calibration procedure is absolutely necessary, otherwise the joystick will not function in SecurOS!

8 Audio Subsystem

The audio subsystem is used to operate and configure the audio devices (audio capture cards, microphones) within the SecurOS security network, transmit audio streams between servers and workstations and also work with live and archived audio from within workstations.

8.1 Operation Modes

Working with an audio stream can be carried out in one of the following modes:

1. [Synchronized Audio/Video Recording and Playback](#);
2. [Separate Audio Recording and Playback](#).

Possibilities to use system objects to record and playback audio streams are different for each mode and depend on their settings. Features of each mode are described in detail below.

8.1.1 Synchronized Audio/Video Recording and Playback

In this mode, the video stream is recorded synchronously with the audio stream, which allows to analyze not only video, but also audio information when playing back records.

Synchronized audio/video recording is configured by making a logical link between the *Camera* and the *Microphone* object. Physical devices are linked during the *Camera* object configuration (see [Camera](#) section).

Synchronized audio/video recording and playback is performed by using controls of the *Media Client*'s cell (see [Media Client](#)), that displays live video from *Camera*, to which the appropriate *Microphone* is linked to.

Warning! A *Microphone* linked to a *Camera* can never be used separately from the *Camera* to record arbitrary audio.

For the detailed description of the system configuration operations required to provide synchronized audio recording mode see [Example of System Configuration for Synchronized Audio/Video Recording and Playback](#) section.

8.1.2 Separate Audio Recording and Playback

Separate recording of the arbitrary audio stream is done with the help of *Microphone*, that is not linked to the *Camera* object.

To control separate recording and playback mode the *Media Client* system object is typically used.

8.2 Object Reference

The audio subsystem involves the following classes of objects:

- **Audio Capture Device.**
- **Microphone.**

8.2.1 Audio Capture Device

The object is designed to configure and initialize within SecurOS network the following typical audio sources:

- IP-devices;
- physical audio capture devices installed on the computer, including the following:
 - sound cards;
 - microphones connected to the computer's audio inputs.

Parent object – *Computer\Devices (Cameras & Microphones)* group.

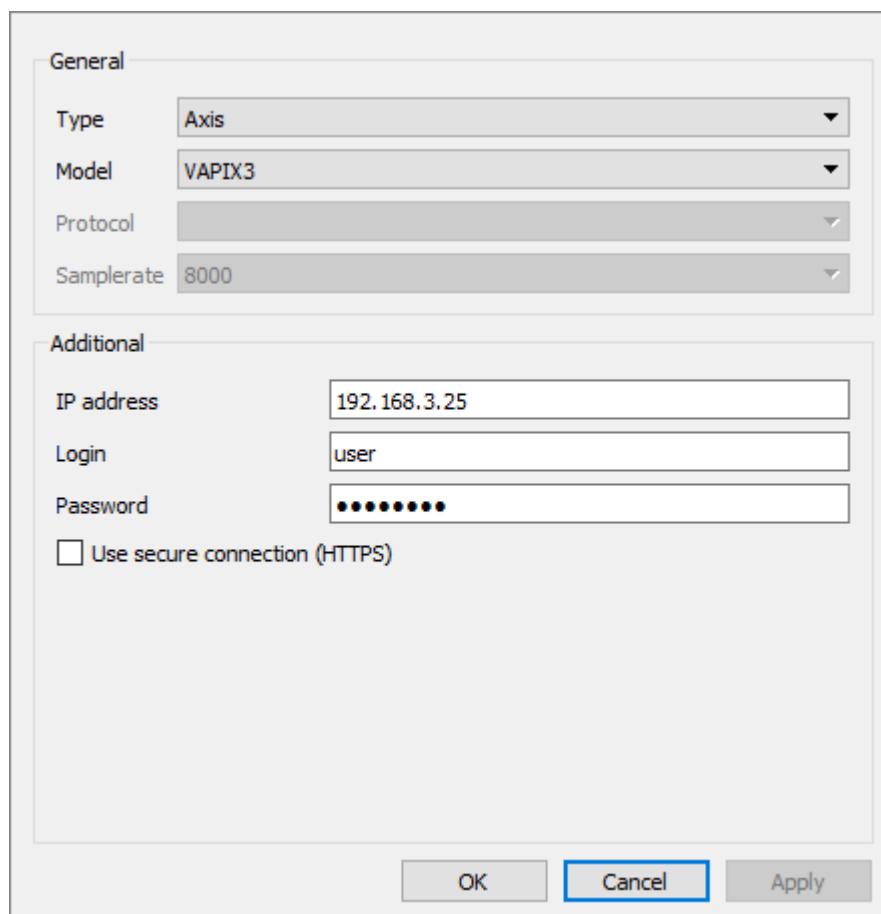


Figure 162. Audio Capture Device object settings window

Table 53. Audio Capture Device object settings

Parameter	Description
General (type independent general parameters of sound source)	
Type	Select audio source type. Mandatory parameter.
Model	Select audio source model. Mandatory parameter. Warning! If SecurOS supports only one model of the device for the selected Type , then parameter is disabled.
Protocol	Select protocol to work with audio source. Warning! If device of the selected Model supports only one protocol, then parameter is disabled.
Samplerate	Select audio source frequency (Hz). Mandatory parameter. Note. The higher the samplerate the better the audio record quality, but more disk space will be required. Warning! This parameter is enabled only for devices, which Type is SoundBlaster. For all other <i>Audio Capture Devices</i> this parameter is disabled.
Additional (type dependent additional parameters of sound source)	
For IP-device	Set the following parameters (see figure 162): <ul style="list-style-type: none">• IP-address – IP-address of audio source within SecurOS network;• Login – user name to access device. Value is set with the help of device's configuration interfaces (see original device' User Manual);• Password – user password to access device. Value is set with the help of device's configuration interfaces (see original device' User Manual).
Use secure connection (HTTPS)	This parameter allows specify the type of connection with the device. To use secure connection do the following: <ul style="list-style-type: none">• tick this checkbox;• use device's web-interface to select HTTPS for user and to select trusted certificate of encryption in own device's settings. Warning! If at least one of the listed conditions is not met, then secure network connection with device will not be established. Note. This parameter is available for Axis and Bosch <i>Audio Capture Devices</i> .

Parameter	Description
For Sound card	<p>Set the following parameters (see figure 163):</p> <ul style="list-style-type: none">• PCI channel – PCI channel number to connect device. Mandatory parameter. Range of values: [1; 64]. Parameter value is unique for each <i>Audio Capture Device</i> child to <i>Computer</i> system object. Default value – min from range of available, excluding already assigned values to other <i>Audio Capture Devices</i>. <p>Note. In case of some microphones are connected to the audio card only one of them can be used.</p>

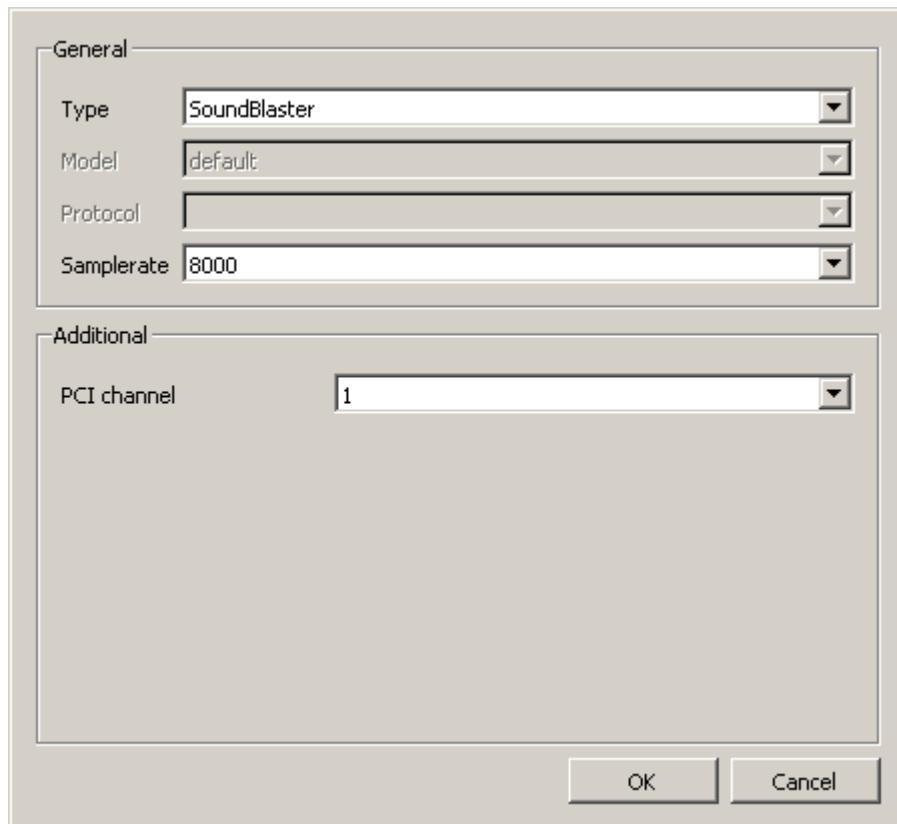


Figure 163. Sound Card or Video Capture Device Settings Window

8.2.2 Microphone

This object represents a single mono channel to connect a microphone.

Parent object – **Audio Capture Device**.

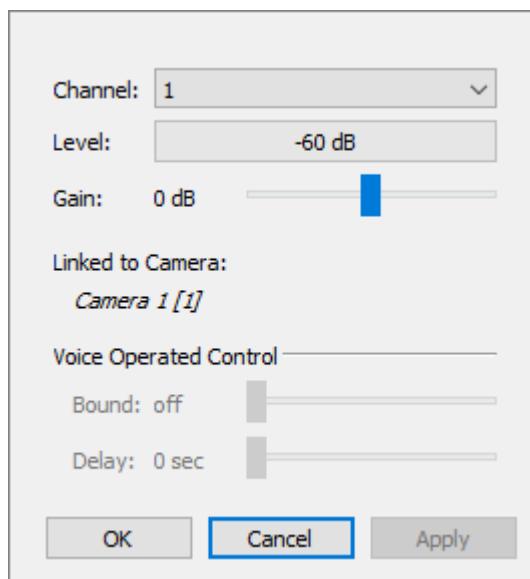


Figure 164. Microphone object settings window

Table 54. Microphone object settings

Parameter	Description
Channel	Select a channel from the list of available channels of the parent Audio Capture Device object.
Level	Information field: Read-only indicator of current volume level. Used to test microphone on-the-fly.
Gain	Choose gain level (-12...12 dB). Increase gain if your audio source is weak. Use Level indicator above to visually control volume level.
Linked to Camera	If <i>Microphone</i> linked to the <i>Camera</i> (see Audio Tab) the Name and ID of the corresponding <i>Camera</i> are displayed in this field. Otherwise (free <i>Microphone</i>) no is displayed in this field.

Voice Operated Control (feature of automatic sound recording upon reaching threshold volume).

Note. This set of parameters is valid only for separate audio recording mode (see **Separate Audio Recording and Playing Back** section).

Warning! In order to trigger Voice Operated Control, *Microphone* must be armed using **Macro** or **VB/JScript program**, or must be set to recording mode with the help of *Media Client*.

Bound	Move slider to specify threshold level (from -60 to 0 dB). When volume reaches this level, automatic sound recording starts. Use Level indicator above to visually estimate current volume level. If set to Off, voice operated control feature is disabled.
Delay	Specify the pot-recording time (sec) in case recording is activated through the Voice Operated Control mode.

8.3 Example of System Configuration for Synchronized Audio/Video Recording and Playback

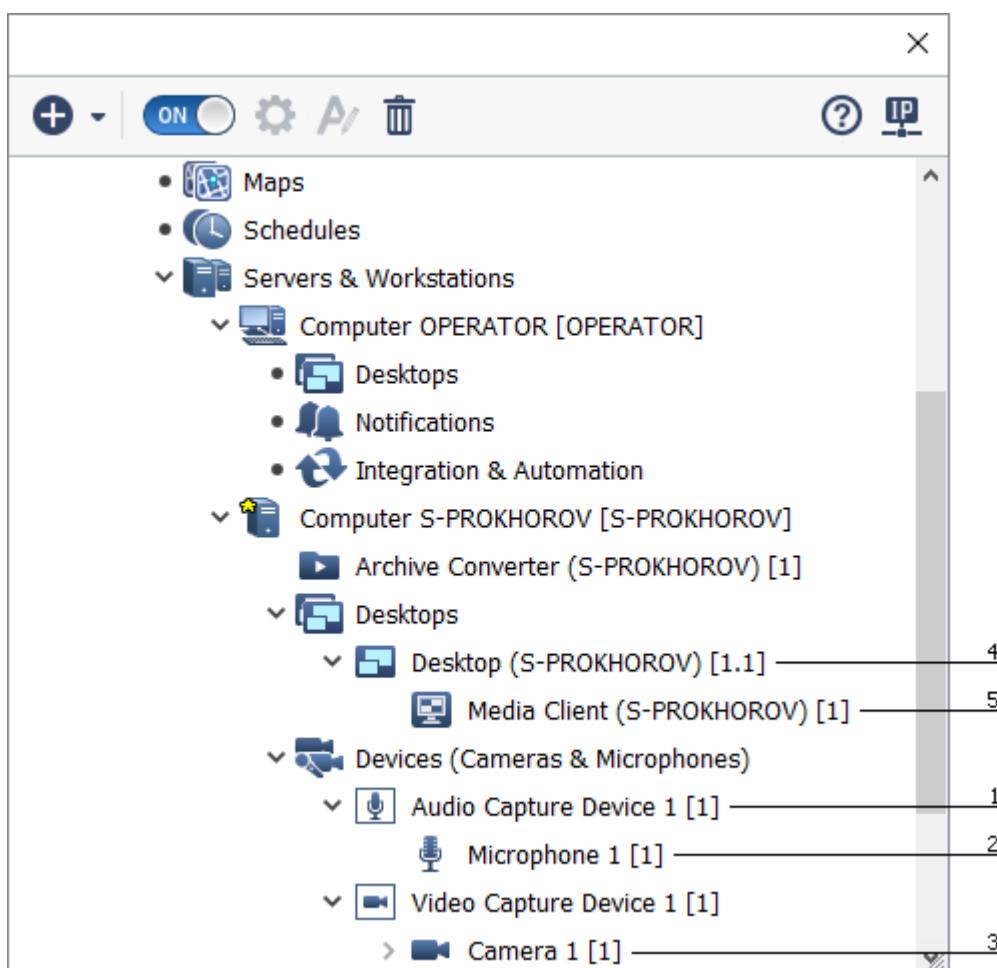


Figure 165. Object Tree for Workstation Configured for Synchronized Audio/Video Recording

To configure synchronized Audio/Video Recording and Playback Mode do the following:

1. In the object tree choose the *Computer* object which represents the physical computer with the installed or connected appropriate hardware, then create a *Audio Capture Device* child object in the *Devices (Cameras & Microphones)* group (see [Audio Capture Device](#)). Set up its specific parameters depending on device type.
2. For the created *Audio Capture Device* create a *Microphone* child object (see [Microphone](#)). Default parameter values are normally sufficient for audio recording.
3. To link a created microphone to a certain camera, select appropriate microphone in the *Camera* object's **Microphone** parameter drop-down list (see [Camera](#)). After that it will be possible to watch the live video with audio. Audio/video will also be recorded synchronously.
4. Choose the *Desktops* group of the corresponding *Computer* object and create a *Desktop* child object.
5. For the created *Desktop* create a *Media Client* child object where place the *Camera* with linked *Microphone*.

9 I/O Subsystem

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*, *SecurOS Xpress*.

The I/O subsystem is used to control and configure general purpose I/O devices (sensors and relays) within the SecurOS network.

Note. Universal I/O devices are connected to supported IP devices.

9.1 Object Reference

The I/O subsystem includes the following objects:

- **Sensor**.
- **Relay**.
- **CCTV Keyboard or joystick**.

9.1.1 Sensor

This object represents a physical sensor device or a daisy chain of sensors (security loop).

When *Sensor* is triggered, this event is added to the *Event Viewer*, from which one can jump to the *Media Client* to view corresponding video. If *Sensor* linked with several *Cameras*, all these *Cameras* will be displayed on the *Media Client*. This functionality allows you to synchronously view video, corresponding to the moment the sensor is triggered, from various monitored zones.

Parent object – **Video Capture Device**.

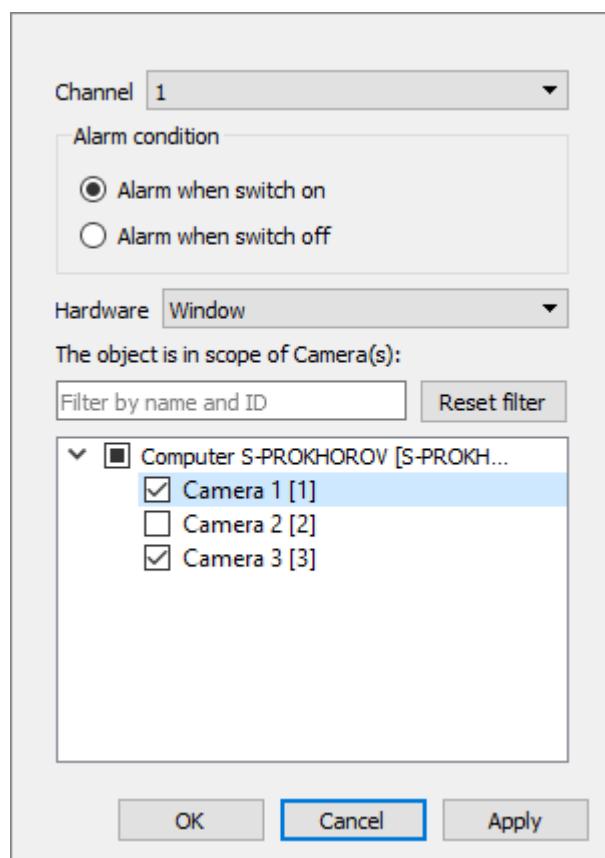


Figure 166. Sensor object settings window

Table 55. Sensor object settings

Parameter	Description
Channel	Select channel number the sensor is connected to.
Alarm condition	Select the type of alarm condition. Possible values: <ul style="list-style-type: none"> • Alarm when switch on – check this option to trigger alarm state when contacts are short circuited; • Alarm when switch off – check this option to trigger alarm state when contacts are open.
Hardware	Select the most appropriate sensor type (this only changes device's icon on <i>Map</i> , not its behavior).
The object is in scope of Camera(s):	
Filter	To search object by name (part of its name) or by ID, type required characters in the field; only those objects that meet the search condition will automatically be displayed in the tree. To clear the field click the Reset filter button.

Parameter	Description
Object tree	<p>Object Tree of the <i>Computers</i> having role <i>Video Server</i> existing within the SecurOS network. When expanding the <i>Video Server</i> node all <i>Camera</i> children objects are displayed.</p> <p>Tick the checkboxes for the <i>Cameras</i> that you want to watch video from when the <i>Sensor</i> is triggered.</p>

9.1.2 Relay

This object represents an electrically operated switch (e. g. relay) that controls some device.

Parent object – [Video Capture Device](#).

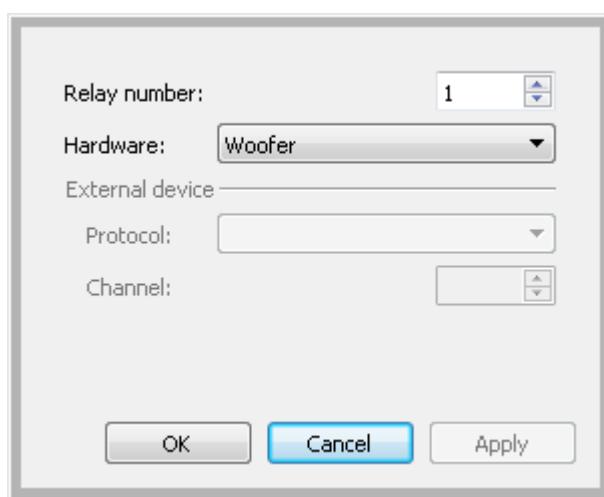


Figure 167. Relay object settings window

Table 56. Relay object settings

Parameter	Description
Relay number	Select the channel number the relay is connected to.
Hardware	Select the most appropriate device type controlled by this relay (this parameter changes device's icon on map). Possible values: Lock, Woofer, Light, Wiper.
External device	
Protocol	Select the protocol to connect to the control device (the parameter is used to control a Wiper).
Channel	Select the channel to connect to the control device (the parameter is used to control a Wiper).

9.1.3 CCTV Keyboard or joystick

CCTV keyboards are designed to control user interface objects (for example, *Media Client*), cameras and their modes, to execute operations with layouts, record operations, etc.

SecurOS supports the following types of keyboards:

- Keyboards that must be configured by *CCTV Keyboard or joystick* object;
- Plug and Play keyboards that do not require any additional configuration.

Parent object – **Computer**.

Within the object settings the following keyboards can be configured:

- **Bosch Intuickey**;
- **Hikvision DS-1100KI**;
- **Panasonic WV-CU950**;
- **Pelco KBD300A**.

The following keyboards do not require any configuration:

- AXIS T8311;
- Bosch KBD-Universal-XF.

Note. See **SecurOS Quick User Guide** to learn how to operate keyboards described above.

Device type is selected in the object settings window.

Warning! Please view DevicesIntegrationList for additionally supported USB joysticks.

9.1.3.1 Bosch Intuickey

Warning! The PL-2303 chipset of the COM port must be supported by used operation system to use the keyboard properly. It can be checked on the manufacturer http://www.prolific.com.tw/US>ShowProduct.aspx?p_id=225&pcid=41 web-page.

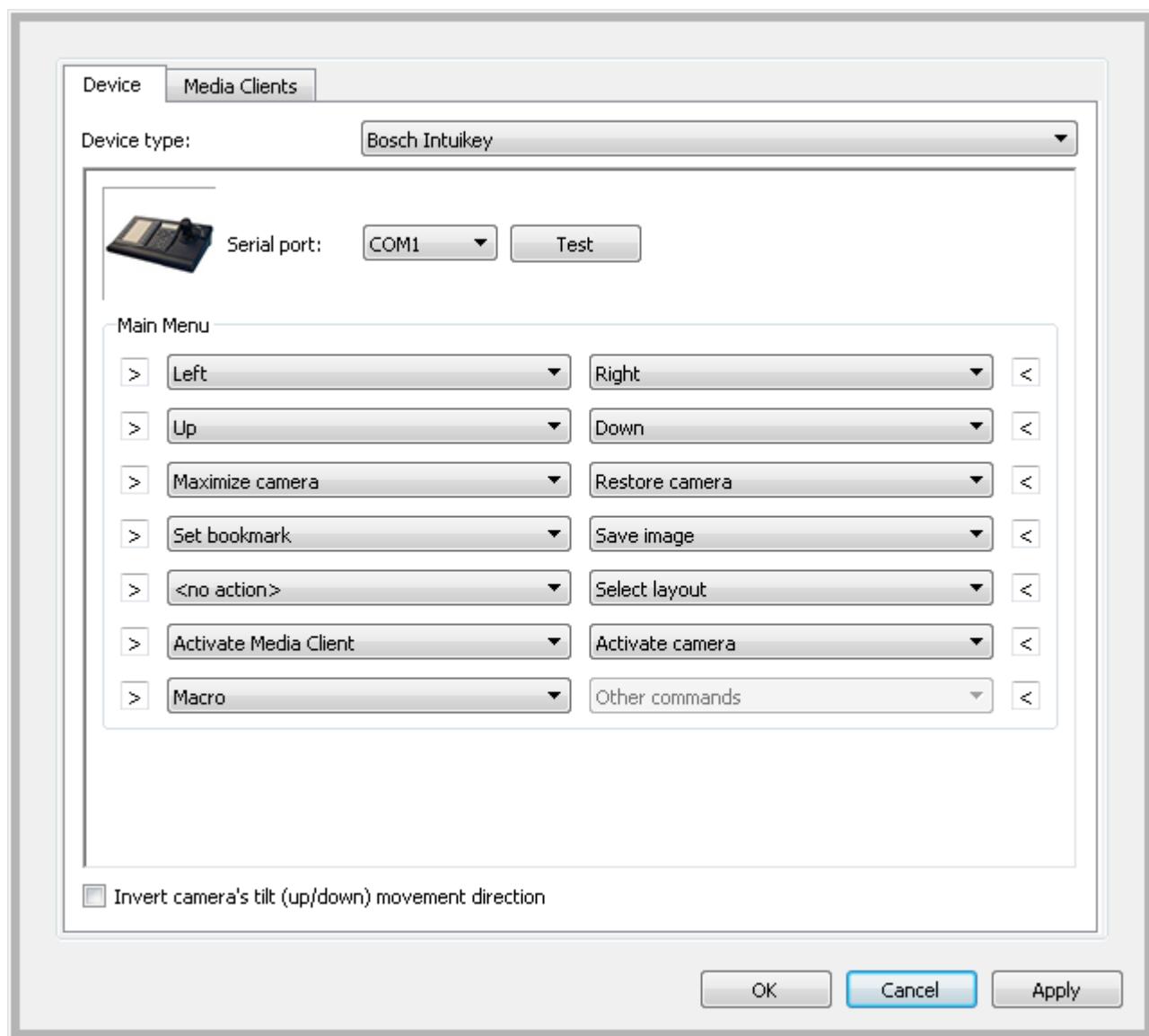


Figure 168. Bosch Intuikey object settings window

Warning! Code page that is used when transferring text data from SecurOS to the keyboard, is specified by **Format** parameter (**Control panel → Clock, Language and Region → Region and Language → Format**).

Table 57. Bosch Intuikey object settings

Parameter	Description
Serial port	Serial port to connect device.
Test (button)	Is used to check if device is available when specified COM port is used for connection (see Checking Keyboard Connection).
Main Menu	Programmable buttons and assigned actions. List is populated with SecurOS commands that are supported by the device. Note. The Other commands is used for all other commands that are not specified in the Main Menu .
Invert camera's tilt (up/down) movement direction	Select this checkbox to invert vertical camera movement when moving joystick's shaft up and down.

Checking Keyboard Connection

To check keyboard connection do the following:

1. Select appropriate **Serial port**, click the **Test** button. System will display the **Check the keyboard connection** window (see figure 169).

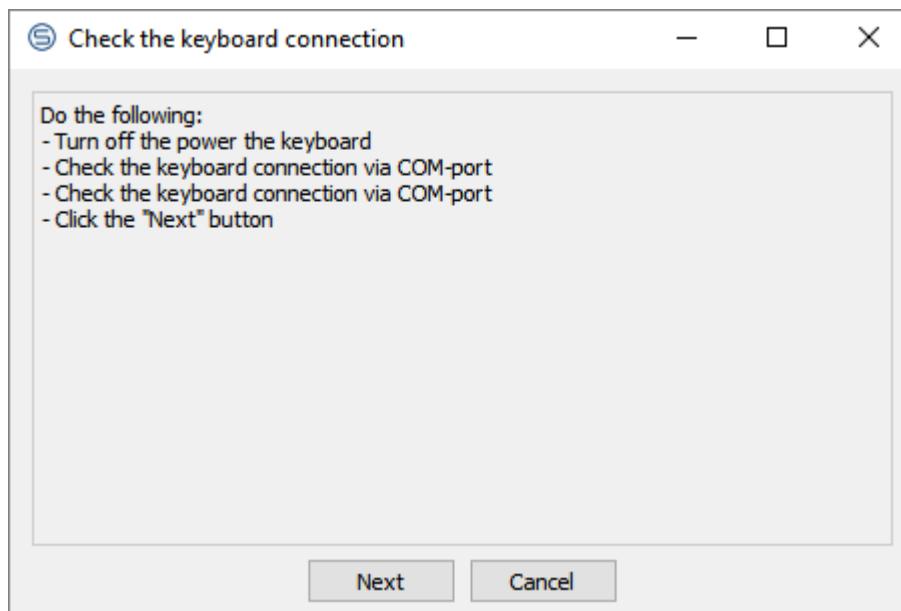


Figure 169. Check the keyboard connection window

2. Perform operations (step by step), listed in the window. Click the **Next** button.
3. Follow the instructions displayed in the window.

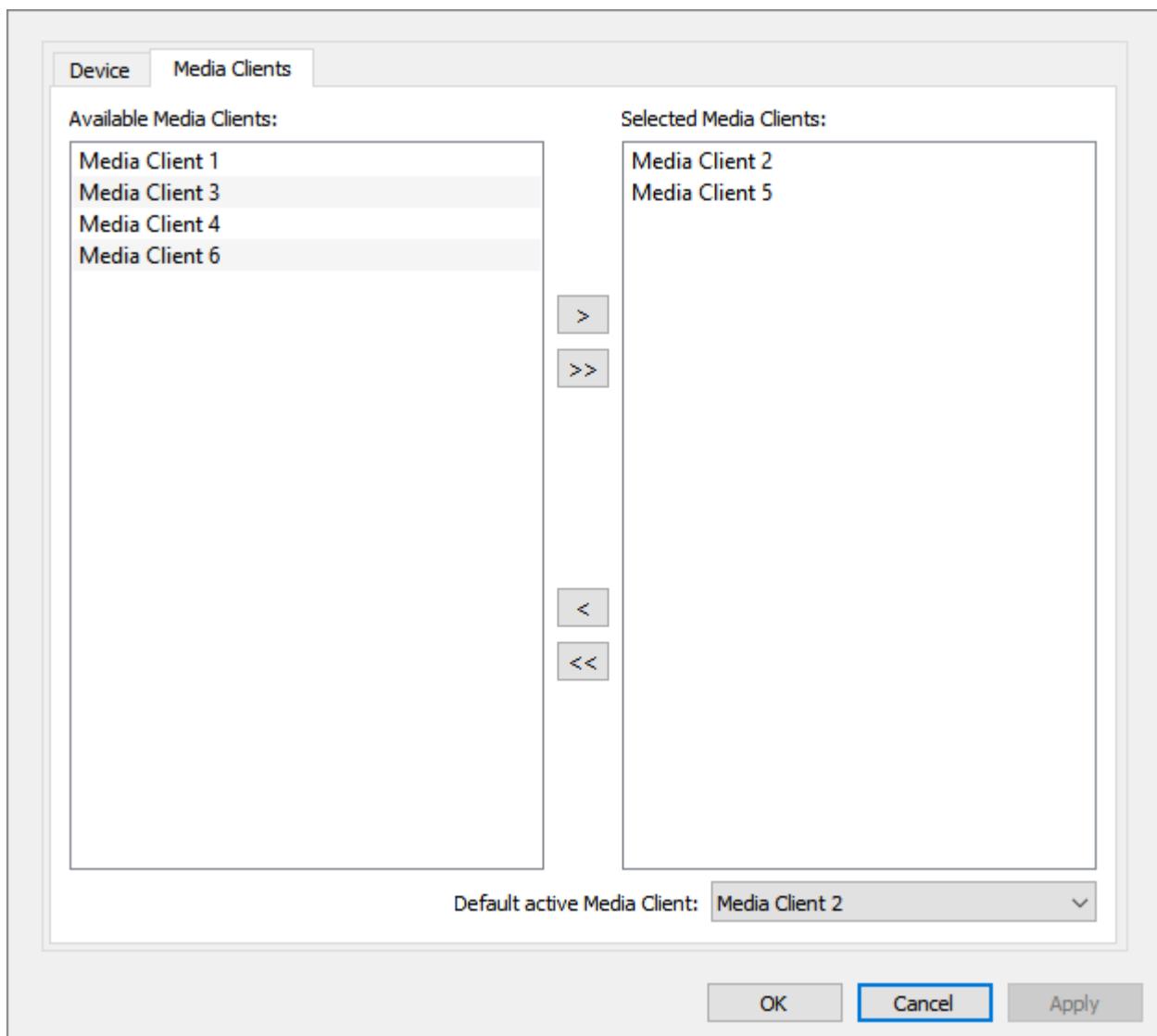


Figure 170. Device settings window. Media Clients tab

Media Clients tab is used to create a list of *Media Clients*, that can be controlled with the configured device.

Note. At the moment only one *Media Client* can be controlled with the *CCTV Keyboard or joystick*.

Table 58. Media Clients tab

Parameter	Description
Available Media Clients	List of all <i>Media Clients</i> that are children of the same <i>Computer</i> , as an object is being configured. To define <i>Media Client</i> that can be controlled, select required one and click the > button.
Selected Media Clients	List of the <i>Media Clients</i> that can be controlled with the given <i>CCTV Keyboard or joystick</i> object.

Parameter	Description
Default active Media Clients	<p><i>Media Client</i>, which will be selected for control with the <i>CCTV Keyboard</i> by default after SecurOS startup. Possible values: any <i>Media Client</i> from the list of Selected Media Clients.</p> <hr/> <p>Note. In order to change controlled <i>Media Client</i> when working with the system use the device interface to enter it's ID or select <i>Media Client</i>'s name from the list (see User Manual for the appropriate <i>CCTV keyboard</i>).</p>

9.1.3.2 Hikvision DS-1100KI

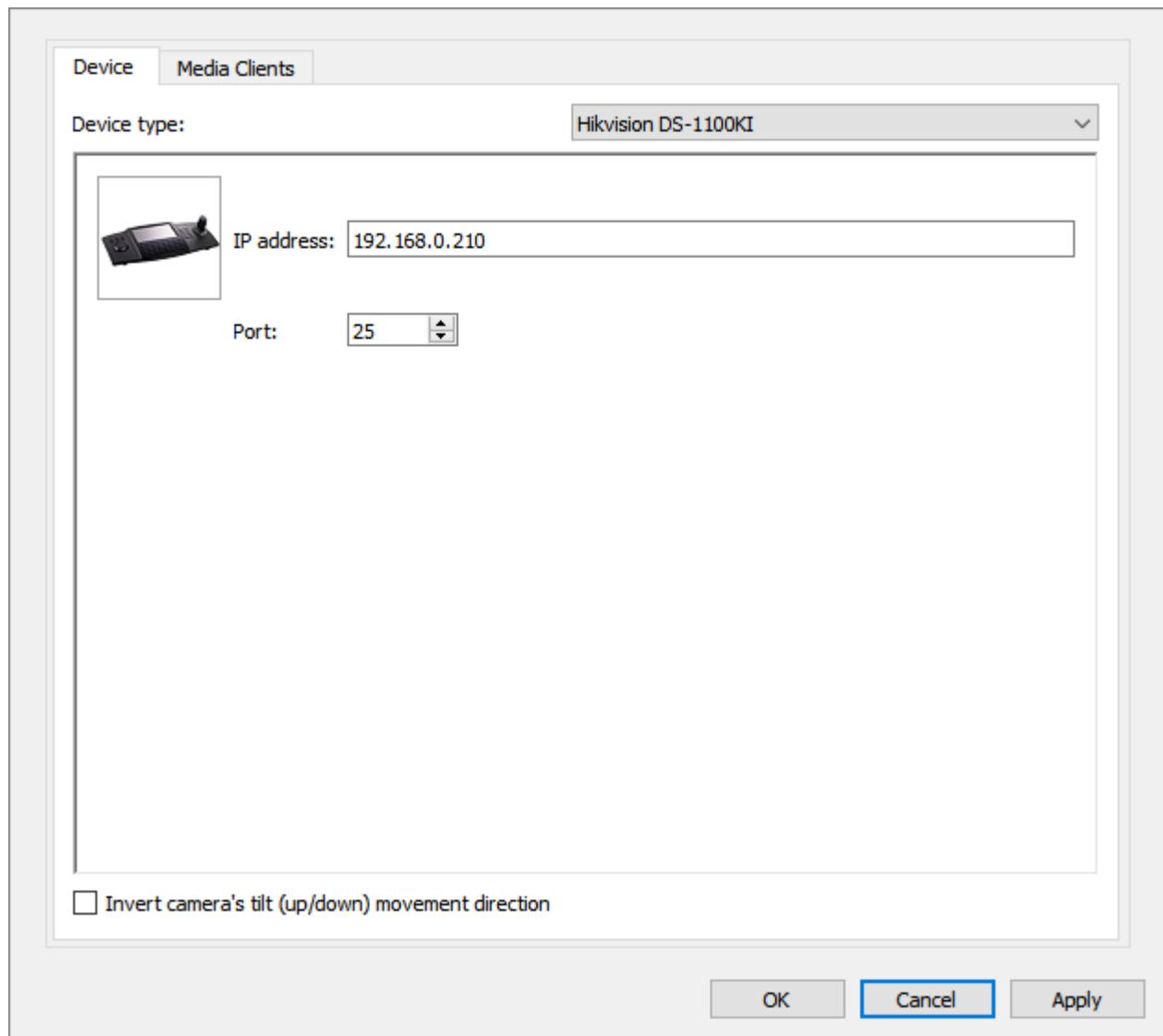


Figure 171. Hikvision DS-1100KI object settings window

Table 59. Hikvision DS-1100KI object settings

Parameter	Description
IP address	IP address of the device.

Parameter	Description
Port	Network port that is used to communicate with the keyboard.
Invert camera's tilt (up/down) movement direction	Select this checkbox to invert vertical camera movement when moving joystick's shaft up and down.

Media Clients tab and its actions are described in the [Bosch IntuiKey](#) section.

9.1.3.3 Panasonic WV-CU950

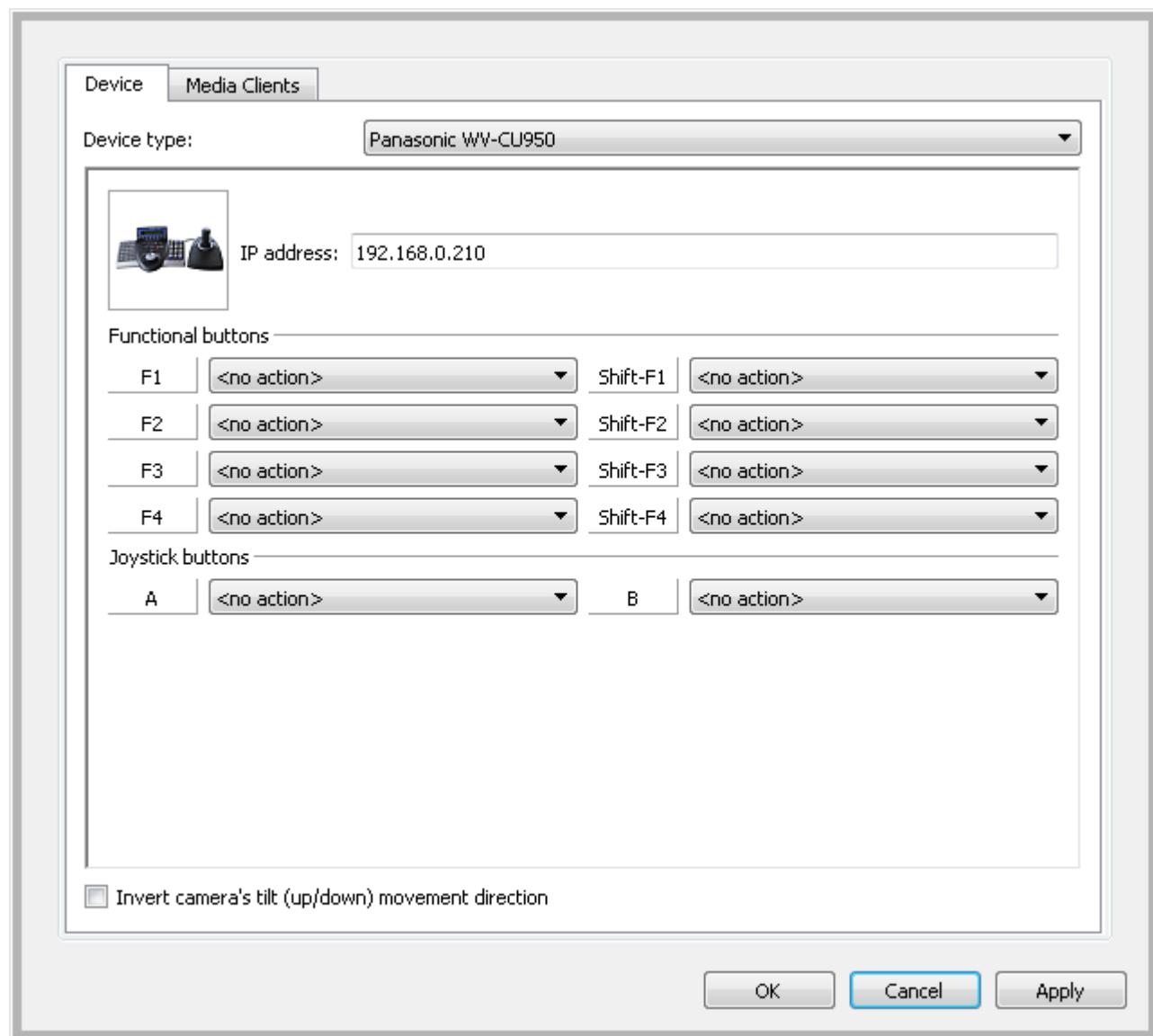


Figure 172. Panasonic WV-CU950 object settings window

Table 60. Panasonic WV-CU950 object settings

Parameter	Description
IP address	IP address of the device.

Parameter	Description
Functional buttons	Programmable buttons and assigned actions. List is populated with SecurOS commands that are supported by the device.
Joystick buttons	Joystick's programmable buttons and assigned actions. List is populated with SecurOS commands that are supported by the device.
Invert camera's tilt (up/down) movement direction	Select this checkbox to invert vertical camera movement when moving joystick's shaft up and down.

Media Clients tab and its actions are described in the [Bosch IntuiKey](#) section.

9.1.3.4 Pelco KBD300A

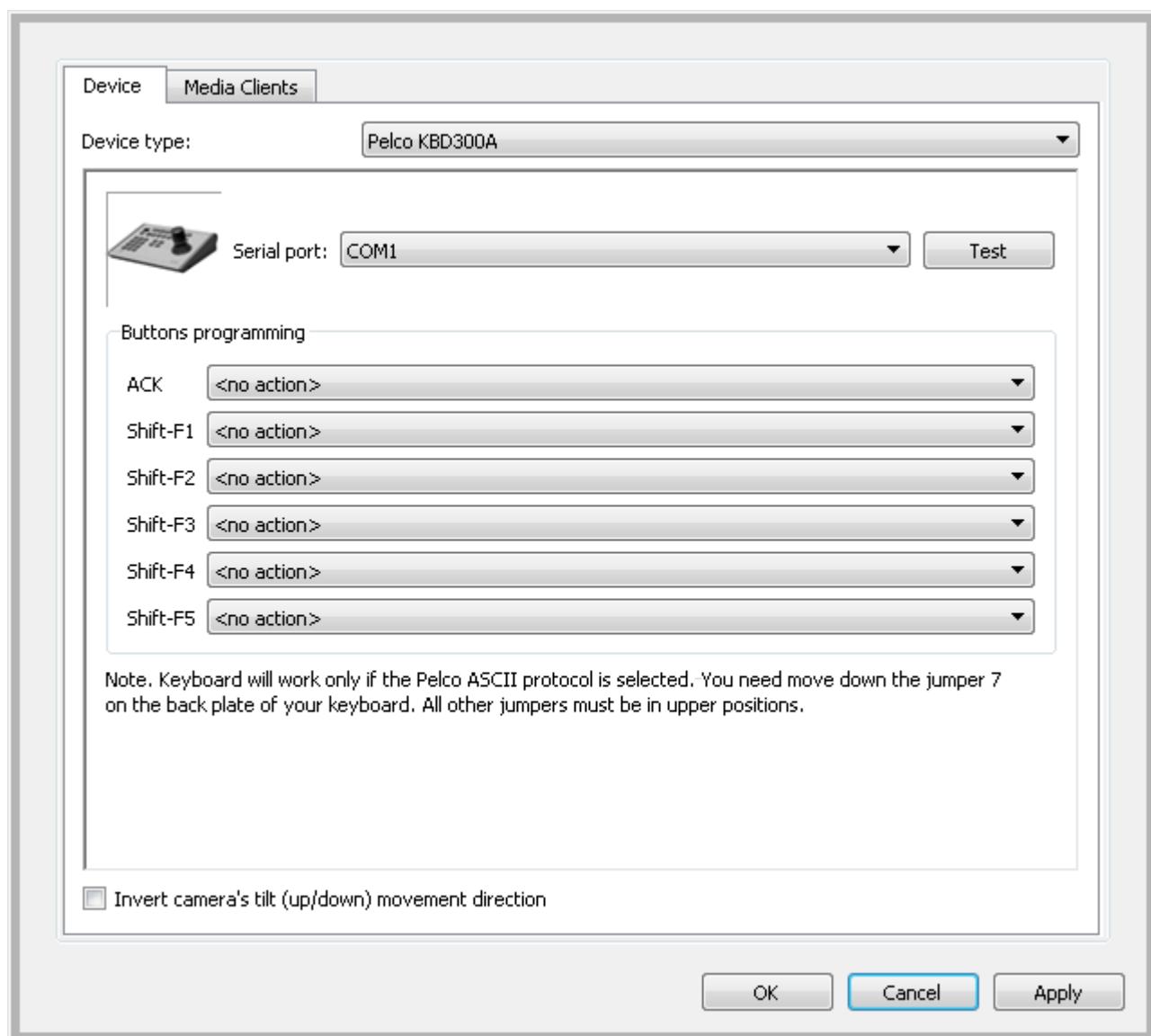


Figure 173. Pelco KBD300A object settings window

Table 61. KBD300A object settings

Parameter	Description
Serial port	Serial port to connect device.
Test	Press to check if device is available when connecting using the specified port number.
Button programming	Programmable buttons and assigned actions. List is populated with SecurOS commands that are supported by the device.
Invert camera's tilt (up/down) movement direction	Select this checkbox to invert vertical camera movement when moving joystick's shaft up and down.

Media Clients tab and its actions are described in the [Bosch IntuiKey](#) section.

9.2 Configuring System to Work with Wiper

The wiper is an optional component of the PTZ device designed to be mounted on the video camera and used to clean the lens remotely.

The ability to support wiper and wiper configuration parameters are normally specified in the camera specification.

Wiper configuration and control are performed with the help of the following SecurOS objects:

- *Relay* – is used to configure *Wiper* control parameters. Not required for cameras with built-in wiper;
- *Camera* – object settings define the *Relay* object, that is used to control the *Wiper* for the given camera.

To configure the *Wiper* for a just installed camera, do the following:

1. In the SecurOS object tree create the [Video capture device](#) object with child [Camera](#) object appropriate to the camera mounted;
2. Create [Relay](#) child object for the created *Video capture device*;
3. In the *Relay* object settings window select the appropriate **Hardware** (*Wiper*). Define its **Protocol** and **Channel** control parameters if necessary;
4. In the created *Camera* object settings jump to the **General** tab and select the created *Relay* object or the *Built-in* value in the **Wiper** drop-down list;
5. If *Media Client* works with the list of cameras add created *Camera* to the **Use only selected Cameras** list. To display *Wiper* control option () in the *Camera* cell in the *Media Client* operator must have not less than **Control** access level for this camera.

10 Notification Subsystem

The notification subsystem allows to inform personnel of events within the security network by the means of e-mail, voice phone calls, SMS messaging and audible notifications. Notifications for object events can be configured using Macros or Scripts (see [SecurOS Programming Guide](#)).

10.1 Object Reference

The notification subsystem includes the following objects:

- [HTML Dialog](#).
- [E-mail Message Service](#).
- [E-mail Message](#).
- [Short Message Service](#).
- [Short Message](#).
- [Audible Notification Service](#).
- [Emergency service](#).

10.1.1 HTML Dialog

This object is used to call pop-up HTML windows, that are displayed on the Monitor dynamically as a response to the external event or system behavior. For example, an HTML Dialog can be activated with the help of a *VB/jScript Program* when processing events. Objects of this type can be closed manually or automatically by the system (and also by scripts). For example, pop-up HTML window may represent control interface or simple message.

More details on operations with HTML dialogs are given in [SecurOS Programming Guide](#).

Parent object – *Computer\Notifications* group.

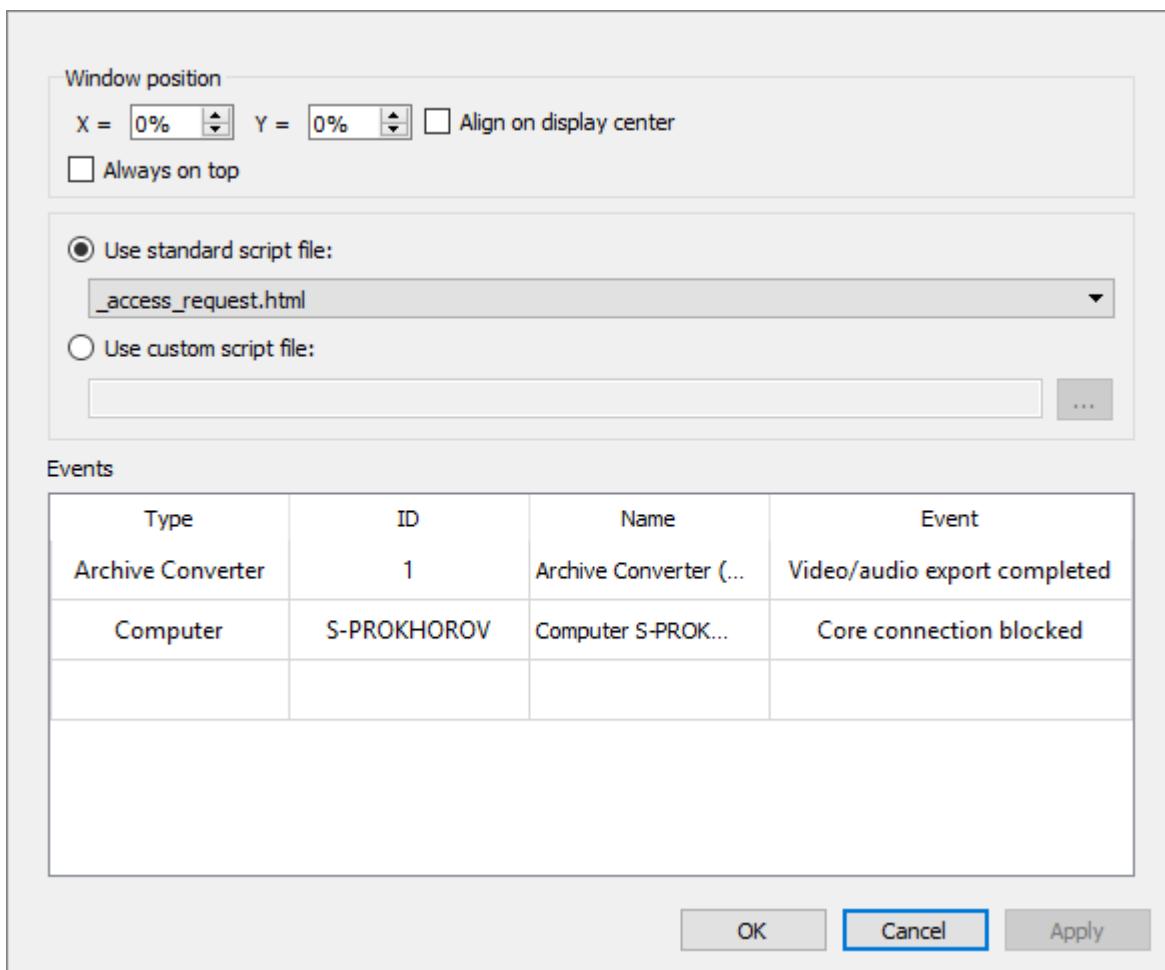


Figure 174. HTML Dialog object settings window

Table 62. HTML Dialog object settings

Parameter	Description
Window position	
X, Y	Specify coordinates of the HTML window's top left corner on the screen in percent, relative to the desktop top left corner.
Align on display center	Select the checkbox to display HTML window in the center of the screen.
Always on top	Select the checkbox to display HTML window in front of all windows.
Scripting	
Use standard script file	<p>Select this option to use default HTML form that is included in SecurOS. Select file with form's HTML source code from the list.</p> <hr/> <p>Note. Default HTML forms are located in <SecurOS_Folder>\Dialogscript directory.</p>

Parameter	Description
Use custom script file	<p>Select this option to use custom HTML form created by user. Enter the following into the field:</p> <ul style="list-style-type: none"> • HTML file name, if HTML source code is located in <SecurOS_Folder>\Dialogscript directory; • full path to HTML file, if HTML source code is located somewhere else. <hr/> <p>Notes:</p> <ol style="list-style-type: none"> 1. To specify the path with help of file manager click the  button. 2. It is unable to specify path with file manager when configuring remotely.
Events	In the table specify events for which the HTML form must be displayed (see Scripts parameter). Table contains following fields: <ul style="list-style-type: none"> • Type – type of SecurOS object; • ID – identifier of the object of selected type; • Name – name of the object; • Event – event occurred with the object.

10.1.2 E-mail Message Service

This object represents an SMTP service which will be used to send E-mail notifications.

Parent object – *Computer\\Notifications* group.

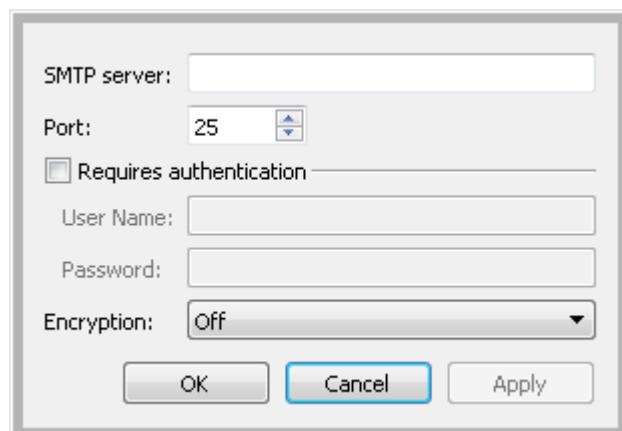


Figure 175. E-mail Message Service object settings window

Table 63. E-mail Message Service object settings

Parameter	Description
SMTP Server	Specify IP address or DNS/WINS name of the SMTP server. You can either use local or external SMTP servers, or install SMTP service on the local computer (see SMTP Mail Server Installation and Configuration). Mandatory parameter.
Port	Specify SMTP server port. Default value is 25.
Requires authentication	Select this checkbox if your SMTP server requires authentication. Warning! If this field is checked, then the checkboxes of the next two parameters will be activated.
User Name, Password	Specify user name and password for SMTP authentication.
Encryption	Choose an encryption protocol from the list. Possible values: Off – encryption is not used (default value). SSL/TLS – use the SSL/TLS protocol. STARTTLS – use the STARTTLS protocol.

10.1.3 E-mail Message

Object represents an individual e-mail message (or a message template). Use *Macros* and *VB/JScript Programs* to send e-mail messages.

Parent object – [E-mail Message Service](#).

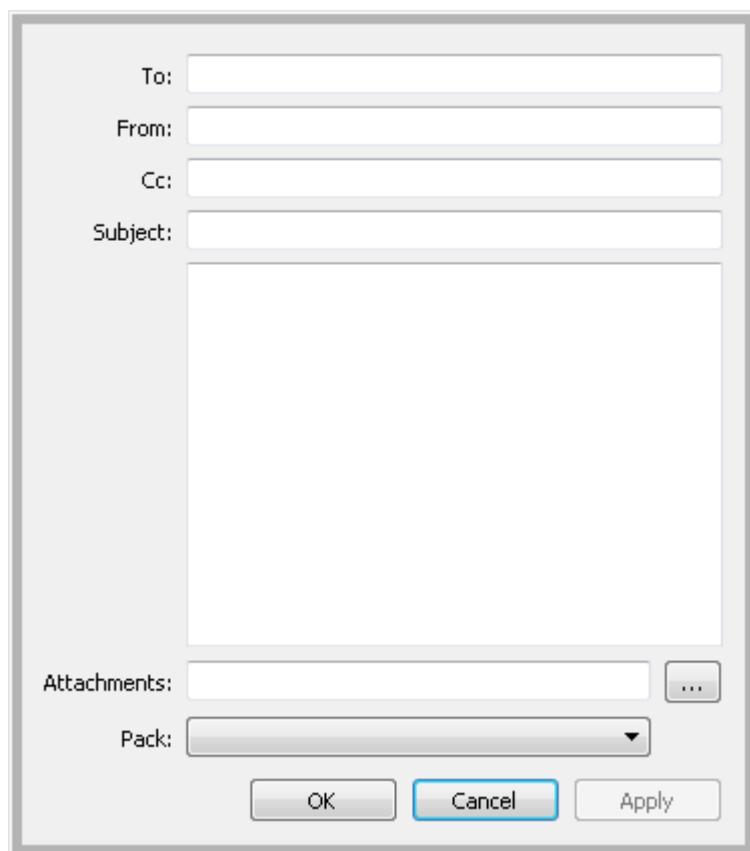


Figure 176. E-mail Message object settings window

Table 64. E-mail Message object settings

Parameter	Description
To	Specify e-mail address of a recipient. You can specify several addresses separated by a semicolon. For example, admin@domain.com; security@domain.com.
From	Specify e-mail address of a sender. You can specify several addresses separated by a semicolon.
CC	Specify e-mail address to which you want to send copy of the message. You can specify several addresses separated by a semicolon.
Subject	Specify subject of the message. You can specify variable parameters here in #param_name\# format. The real parameters are substituted automatically when the message is sent. Parameters are useful when sending e-mail messages from scripts.
Message field	Type in the message body. You can specify variable parameters here.

Parameter	Description
Attachments	Select the files that should be attached to the message. Format: a string, max length – 250 symbols. You can define the exact path or just a file name. In the latter case the system will search for the specified file in the product folder. You can select the file using the <input type="button" value="..."/> button. If you need to specify more than one file, type their names, separated by commas (for example, C:\temp\image.jpg, C:\temp\log.txt).
Pack	Optional: select archiver to compress the selected file(s). Each of the attached files will be compressed into separate archives. Possible values: no compress, 7Z, GZIP, ZIP.

10.1.4 Short Message Service

Represents a mobile phone or other similar device connected to the computer via a serial (COM) port or via a USB port.

Parent object – *Computer\Notifications* group.

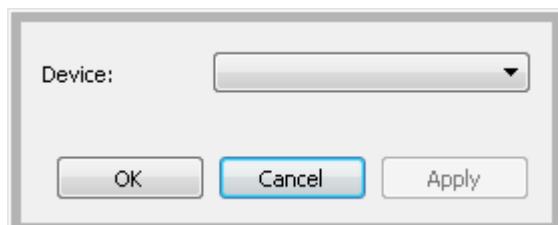


Figure 177. Short Message Service object settings window

Table 65. Short Message Service object settings

Parameter	Description
Device	Select device from the list. Any phone models that can be connected as an Android modem are compatible.

10.1.5 Short Message

This object represents an individual SMS message. Use *Macros* and *VB/JavaScript Programs* to send SMS messages.

Parent object – **Short Message Service**.

Notification Subsystem

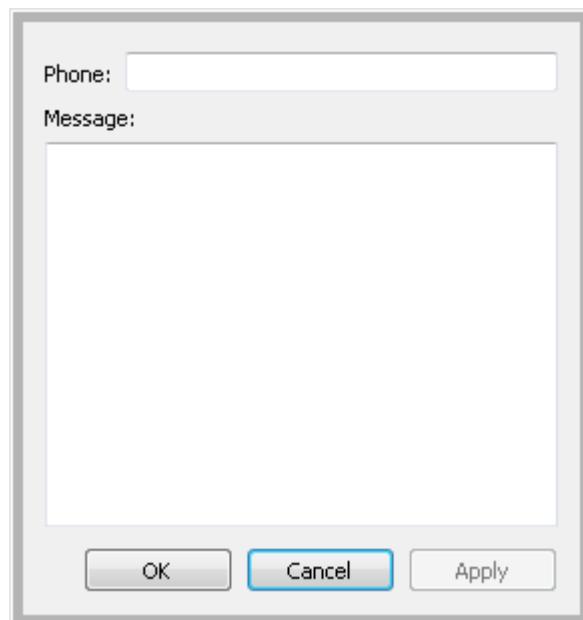


Figure 178. Short Message object settings window

Table 66. Short Message object settings

Parameter	Description
Phone	Specify a number of the target mobile phone to send message to. Use international phone format: ``+'' character, country code, city code, local phone number. Maximum phone length is 30 symbols (for example, +74951234567).
Message	Type in the message body. Both Latin and Cyrillic characters (ASCII) can be used. Max message length – 70 symbols.

10.1.6 Audible Notification Service

This object represents a sound card that should be used to playback event-specific audio recordings. The correspondence between individual audio files and object events can be viewed and altered via the DDI utility (see [ISS SecurOS Registration Files Editor](#)). All audio files should be placed in the \wav subdirectory of the SecurOS program folder.

Parent object – *Computer\Notifications* group.

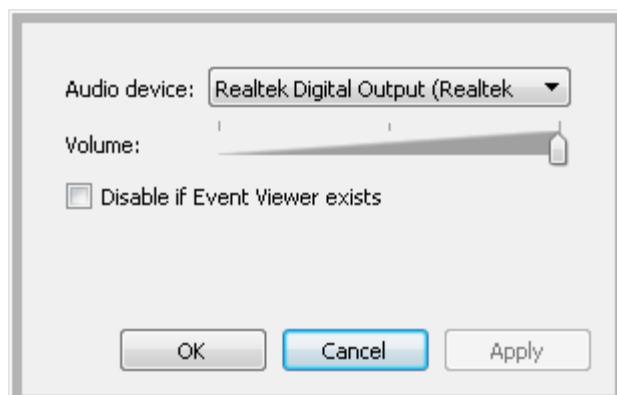


Figure 179. Audible Notification Service object settings window

Table 67. Audible Notification Service object settings

Parameter	Description
Sound card	Select an audio output line to play the audio files through.
Volume	Specify volume of the audible notifications by moving slider.
Disable if Event Viewer exists	Select this checkbox to disable audible notifications if a <i>Event Viewer</i> object exists. To use this option it is necessary to enable the <i>Event Viewer</i> object on the computer where the <i>Audible notification service</i> is configured.

10.1.7 Emergency service

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

This object is intended to send to emergency service an emergency ticket that contains information about incident. Details of the SecurOS settings and principles of interaction with the Emergency service are described in the [Interaction with External Emergency Service](#).

Parent object — [Computer](#).

Notification Subsystem

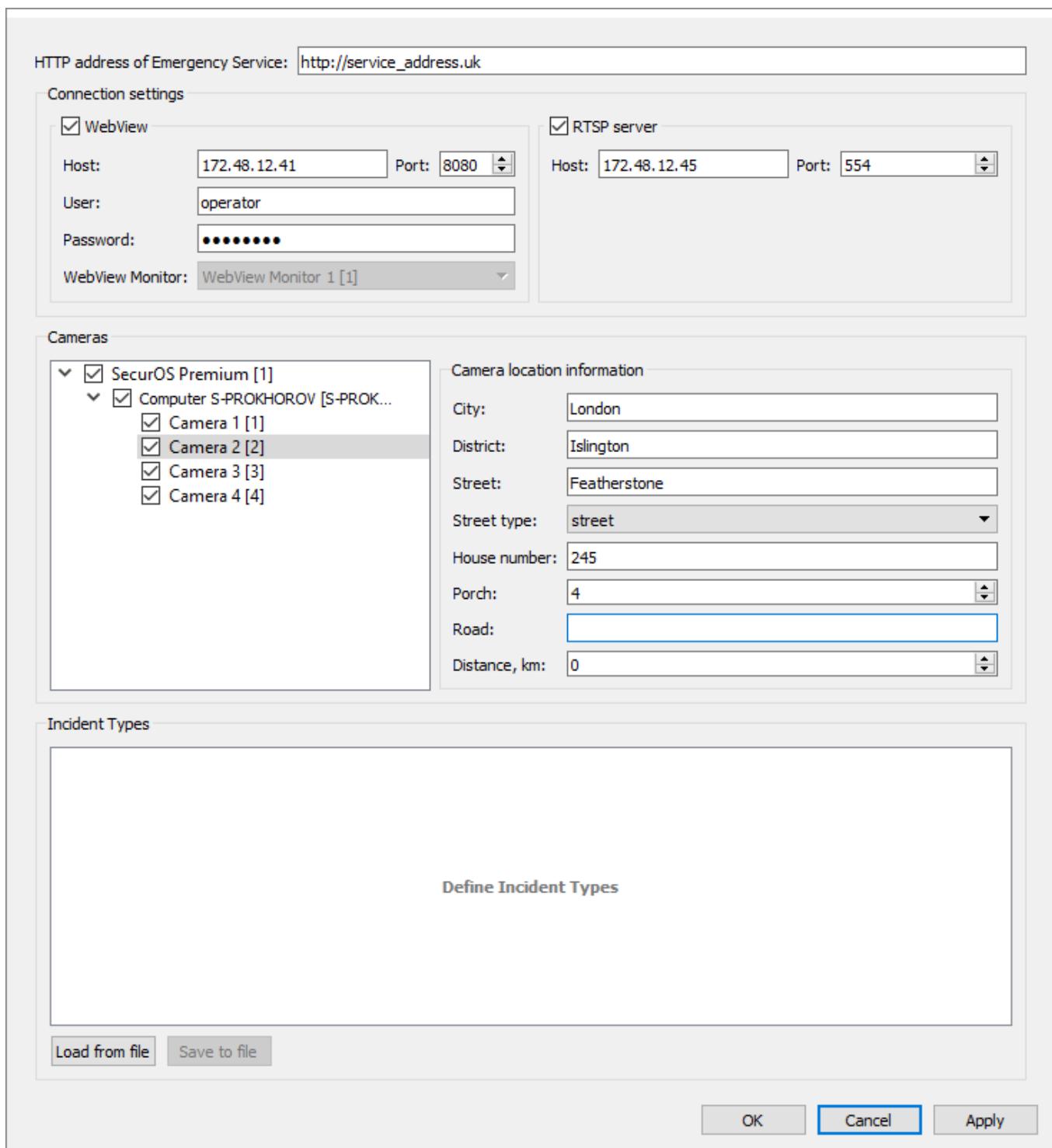


Figure 180. Emergency service object settings window

Table 68. Emergency service object settings

Parameter	Description
HTTP address of Emergency Service	Specify http address to which <i>Emergency ticket</i> and link to the related video will be sent.
Connection settings (parameters of this block are used to create links to the video related to the incident)	

Parameter	Description
WebView	Select this checkbox to create a link to the video that can be loaded with the help of the WebView module via <code>http</code> protocol.
Host/Port	Specify IP address and port number of the WebView module that will be used to provide interaction with external system.
User/Password	Specify login and password of the user registered within SecurOS that has access rights to work with the SecurOS's WebView module.
WebView Monitor	Select from the list the <i>WebView Monitor</i> object that will be used to display video from <i>Cameras</i> .
RTSP server	Select this checkbox to create a link to the video that can be loaded with the help of the RTSP server module via <code>rtsp</code> protocol.
Host/Port	Specify IP address and port number of the RTSP server module that will be used to provide interaction with external system.
Cameras	
Cameras tree	<p>Select <i>Cameras</i> for which an <i>Emergency ticket</i> can be created and sent to the Emergency service. To choose a <i>Camera</i> select checkbox on the left of the required one.</p> <p>Warning! If <i>Media Client</i> works only with selected cameras (the Use only selected Cameras checkbox is selected), then all cameras specified in this parameter must be selected in the <i>Media Client</i> settings. Otherwise <i>Camera</i> cell will not be displayed on the <i>Media Client</i> and one will not be able to create an <i>Emergency ticket</i>.</p>
Camera location information	
City, District, Street, Street type, House number, Porch, Road, Distance	Use required fields to specify <i>Camera</i> location address. This address will be transferred within the body of <i>Emergency ticket</i> .
Incident Types	
Incident Types List	<p>This field displays Incident Types List that is used when creating and sending <i>Emergency ticket</i>.</p> <p>Warning! If Incident Types List is not loaded, the <i>Emergency ticket</i> can not be sent to the external Emergency service.</p>
Load from file (button)	Click this button to download Incident Types List from file. Depending on operation result system will display corresponding message (for example, see Figure 181).
Save to file (button)	Click this button to save Incident Types List to file. Depending on operation result system will display corresponding message (for example, see Figure 182).

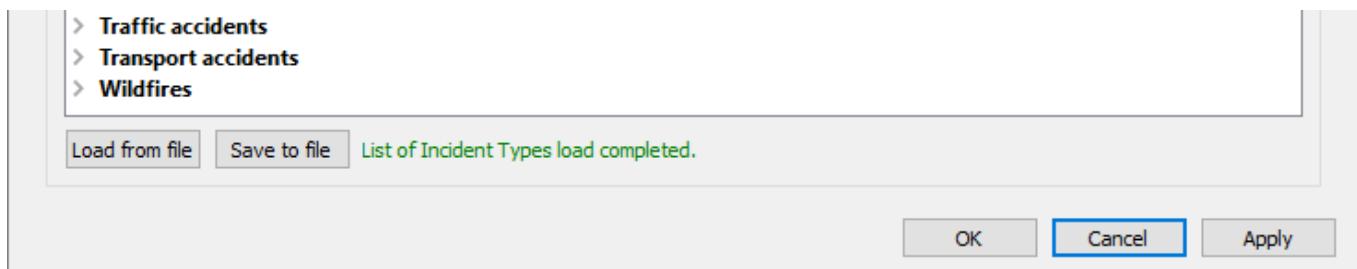


Figure 181. Successful file downloading message

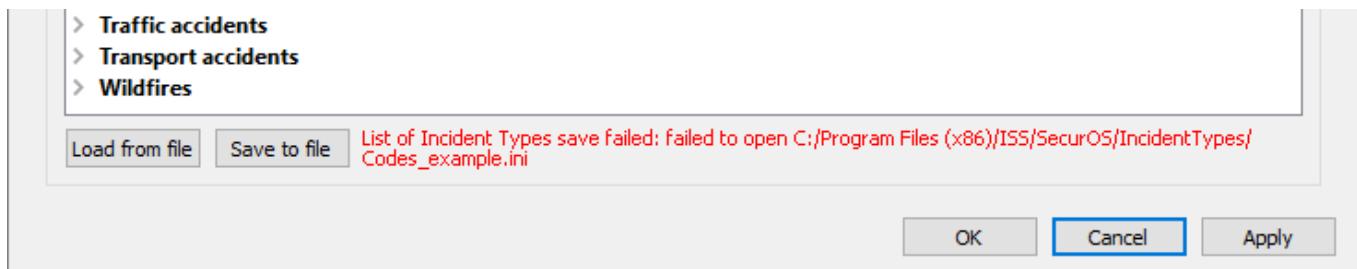


Figure 182. Cannot save to file message

10.1.7.1 Incident Types List. File Format

When creating Emergency ticket it is necessary in accordance to the requirements of the Emergency services to use code and description of the incident in standard format. Incident Types List file is used to load these data into SecurOS.

Note. When installing SecurOS these files are automatically created in \IncidentTypes folder of the product root folder.

Custom list of incident types can be created and loaded into the system in any local character encoding or UTF-16 LE with BOM encoding. File format is represented in Listing 2:

Listing 2. Incident Types List File Format

```
[section1]
Name=<Incident Type Category Name>
<Incident Code>=<Incident Type Name>
<Incident Code>=<Incident Type Name>
...
[section2]
Name=<Incident Type Category Name>
<Incident Code>=<Incident Type Name>
<Incident Code>=<Incident Type Name>
...
```

where:

- [sectionN] – unique section name. Section name can consist only of the latin characters and/or digits.
- Name=<Incident Type Category Name> – unique incident type category name. It is allowed to use characters in any character encoding in incident type category name. String length: [1; 255] characters.

Warning! Hyphenation of the string that contains incident type category name is prohibited.

- <**Incident Code**> – unique incident code. Section name can consist only of the latin characters and/ or digits in incident code. String length: [1; 16] characters.
- <**Incident Type Name**> – incident type name. It is allowed to use characters in any character encoding in incident type name. String length: [1; 255] characters.

Warning! Hyphenation of the string that contains incident type name is prohibited.

Example of the Incident Types List file 3.

Listing 3. Incident Types List File Example

```
[S1]
Name=Man-made fires
S101=fires in buildings, communications and technological equipment
S102=fires in transport
S103=fires in the metro
S104=fires in buildings housing, welfare, cultural
S100=other man-made fires

[S2]
Name=Wildfires
S200=other wildfires
S201=forest fires
S202=steppe and grain fields fires
S100=other man-made fires

[S3]
Name=Traffic accidents
S300=other traffic accident
S301=vehicle collision
S302=vehicle rollover
S303=hit on stationary vehicles
S304=hit a pedestrian
S305=hit a cyclist
S306=hitting an obstacle
S307=impact on animals

. . .

[S7]
Name=Geological / hydrological hazards
S700=other geological / hydrological hazards
S701=landslides, debris
S702=a hole in the earth's surface, roads
S703=high water levels / floods

[S8]
Name=Other incidents
S800=other incidents
S801=crowds
S802=loitering
S803=vandalism
S804=fight, attack
S805=entrance into the forbidden zone / perimeter intersection
S806=abandoned things
S807=vehicle detection from the black list or a wanted
```

Notification Subsystem

S808=human detection from the black list or a wanted
S809=need medical help

11 Automation Subsystem

The automation subsystem provides the means to configure custom reactions to specific events within the SecurOS network, thus building custom logic within the entire security network.

11.1 Object Reference

Automation subsystem includes the following objects:

- [Schedule](#).
- [Macro](#).
- [VB/JScript program](#).
- [IIDK Interface](#).
- [HTTP Event Gate](#).
- [REST API](#).

11.1.1 Schedule

Schedule object represents a time schedule and is used to define activity time for *Macros* and *VB/JScript programs* (scripts). For each *Schedule* specify time intervals, days of week, single dates and periods at which certain actions of macros and scripts will be executed. *Schedule* rules will be active for the specified days.

Example. If in the *Schedule* you select time interval from 8:00:00 AM to 10:00:00 PM and specify Monday and Wednesday, the event handling rules will be applied from 8:00:00 AM to 10:00:00 PM on Mondays and Wednesdays.

Parent object – *Security Zone\Schedules* group.

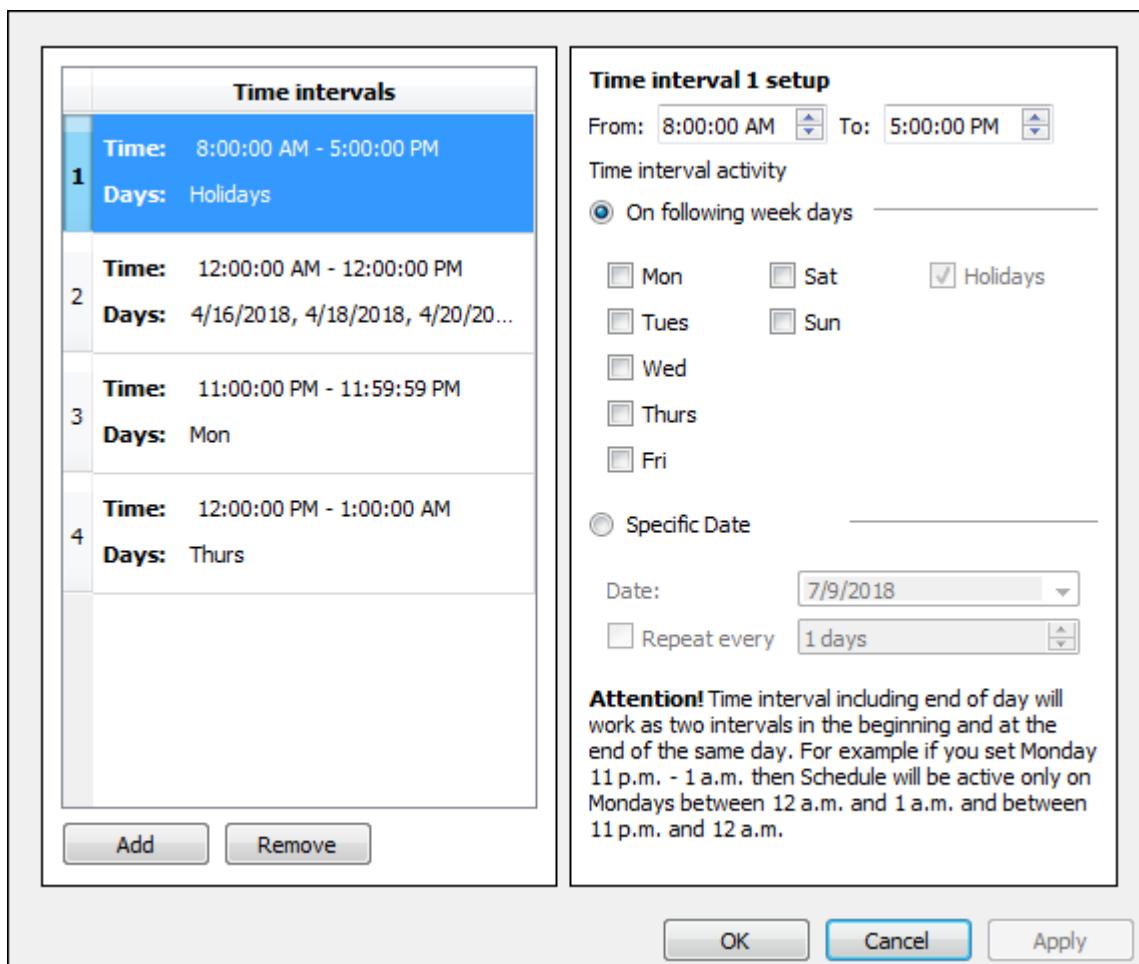


Figure 183. Schedule object settings window

Table 69. Schedule object settings

Parameter	Description
List of Time intervals (located on the left part of the window)	
Time intervals	Numbered list of specified time intervals and their activity periods. To edit parameters of the specified Time interval, click it and specify new parameter values.
Add (button)	Click this button to add new Time interval to the list.
Remove (button)	Click this button to remove selected Time interval from the list.
Time interval setup block (located on the right part of the window)	

Parameter	Description
From, To	<p>Specify interval start and end time in the From and To fields.</p> <p>When specifying time interval the From value can be greater than the To. In this case two intervals, that are valid for one day, are actually created within system:</p> <ul style="list-style-type: none"> • from 00:00:00 AM till To; • from From till 11:59:59 PM. <hr/> <p>Note. Valid days or periods for this interval are set by the general rules (see below).</p>
From, To	<p>For example, if interval is set as 3:00:00 PM – 11:00:00 AM and day of the week is set as Monday, then this interval is valid from 12:00:00 AM till 11:00:00 AM a.m. and from 3:00:00 PM till 11:59:59 PM p.m. each Monday.</p> <p>If you want to set a continuous time period, which begins on one day and ends on the next, then in this case it is necessary to set 2 Time intervals, the first of which ends and the second starts at midnight. For example, it is required to specify continuous Time interval that starts on Monday 6:00:00 PM and ends on Tuesday 02:00:00 AM. In this case one should specify the following time intervals:</p> <ul style="list-style-type: none"> • from 6:00:00 PM to 11:59:59 PM with a Mo period of activity; • from 00:00:00 AM to 2:00:00 AM with a Tu period of activity.
Time interval activity	
On following week days	<p>Select this option to specify Time interval activity as the days of week and/or holidays:</p> <ul style="list-style-type: none"> • Tick checkboxes for that Days of week on which specified Time intervals will be active; • If it is necessary to activate Time interval in holidays, tick the Holidays checkbox. <hr/> <p>Note. List of Holidays is specified in the Security Zone object settings.</p>
Specific date	<p>Select this option to specify Time interval activity at the calendar dates:</p> <ul style="list-style-type: none"> • In the Date field select the calendar date of the Time interval activity. • If it is necessary to provide Time interval re-triggering, select the Repeat every checkbox. Specify re-triggering period (in days) beginning from the specified date.

11.1.2 Macro

Used to define SecurOS system behavior by catching specific system events and generating custom reactions for those events.

Parent object – *Security Zone\Macros* group.

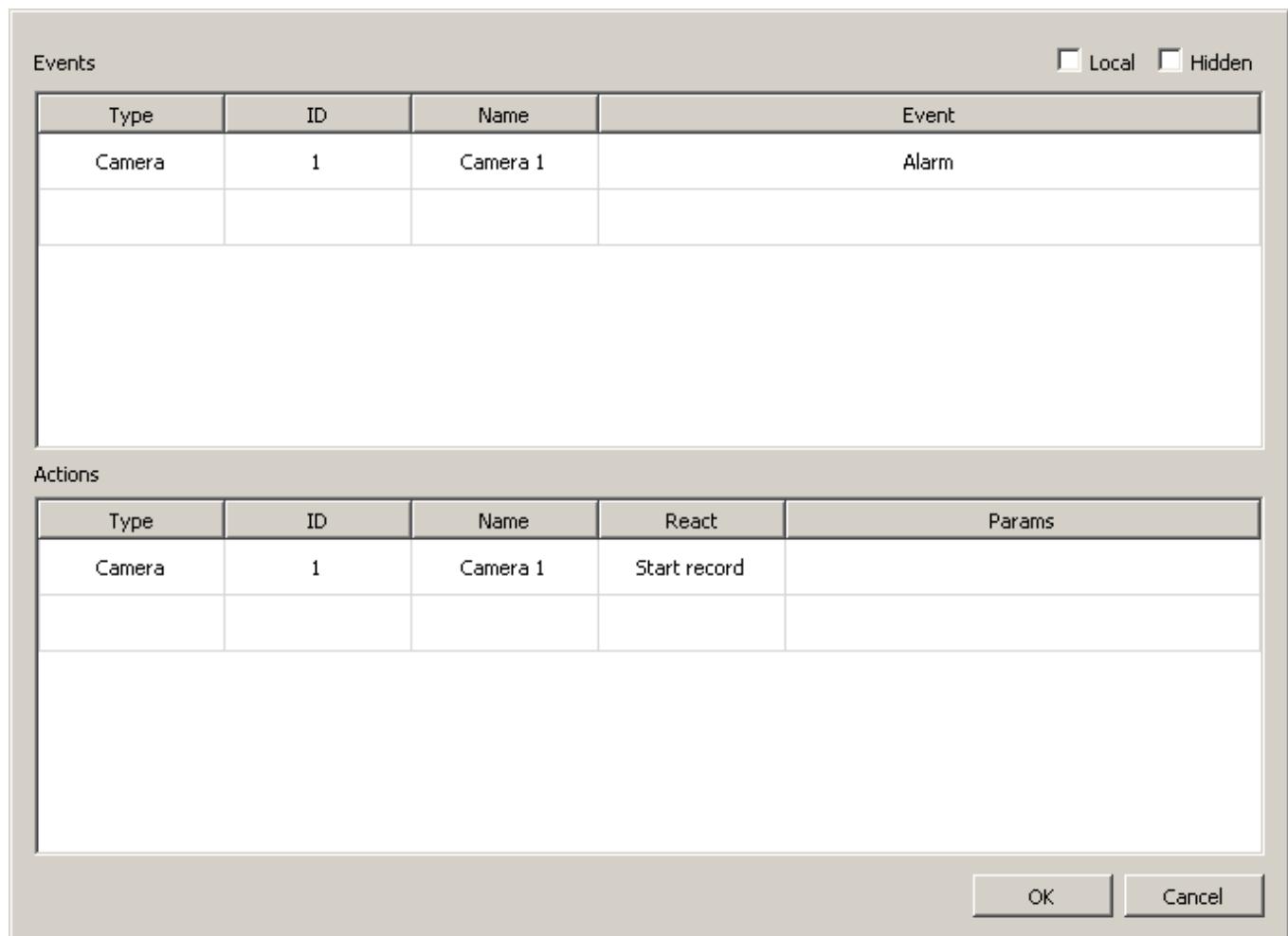


Figure 184. Macro object settings window

Table 70. Macro object settings

Parameter	Description
Local	Enable this option to prevent the event MACRO(X) RUN from being processed on any other computer located on the same network. If the macro is executed manually then it can not affect the other computers in the same security network. In the case when the macro is executed by some event it will be processed by all computers of the network which received the event. If the macro is executed at system startup then it is executed similarly to a manually executed macro. If this parameter is left unchecked then macro will be executed on all computers of the network.

Parameter	Description
Hidden	Tick this checkbox to hide the macro on the <i>Control panel</i> of all computers in the security network. By default, all macros can be executed manually on <i>Video Servers</i> or <i>Operator Workstations</i> which belong to the same security zone as the <i>Macro</i> object itself.
Event (table of source events that trigger macro execution, all events are equal in rights and any single event can trigger the macro).	
Type	Choose source object type.
ID	Choose source object ID. You can select the All value to refer to any objects of the specified type within the security network.
Name	<i>Information field</i> : name of the object (appears automatically after you select object type and specific ID).
Event	Choose source object event. List of values depends on the object type.
Actions (table of target objects and actions to perform on them on macro execution; actions are executed in the order they appear in the table).	
Type	Choose target object type.
ID	Select ID of an object. You can select the All value to refer to any objects of the specified type within the security network.
Name	<i>Information field</i> : name of the object (appears automatically after you select object type and specific ID).
Action	Choose action to perform on object. The list of actions depends on the type of the object. Warning! For the same object it is not possible to select two identical Actions even if these Actions have a different set of Parameters . If it is necessary to transmit several identical commands to the same object, create several <i>Macro</i> objects.
Params	Parameters of the selected action. Parameters are set as a string, maximum length – 255 symbols. String format: param1<value1>, param2<value2>. For example, file<\wav\sound1.wav>, color<green>.

11.1.3 VB/JScript program

This object contains the script settings interface as well as the programmer developing interface for scripting in SecurOS (see [SecurOS Programming Guide](#)).

Warning! To control objects located on the *Operator Workstation* with the help of *VB/JScript program* it is necessary to create it on the *Computer*, profile of which is used by this *Operator Workstation* as *Operator Workspace*. If *Local Environment* is used then the *VB/JScript program* must be created on the current *Computer*. For details see [Operator Workstation Profiles](#).

Parent object – *Computer\Integration and Automation group\VB/JScripts programs*.

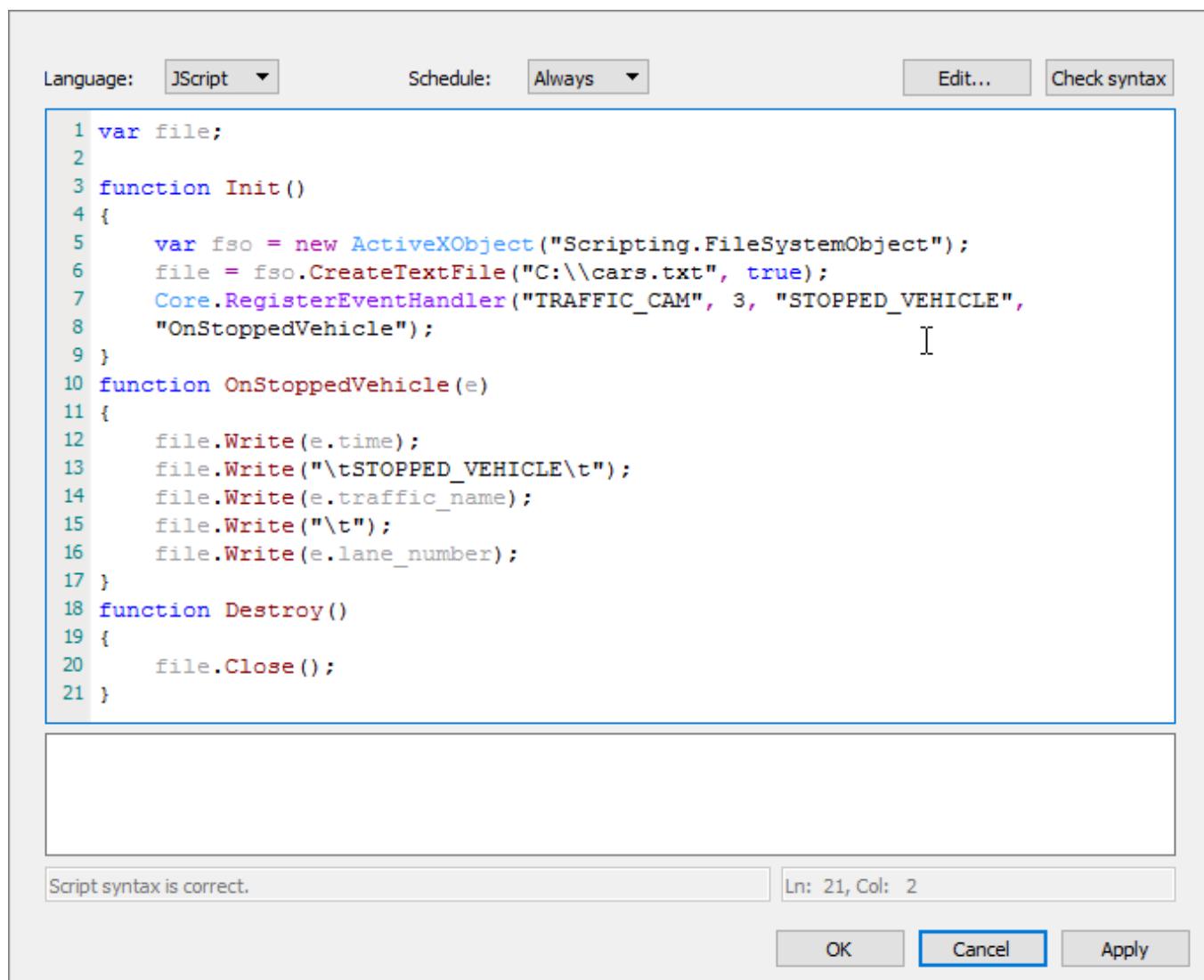


Figure 185. VB/JScript program object settings window

To create and configure a *VB/JScript program* object do the following:

1. Enter the Administration Mode.
2. In the SecurOS Object Tree select or create the *VB/JScript programs* object, for which create a *VB/JScript program* child object. Set the required values in the **Parameters of created object** window.
3. In the object settings window set the required object parameters (see below).

Table 71. VB/JScript program object settings

Parameter	Description
Language	Select the required programming language of the current script from the drop-down list. Possible values: <ul style="list-style-type: none">• VBScript;• JScript.

Parameter	Description
Schedule	Select schedule from the list (see Schedule section) for scenario execution (if selected schedule is disabled the program will not be executed). Schedule rules are specified in the appropriate <i>Schedule</i> object settings. Possible values: <ul style="list-style-type: none">• Always – script functions anytime;• Never – script never functions;• list of available <i>Schedule</i> objects – scenario is being executed in accordance with selected schedule.
Buttons	<p>Click this button to call an external VB/JScript editor.</p> <hr/> <p>Note. An External editor, is typically more functional than the built-in one, and is more convenient for use if the script contains a large number of rows.</p> <hr/>
Edit	Notepad.exe is called by default. To specify an editor press and hold the Shift key, then click the Edit button. In the standard Edit with window select required program. When you save the script, edited with an external editor, SecurOS displays an information message about changing the script from outside the system, and you are prompted to save changes to the script into the SecurOS database.
Check syntax	Click the button to check script syntax. In case of an error, the standard message according to the script language will appear in the state line and the source line of error will be highlighted in red in the script body.

4. Create script.
5. Check syntax of the created script.
6. Click the **OK** button to save the created script and close the editor window.

11.1.4 IIDK Interface

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

SecurOS provides the capability to exchange data with external / 3rd party systems. Data exchange is implemented by the means of a special IIDK (ISS Integration Development Kit) protocol. Using this data exchange protocol, an external computer/system can be connected to the SecurOS network to transmit events to the security network and to control the SecurOS.

IIDK Interface is a service for external connection to SecurOS via IIDK protocol. Create this object on one or more computers that will act as IIDK servers (see **IIDK Manual** for more information).

Note. **IIDK Manual** is not included into common documentation package and is provided by request.

When connecting to SecurOS via IIDK interface, user rights are ignored.

Parent object – *Computer\Integration and Automation* group.

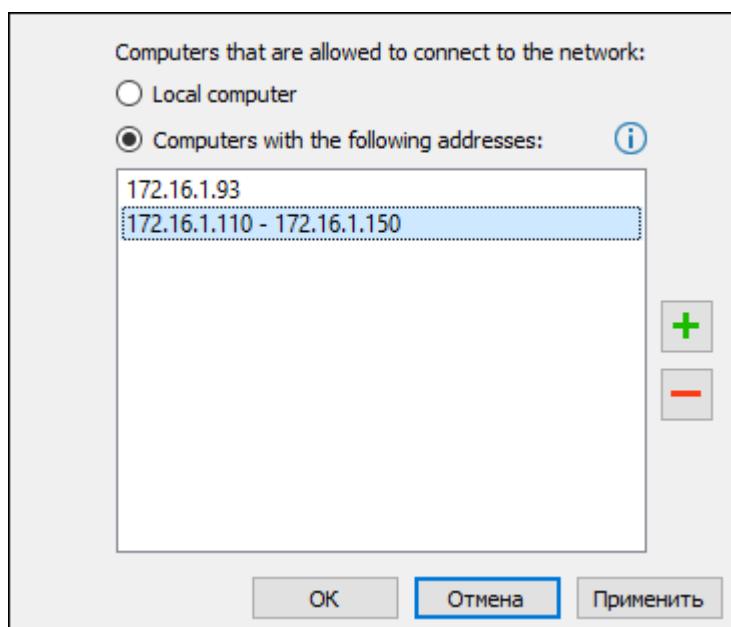


Figure 186. IIDK Interface object settings window

Table 72. IIDK Interface object settings

Parameter	Description
Computers that are allowed to connect to the network	Choose one of the options that determines which computers can connect to this IIDK server: <ul style="list-style-type: none">• Local computer. Only local connection is possible.• Computer with the following addresses. Computers with addresses specified in the list below can connect to this IIDK server.
List of the addresses	Specify IP addresses of the computers that can connect to this IIDK server. IP addresses must be specified in the IPv4 standard. It is possible to specify address ranges with a dash (for example, 172.16.1.110-172.16.1.150).

11.1.5 HTTP Event Gate

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

This object is used for transmitting data from an external system to SecurOS. Data is transmitted via HTTP GET/POST requests.

Parent object – *Computer\Integration and Automation* group.

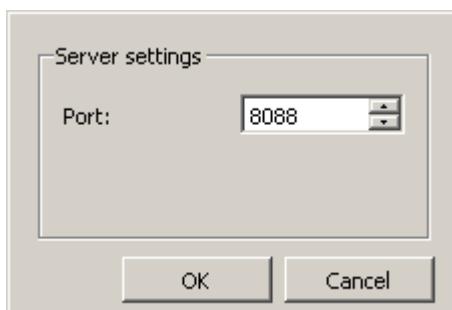


Figure 187. HTTP Event Gate object settings window

Table 73. HTTP Event Gate object settings

Parameter	Description
Port	Port number of the SecurOS HTTP server, which receives requests from the external system.

To transmit data to SecurOS, an external system should send a request to the specified port number of the HTTP server.

For more information about using *HTTP Event Gate*, please contact your regional Intelligent Security Systems representative.

11.1.6 REST API

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

This object implements a program interface for interaction of the SecurOS with an external systems via HTTP/HTTPS. Using this interface one can do the following:

1. Configure SecurOS partially.
2. Receive information about SecurOS' objects and their states.
3. Subscribe for notification about SecurOS' events.
4. Filter events transmitted from the SecurOS to the external system.
5. Receive fragments of video archive and separate frames.
6. Control PTZ.
7. Receive *Maps*, configured in SecurOS.

Parent object – *Computer\Integration and Automation* group.

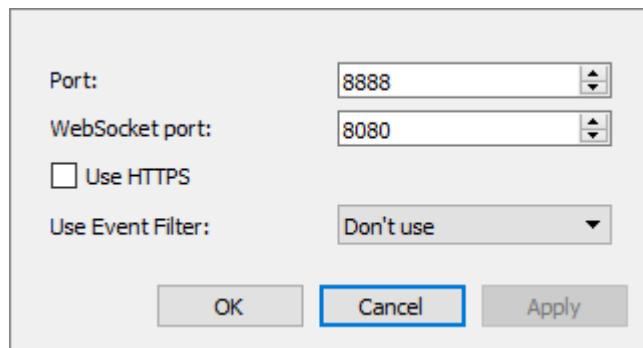


Figure 188. REST API object settings window

Table 74. REST API object settings

Parameter	Description
Port	SecurOS's port for interaction with external system via HTTP/HTTPS. Range of values: [1; 65535]. Default value is 8888.
WebSocket port	SecurOS's port for interaction with external system via WebSocket. Range of values: [1; 65535]. Default value is 8080.
Use HTTPS	Select this checkbox if it is necessary interact with SecurOS via HTTPS.
Use Event Filter	Select one of the <i>Event Filters</i> existing in the system to filter events transmitted from the SecurOS to the external system.

Refer to **REST API User Guide** for a detailed explanation of how to configure system and use the *REST API* object.

Note. **REST API User Guide** is not included into common documentation package and is provided by request.

11.2 Setting up Macros and Scripts

This section describes specifics of configuring and using the macros and programs.

11.2.1 Macros

Macros are used to define the links between the events and system actions. On occurrence of the event described in the macro command, the predetermined actions are executed automatically. The macro command can also be launched by an operator manually. Most of the system objects have a list of corresponding events and reactions.

Note. A detailed description of macros can be found in the [SecurOS Programming Guide](#).

To configure *Macros* perform the following steps:

1. In the SecurOS *Object Tree* within the *Macros* group child to *Security Zone* object create a *Macro* object.
2. In the **Parameters of created object** window set the required values.

3. In the object properties window (see figure 189) create the macro command description.

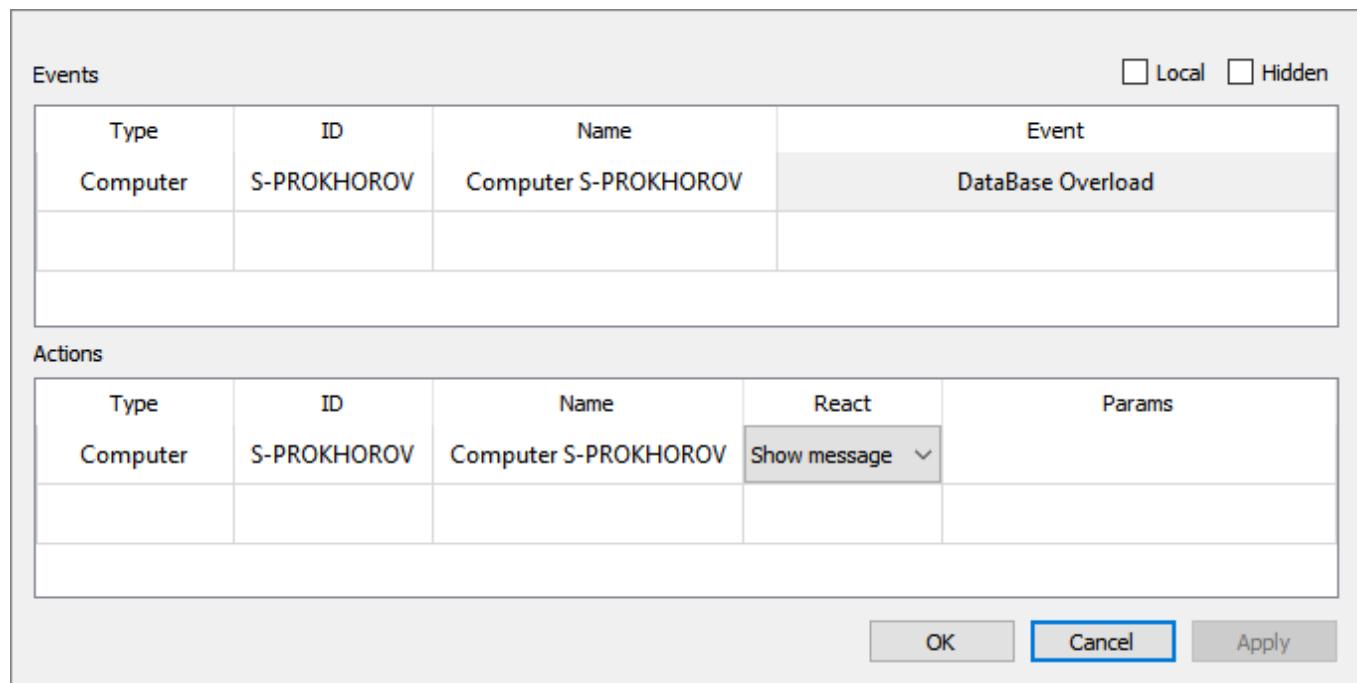


Figure 189. The object settings window

4. Apply new settings.

Buttons to execute the created *Macros* are displayed on the system *Control Panel* (see figure 190).



Figure 190. Control panel. Available Macros

11.2.2 VB/JScript programs

VB/JScript programs are a more advanced and versatile (in comparison with macros) way to handle event/reaction logic in the system.

Note. A detailed description of VB/JScript programs can be found in the [SecurOS Programming Guide](#).

To create a *VB/JScript program* do the following:

1. In SecurOS Object tree select a *Computer* object. In its child group *Integration & Automation* create child group *VB/JScript programs*.
2. In *VB/JScript programs* create *VB/JScript program* object.
3. In the **Parameters of created object** window set the required values.
4. In the *VB/JScript program* object properties window, type in the program code.
5. Check code syntax, correct found errors.
6. Apply new settings.

12 Computer Vision

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

The Computer Vision subsystem of SecurOS makes the security system operator aware of potentially dangerous situations that are, for example, a person or vehicle intersecting a perimeter of a restricted area; a suspicious behavior of a person near a parked car; a crowd of people near a secure area or office buildings, etc.

In SecurOS, this subsystem is represented by the *Computer Vision* object which consists of plugins and individual detectors.

Parent object – [Computer](#).

12.1 General Recommendations on Camera Configuration and Location

Below are the general requirements for the scene, cameras, and light source locations that must be followed to solve video analytics tasks based on the moving objects tracking algorithms. If these requirements are not met, this may result in false positive or false negative detector triggering.

1. Minimum allowed frame resolution is 320x240 pixels. Maximum resolution is not limited, because the initial frame is reduced to one of the following sizes: CIF or D1 (is specified in the tracker common settings).
2. Minimum FPS value: 15 frames per second. FPS of the video stream must be stable, otherwise correct working of the detectors is not guaranteed.
3. Linear sizes of the detected and tracked object should not be less than 5–10% of the frame size. For example, if frame size is 640x480 then human sizes should be ~24x32 pixels.
4. Maximum linear sizes of the detected objects should not be greater than 40% of frame size.
5. For best performance of the detector, the illumination in the scene should be sufficient and even. In other words, the constellation of the parameters of the camera sensitivity, light sources, reflective ability of the background surfaces and also camera position relative to the natural or artificial sources of light and shadow-forming obstacles must provide uniform illumination of the entire observed scene with minimum noise in the video image. If the video analytics detector is required to operate in the dark, it is necessary to provide an adequate level of artificial lighting, and avoid such angles and/or areas of video analysis, where significant glare from vehicle headlights, illuminated advertising boards, etc., are possible.
6. When mounting cameras it is necessary to avoid camera view angles, which cause overlapping of some moving objects (people, vehicles, etc.) by other moving or static ones (trees, architectural objects, etc.).
7. Also you should avoid placing cameras in front of light sources (avoid backlight). If these requirements are not met, the images provided by the camera are not applicable both for visual

analysis by the operator and for processing by the video analytics detectors.

8. It is necessary to avoid strong shadows. Otherwise the influence of the shadows must be minimized by installing additional source of light.
9. If possible, you should avoid the appearance of trees and other verdure, as well as water surfaces in a frame, or to ensure that such zones of the video frame can be masked out to ignore them by the video analytics system.
10. The camera must be firmly and rigidly fastened. One should avoid the presence of oscillations and vibrations or minimize their amplitude.
11. The video analytics algorithms are usually designed to work with fixed cameras. Working with PTZ cameras is possible only using one concrete preset for which a video analytics detector has been configured. False positives are possible if the camera moves from this preset to another position (for example, when rotating/scaling image by operator or when moving to another preset).
12. It is recommended to switch off the automatic white balance, auto iris and auto gain functions in the camera settings, especially for complex and unstable scenes. Otherwise, hard changes of the image which will cause false positives detector triggering may occur when fine tuning camera for the current scene is performed.

12.2 Tracking Kit III Plugin

The Tracking Kit III plugin represents a container integrated into SecurOS, consisting of the following video analytics detectors:

- **Running detector** – is designed to detect people moving at a speed exceeding a predefined value.
- **Left behind and Removed object detector** – is designed to detect left behind and removed objects.
- **Loitering detector** – is designed to detect people moving within a controlled area during a long time period.
- **Crowd detector** – is designed to detect potentially dangerous groups of people.
- **Intrusion detector** – is designed to detect objects that intersect the perimeter of a restricted area.
- **Object counter** – is designed to detect objects that intersect a control line in opposite directions.
- **Line crossing detector** – is designed to detect objects that intersect a control line.
- **Dwell time detector** – is designed to provide statistical data on the long/short-term stay of people in a particular place.
- **Wrong direction detector** – is designed to detect movement in the forbidden direction.

12.2.1 Configuring Plugin and Video Analytics Detectors

This section describes the settings and features of the configuration procedure of the Tracking Kit III plugin and video analytics detectors.

12.2.1.1 Configuring Tracking Kit III Plugin

Within SecurOS a separate instance of the Tracking Kit III plugin, that configured independently, corresponds to each *Camera*. When configuring plugin the parameters, influencing the work of each video analytics detector that is a part of the plugin, are specified.

To configure plugin do the following:

1. In the SecurOS *Object Tree* double click the *Computer Vision* object, plugins of which you want to

configure. System will display the object settings window (see figure 191).

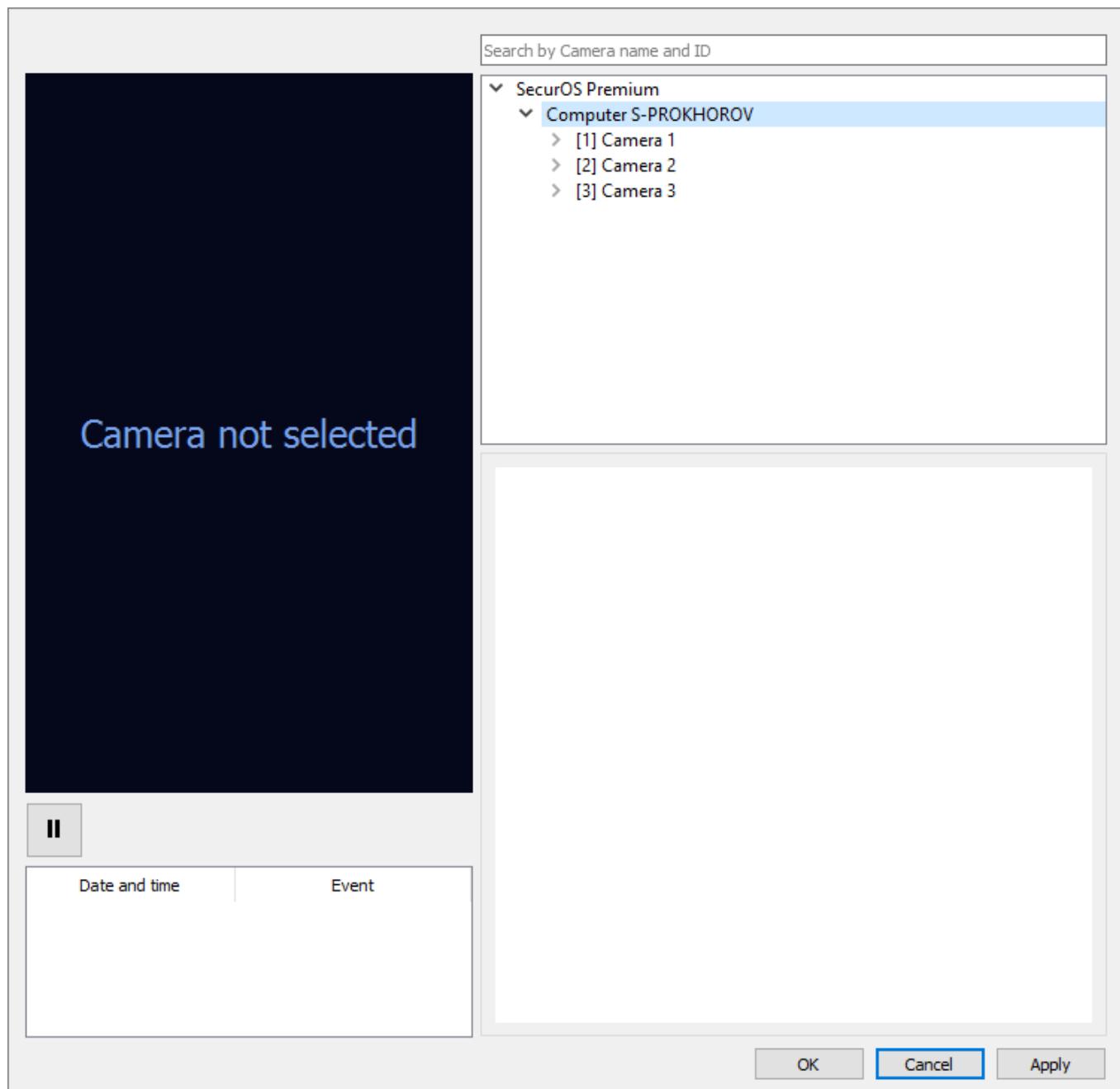


Figure 191. Tracking Kit III plugin settings window at the first start

2. In the *Camera tree* double click the *Camera* for which it is necessary to specify common settings of the image analysis. An image from the selected camera, its identifier and name will be displayed in the top left corner of the window (see Figure 192).

Note. If there are a lot of *Cameras* in the tree, specify a part of camera name or ID in the **Search by Camera name and ID** field to find a required *Camera*. Only *Cameras* whose names or identifiers comply with specified search conditions will be displayed in the tree.

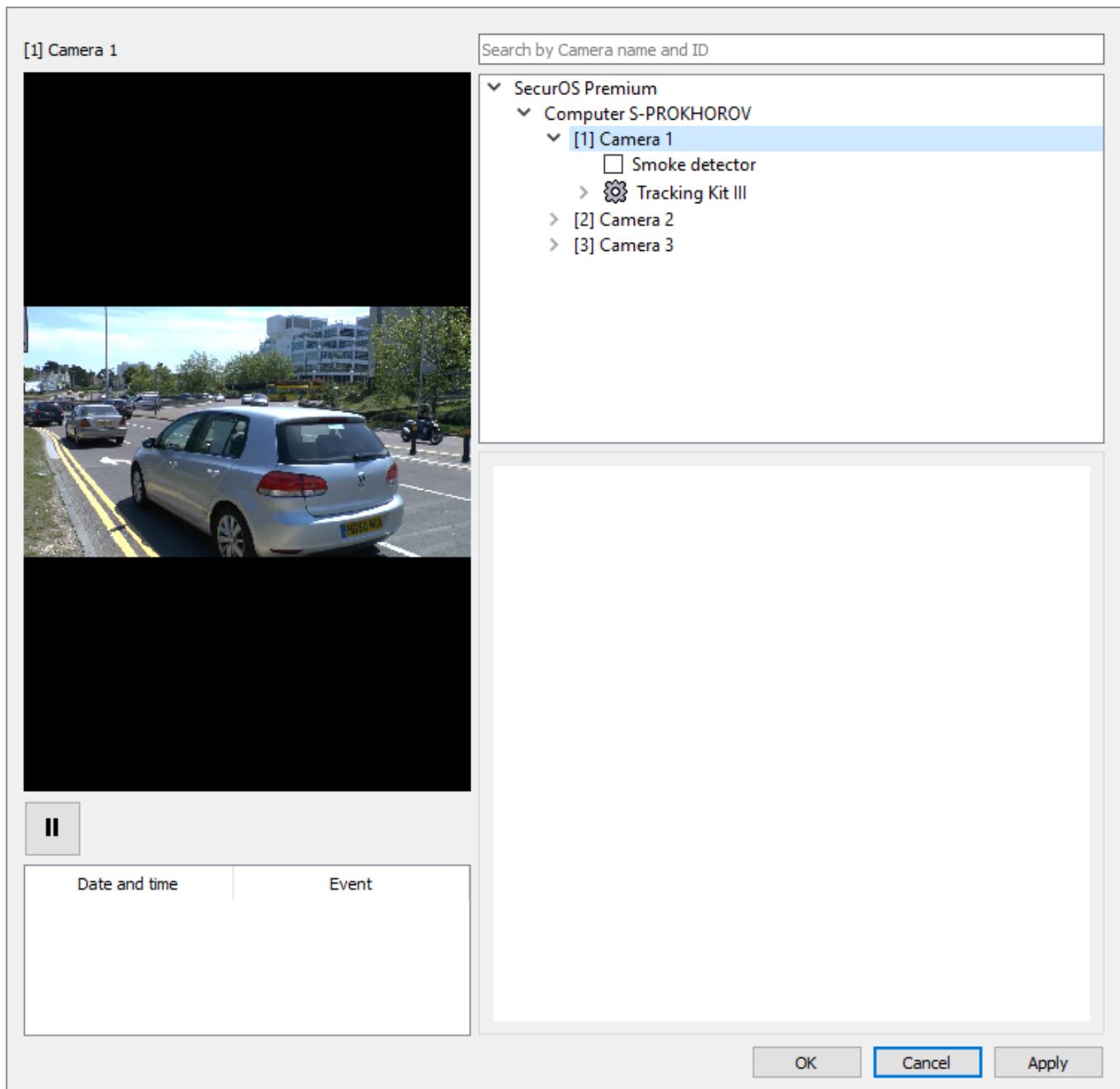


Figure 192. Selected Camera in the plugin settings window

3. Click the *Tracking Kit III* object child to the selected *Camera*. In the bottom right of the window, the plugin settings block will be displayed (see Figure 193).

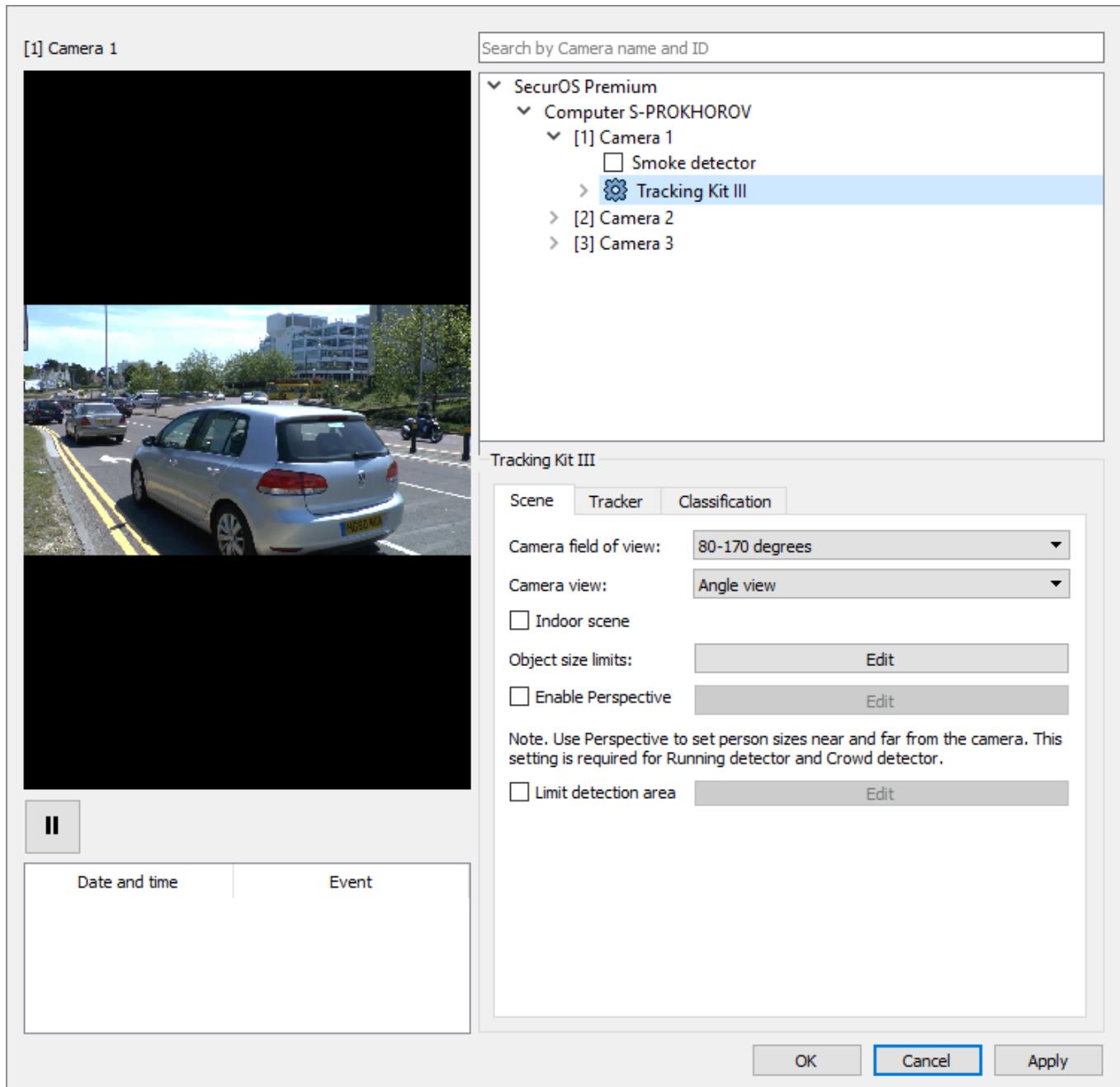


Figure 193. Plugin settings window. Tracking Kit III block

4. Specify required parameters in the **Scene**, **Tracker** and **Classification** tabs.
5. To apply new settings click the **Apply** button or the **OK** button.

Note. Event table, located on the bottom left of the window, is informational only. Data is displayed in the table only in case one or several detectors are selected to work with *Camera* (see [Configuring Video Analytics Detectors](#)).

12.2.1.1 Scene Tab

This tab is used to configure the parameters of the frame that will be analyzed.

Appearance of the tab is represented in figure 194.

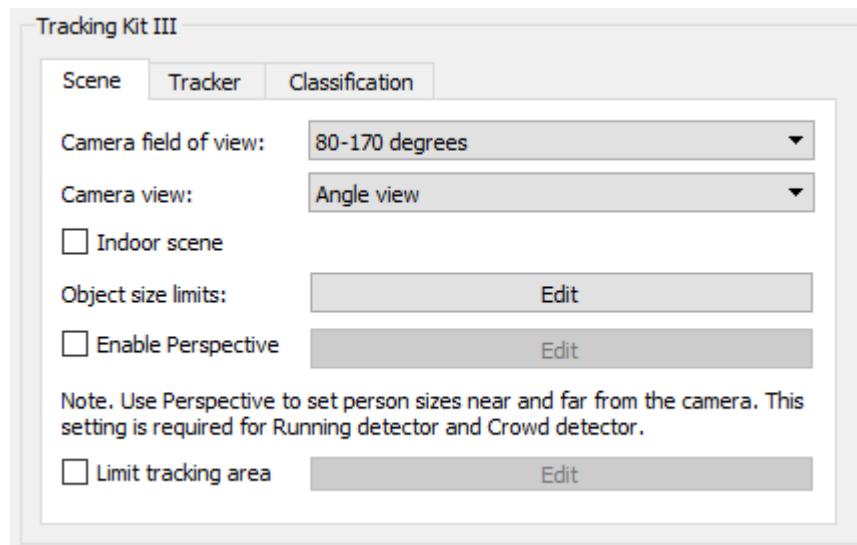


Figure 194. Tracking Kit III Plugin. Scene Tab

To adjust a scene, specify the following parameters:

- **Camera field of view, Camera view, Indoor scene** – these parameters affect the performance of the detection algorithm and accuracy of the detected objects classification.

Warning! When using PTZ camera, an algorithm performance will be correct only if that camera preset is used, for which the detector settings will be performed.

- **Object size limits** – this parameter is used to specify the range of sizes of objects moving within the scene to be detected and tracked. The more precise set values correspond to real objects size, the higher will be the tracking quality. To set objects sizes click the **Edit** button and specify required sizes with the help of mouse (see Figure 195).



Figure 195. Configuring objects sizes

- **Enable Perspective** – this parameter allows to simulate 3D scene on the base of 2D frame and sizes of objects near the *Camera* and in perspective. To enable perspective select checkbox, then click the **Edit** button and specify sizes of an object near and far from *Camera* with the help of mouse (see Figure 197).

Warning! It is necessary to enable Perspective when using the **Running Detector** and **Crowd Detector**. In other cases perspective setup can improve tracking quality.

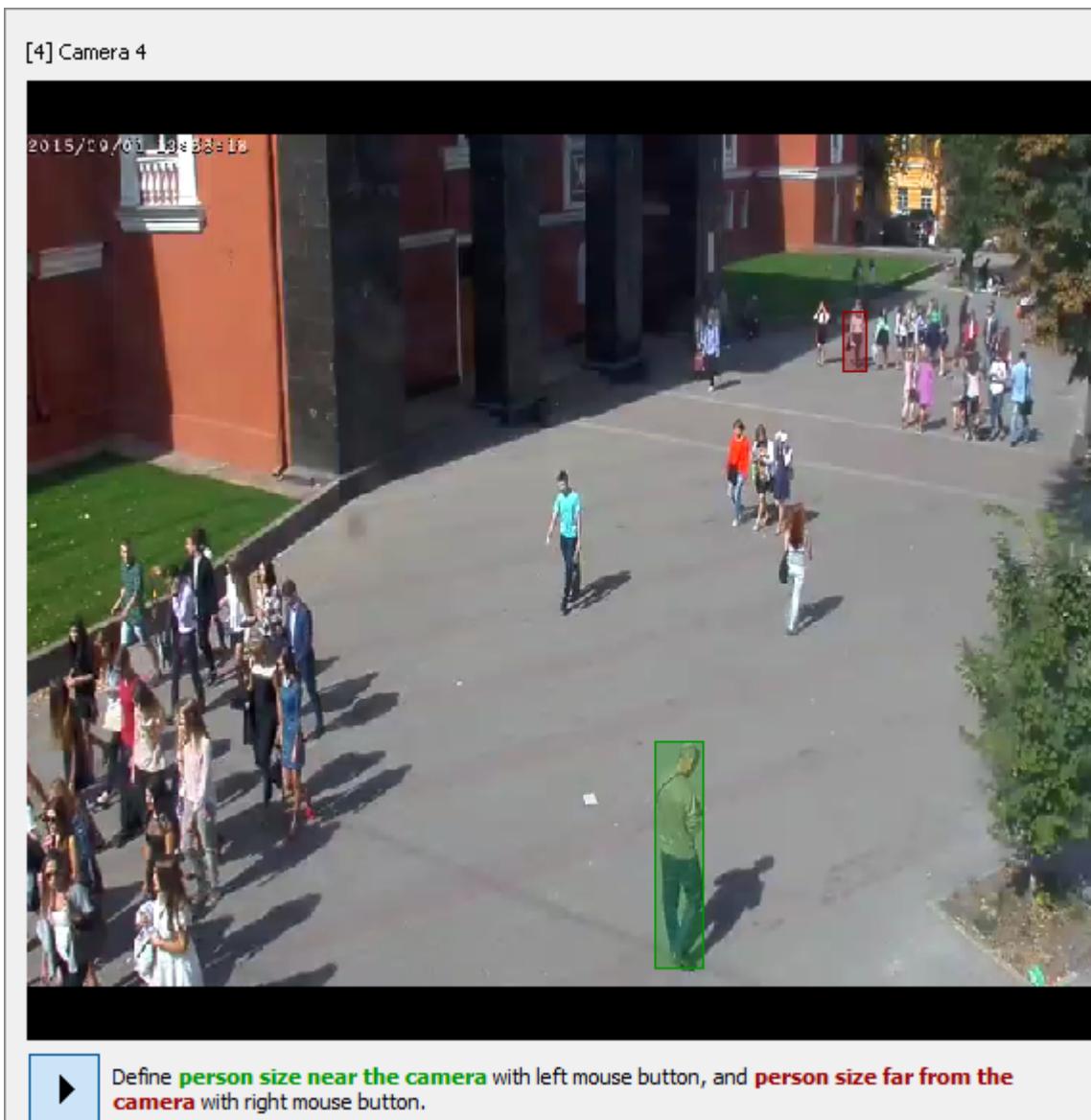


Figure 196. Configuring perspective

Limit tracking area — this parameter allows to limit tracking area for the objects in the scene. Limiting tracking area may significantly reduce CPU consumption, but one should be particularly attentive and responsible when decreasing area size. To limit tracking area select the checkbox and set the tracking area using mouse (see Figure 197). After accepting settings controlled area will be decreased. In settings window the ignore area (within this area object tracking is not performed) will be shaded (see Figure 198).

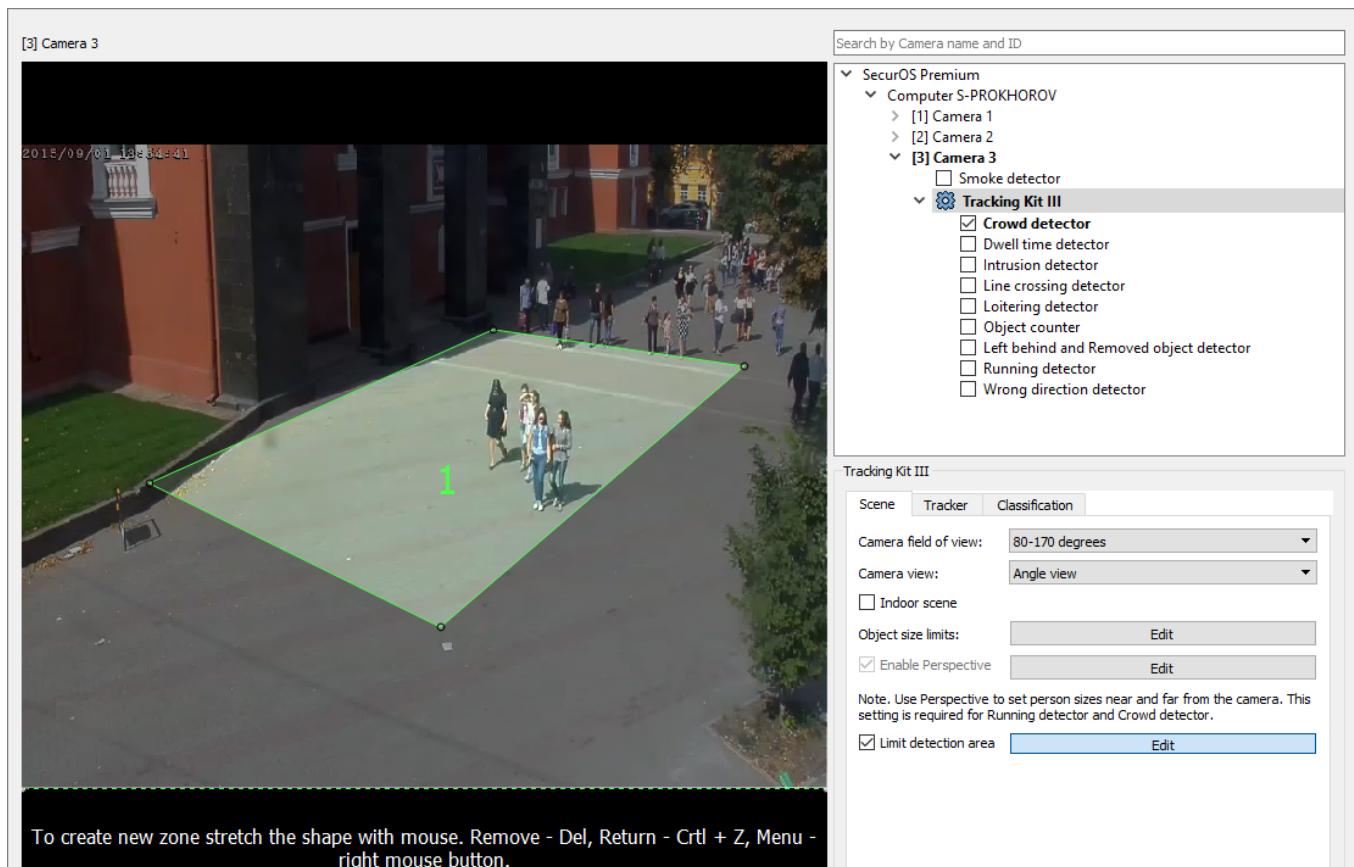


Figure 197. Limiting controlled area in plugin settings

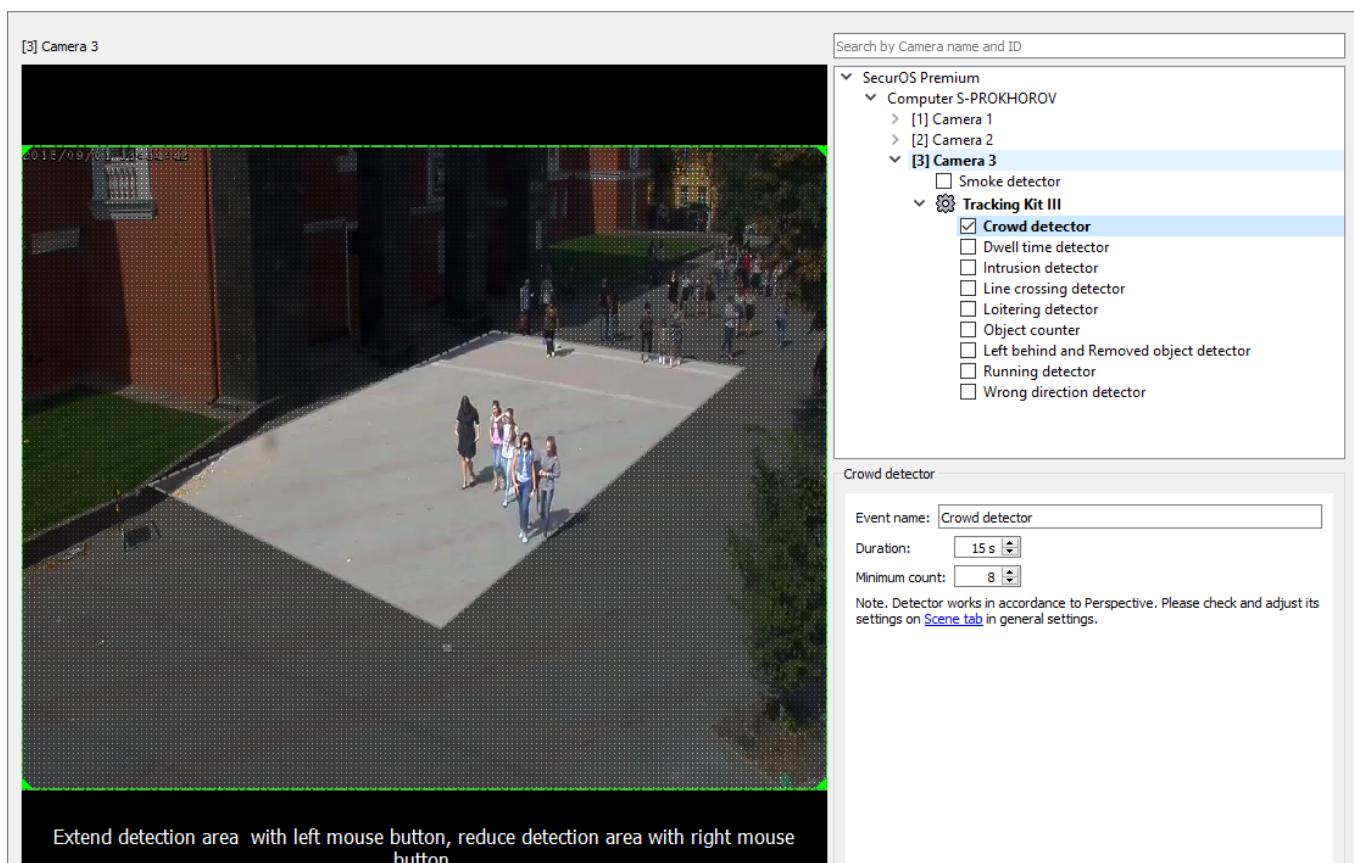


Figure 198. Display of limited controlled area in detector settings

12.2.1.1.2 Tracker Tab

This tab is used to configure the parameters of the tracker used for the analysis of the frame.

Appearance of the tab is represented in figure 199.

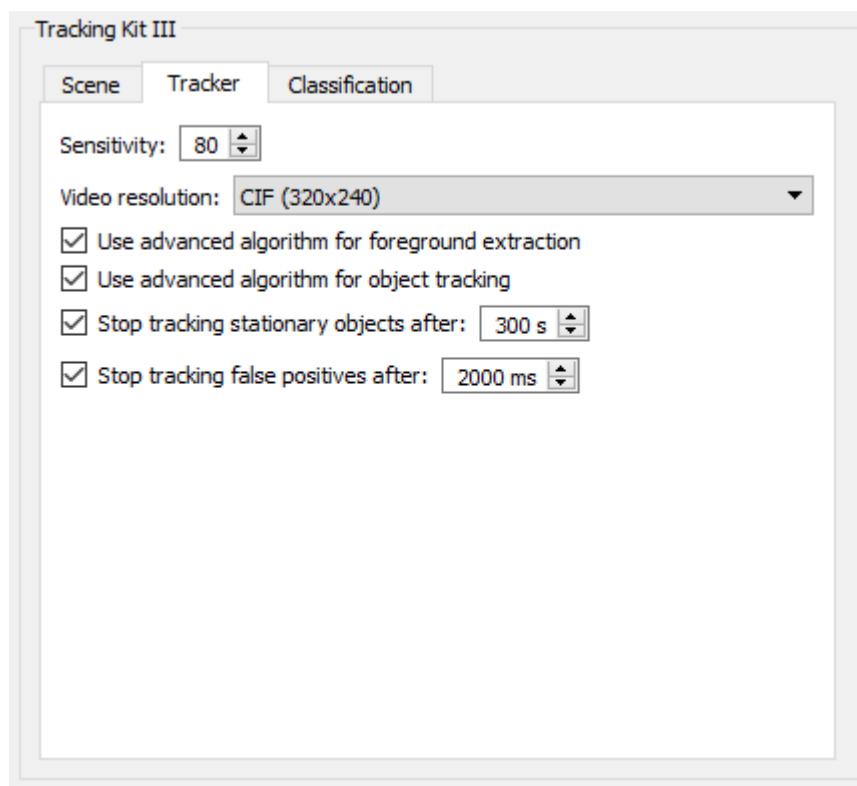


Figure 199. Tracking Kit III Plugin. Tracker Tab

To configure tracker specify the following parameters:

- **Sensitivity** – this parameter sets the sensitivity of the motion detection algorithm. If sensitivity is increased then minimum size of the detected object is decreased and number of detected objects is increased. If sensitivity is decreased then minimum size of the detected object is increased and number of detected objects is decreased.

Note. For most cases it is recommended to use default value.

- **Video resolution** – this parameter sets the resolution of the frame to be analyzed, to which the initial resolution of the video stream will be reduced to. In general, the greater the resolution, the more objects of smaller sizes can be detected. However, the increase in resolution can decrease overall system performance. Recommended value is 320x240 which is minimally sufficient for use of detection algorithms. If this resolution is selected to use then it is also recommended to enable advanced algorithms for foreground extraction and object tracking (the **Use advanced algorithm for foreground extraction** and **Use advanced algorithm for object tracking** parameters). The 320x240 resolution is also optimal if requirements described in the **General Recommendations on Camera Configuration and Location** are complied.

Additional Info

For example, the 640x480 resolution (with no advanced algorithms usage) can be used if it necessary to detect small objects. By performance this settings configuration can be compared with configuration that uses the 320x240 resolution and advanced algorithms for foreground extraction and object tracking.

- **Use advanced algorithm for foreground extraction** – select this checkbox to use advanced algorithm for foreground extraction. Use of advanced algorithm for foreground extraction allows to increase the accuracy of the detection of the moving object, but, at the same time, decreases general system performance. This parameter is recommended to use if specified **Resolution** is 320x240.
- **Use advanced algorithm for object tracking** – select this checkbox to use advanced algorithm for object tracking. Use of advanced algorithm of object tracking allows to increase the accuracy of the separation of the moving objects and reduce possibility of the tracking error when objects' trajectories are crossing or objects are overlapped by each other. This parameter is recommended to use if specified **Resolution** is 320x240.
- **Stop tracking stationary objects after** – select this checkbox to avoid processing of the objects motionless during specified time period. When specified time period is expired, all entities, earlier detected as an objects, will be considered as a background and will not be processed by detection and tracking algorithms.
- **Stop tracking false positives after** – select this checkbox to exclude an imaginary objects from processing. Imaginary object refers to an entity, that can not be classified both object and background. For example, stopped car, earlier detected as an object, leave parking in a few minute's time. As a result, there will be an "empty" area on the frame, that will be considered as an imaginary object.

12.2.1.1.3 Classification Tab

This tab is used to configure general parameters of the classification algorithm, that will be applied to all *classes* of the objects to be detected. Class of object is determined by a combination of its specific characteristics, that are defined within classification algorithm. SecurOS detector can work with the following classes of objects or their combinations:

- Vehicle;
- Animal;
- Human;
- Vehicle and human.

One can enable the classification mode and select the object class for each detector individually in its settings. If an object class is selected, then detector will only track objects of this class, which reduces the detector loading and improves the detection quality.

Warning! Minimum and maximum sizes of the object should be within the range of the detected object sizes, specified in the **Scene** tab.

Appearance of the tab is represented in figure 200.

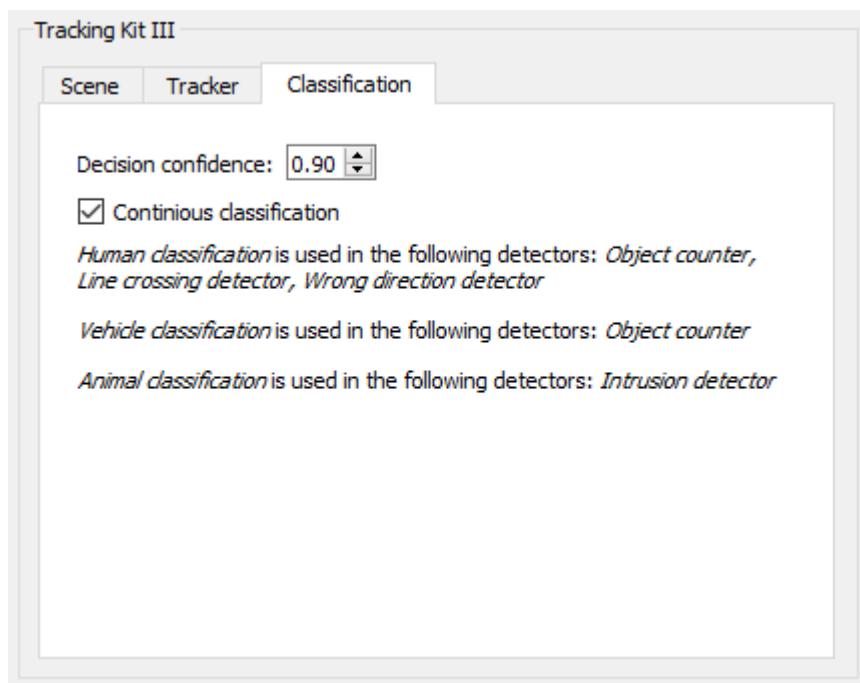


Figure 200. Tracking Kit III Plugin. Classification Tab

Specify the parameters of the object classification procedure:

- **Decision confidence** – threshold of class identification probability, from which the class is presumed to be reliably identified. Range of values: [0.01; 0.99]. The lower set value is, the higher will be class identification speed and, simultaneously, the chance of classification mistake, and vice versa.
- **Continuous classification** – select the checkbox if it is necessary to periodically identify class of the object again (Human, Vehicle, Animal) during all time of its presence in the field of view. Algorithm allow to rise tracking quality through lowering number of class identification mistakes, but it increases CPU load.

Information about using classification algorithms by different detectors is represented in the tab below, see Figure 200.

12.2.1.2 Configuring Video Analytics Detectors

This section describes the settings and features of the configuration procedure of the video analytics detectors.

To configure a detector in the *Cameras tree* select a *Camera* and select checkbox on the left of the required detector. Image from the given *Camera* and selected detector settings will be displayed in the object settings window (see Figure 201).

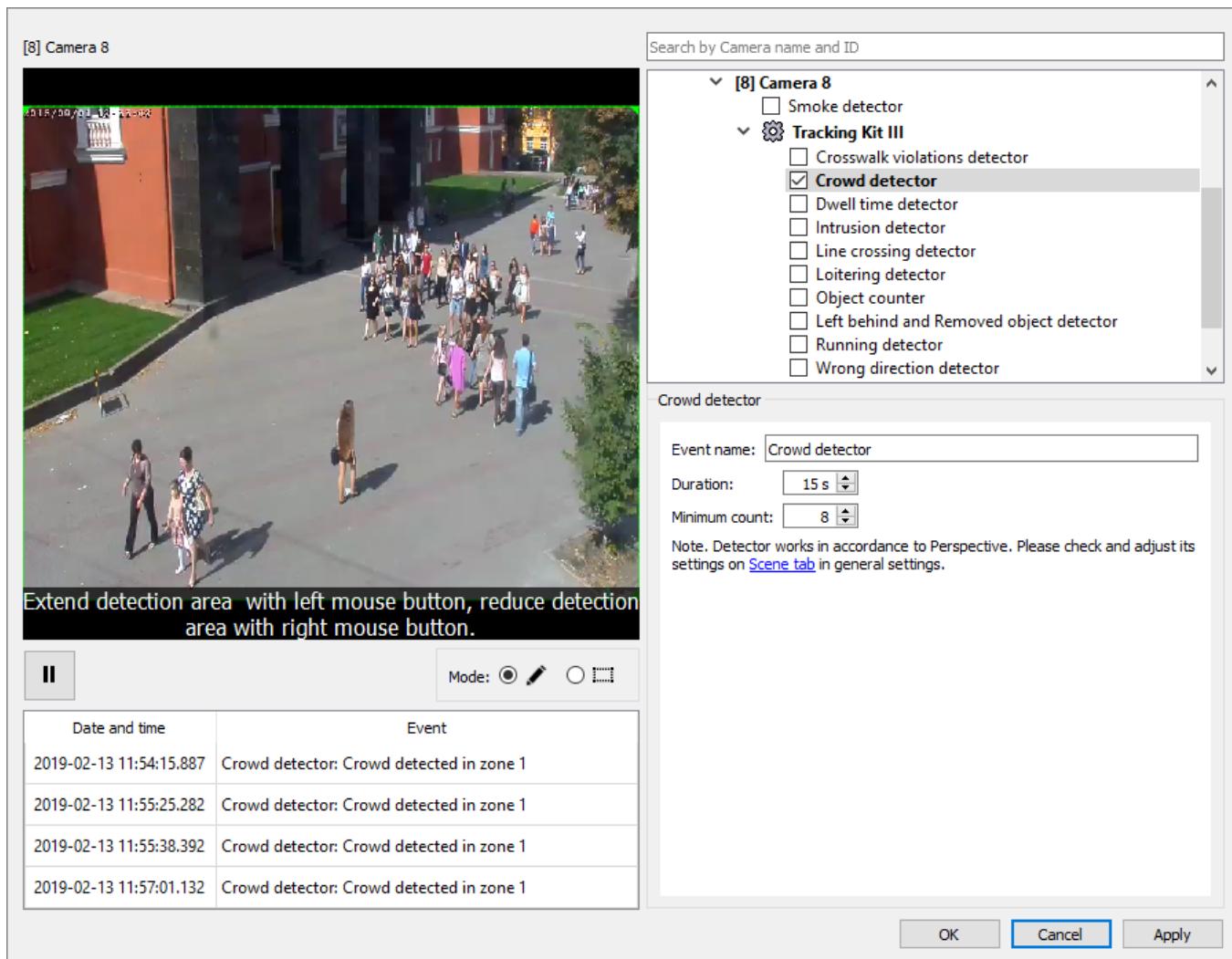


Figure 201. Detector settings window

Note. *Cameras* for which at least one detector is selected are highlighted in the *Cameras tree* in **bold**.

Correctness of the specified settings can be checked immediately after they are applied. To do this use the *Event table* located in the lower left corner of the settings window (see Figure 201). To check the correctness of the detector settings do the following:

1. Specify and apply all required detector's parameters, controlled zones and detection lines.

Note. It is more convenient to use static frame to draw controlled zones and detection lines. To pause video,

click the button then specify required zones and detection lines. Click the button to play video.

2. Viewing video from the *Camera*, the operator visually detects a situation which in accordance with the settings needs to be processed by the detector (e.g., the object crossed the border of the forbidden zone).
3. If a new entry is added into the *Event table* each time when such an event occurs, then detectors settings are considered correct. Otherwise detector settings are considered incorrect and must be changed.

Warning! Detector operation is affected both by the detector's own settings and the plugin common settings (see [Configuring Tracking Kit III Plugin](#)). If detector's own settings do not allow to achieve the correct results, then common plugin settings must be changed.

12.2.1.2.1 Configuring Controlled Zone

When video analytics detector operates, observation objects and detector activation conditions are being controlled within some zone, that set in the frame. Such a zone represents "transparent" frame area for detector.

To provide detector operation in system the following controlled zones are used:

- *Object tracking zone* (further *Tracking zone*) — within this zone only tracking of an object is being performed. Given zone is shared between all video analytics detectors and can be set in **Tracking Kit III** plugin settings on **Scene** tab.
- *Event detection zone* (further *Detection zone*) — within this zone analysis of detector activation conditions are being performed. Given zone is set independently for each detector in its own settings.

Controlled zone may be formed using rectangles or polygons. In a frame one can define one united zone composed from number of rectangles and/or their combinations, and not more than 9 independent zones, formed with polygons.

Way of zone definition are described in following sections:

- [Defining rectangular zone](#).
- [Defining polygonal zone](#).

Notes:

1. In plugin settings not more than 9 polygonal zones can be defined.
 2. In detector settings not more than 9 polygonal zones or 1 rectangular zone can be defined.
 3. When switching mode in detector settings, prior created zones are being deleted.
-

Defining rectangular zone

By default when configuring the system for the first time the area of controlled zone match the area of whole frame (see figure 202).

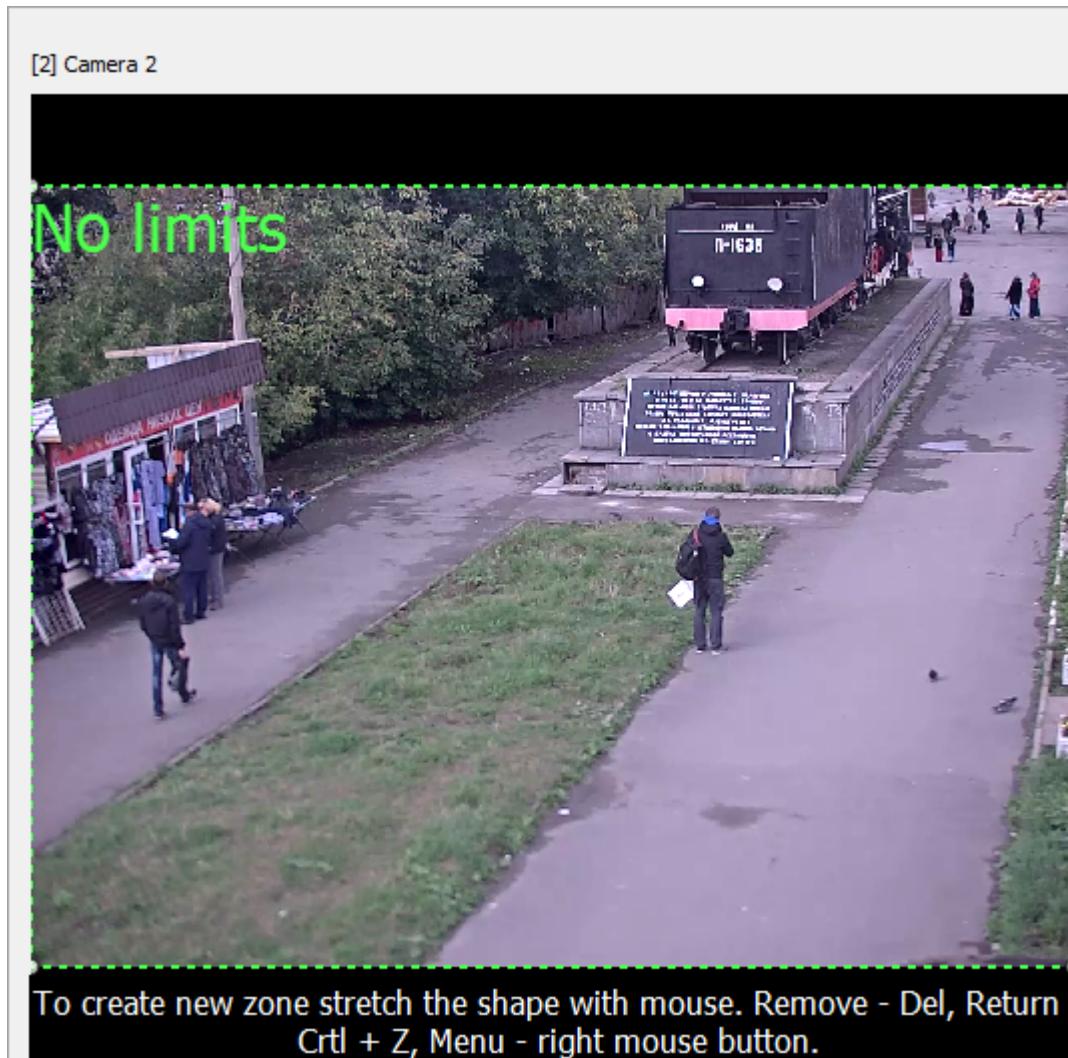


Figure 202. Default size of the zone

To decrease zone size press and hold left mouse button and draw one or several rectangles (or their combinations) within the frame (see figure 203).



Figure 203. Rectangular zone, formed from several figures

Rectangles may overlap each other or stay separated. Number of simple and complex figures is not limited.

Warning! All rectangles defined in the frame work as a single controlled zone, regardless of their number and combination.

Defining polygonal zone

Similar to rectangular zone, the polygonal zone matches full frame are by default (see figure 202). To decrease size of the zone select polygonal mode in frame context menu (see figure 204).



Figure 204. Selecting polygonal mode

Notes:

1. In detector settings switching drawing mode (Rectangle/Polygon) can be performed with options  (Rectangle) and  (Polygon).
2. By default when configuring first time the **Stretching** mode is set for polygons drawing.

In **Stretching** polygon creating mode place the mouse pointer over any side or node of original rectangle (see figure 205).

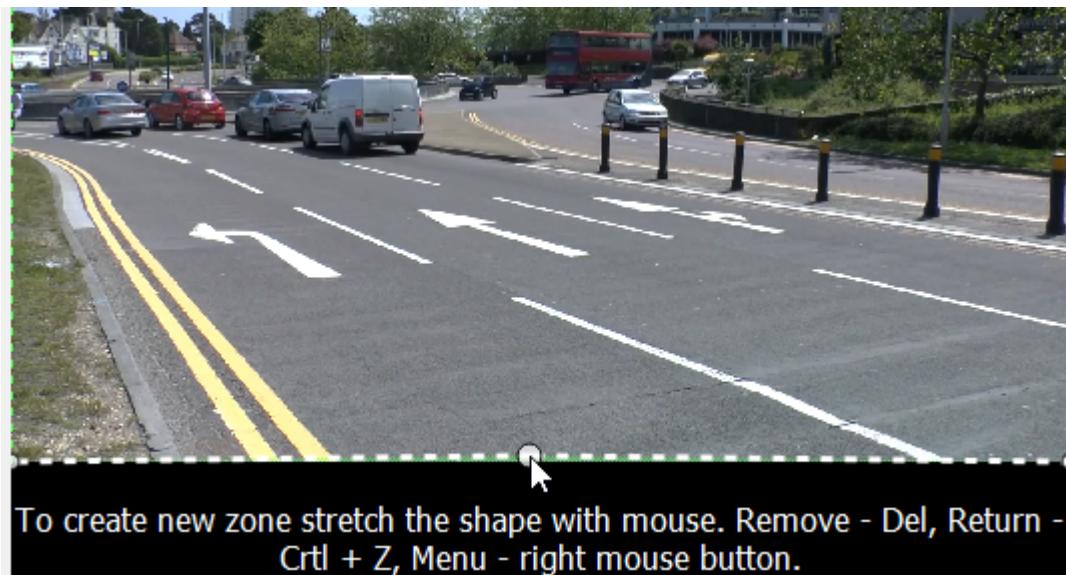


Figure 205. Point of zone stretching

Move the point to required direction. Form the required shape of the figure, consistently picking points at figure nodes or sides (ie, see figure 206).

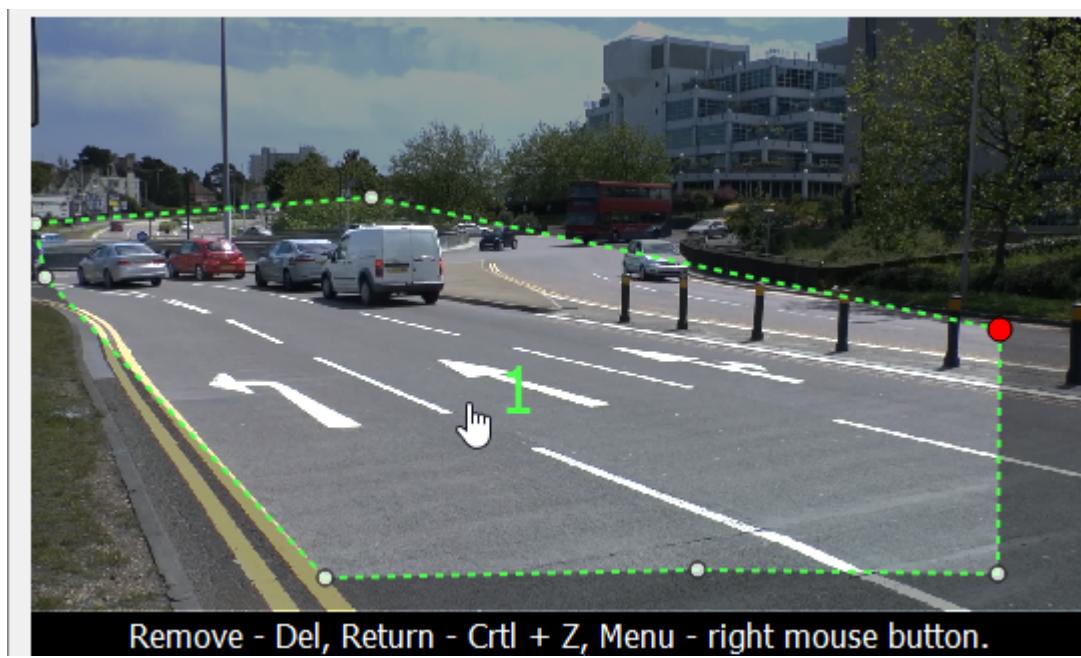


Figure 206. Polygonal zone (stretching)

In **By clicking point** polygon creating mode mouse pointer takes shape like it is shown on figure 207.

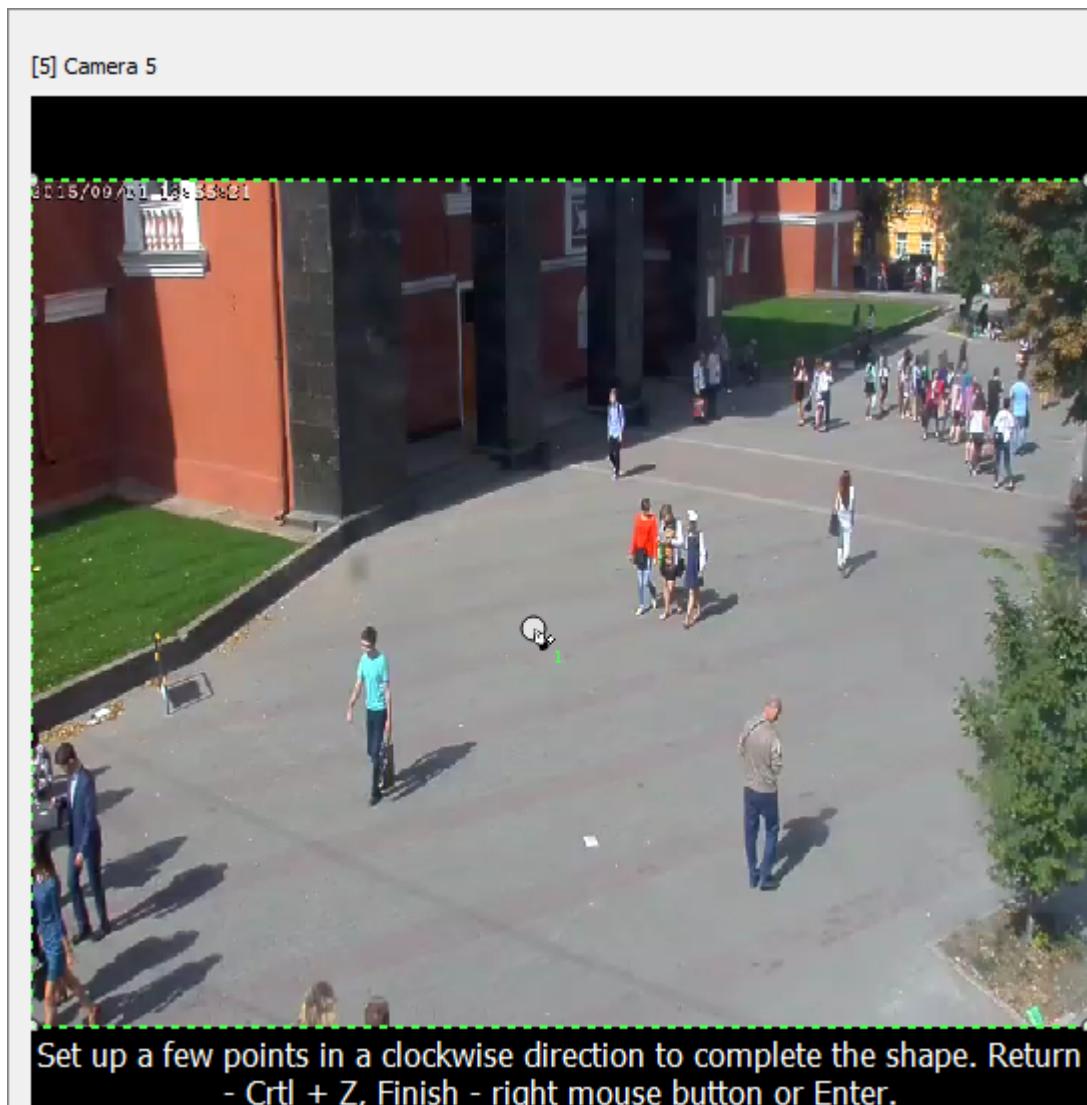
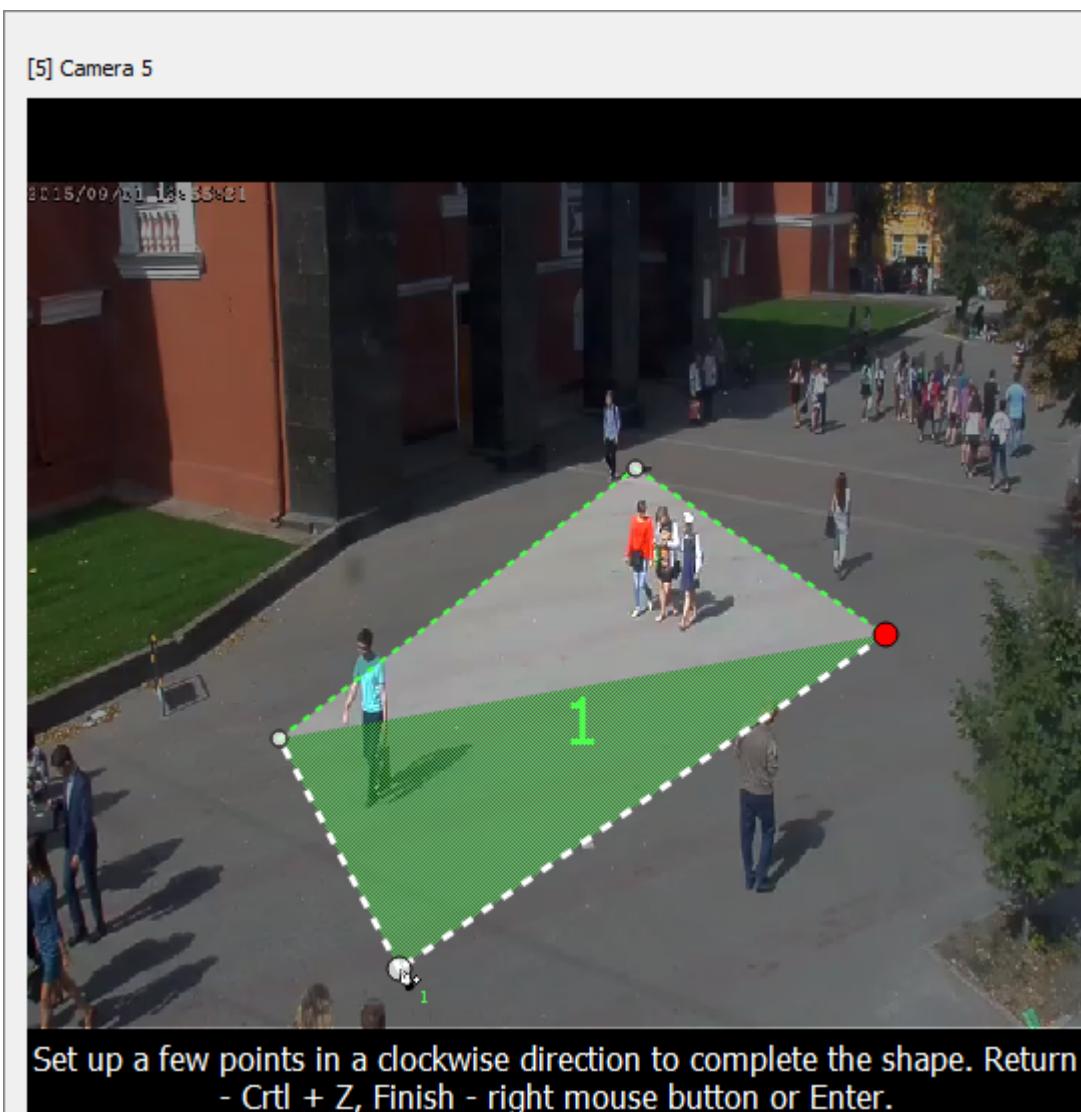


Figure 207. Dot by dot polygon creating mode

Move mouse pointer to required direction and press left mouse button. The fist polygon node will be marked on the frame. To create zone of required shape, consistently repeat mentioned operation several times (see figure 208).



Set up a few points in a clockwise direction to complete the shape. Return - Ctrl + Z, Finish - right mouse button or Enter.

Figure 208. Polygonal zone (by clicking point creation)

To finish working with zone double click left mouse button at last created node.

Warning! In a frame up to 9 polygons can be created, and every of them will be counted as individual zone. Zones will be numbered automatically for more convenience.

12.2.1.2.2 Running Detector

If a person moves in a controlled area with a speed, that exceeds a specified threshold, they are considered running. The current speed is calculated using the average size of a person in a given point of a frame, taking into account perspective. The controlled area and speed threshold are the configurable parameters of the detector.

It is necessary to specify the boundary sizes of objects. To reach the best detector operation quality it is recommended to use "angle view" camera setting. To minimize false positives, the visual separability of the moving objects within the frame is required (persons should not overlap each other or move in heavy traffic).

This detector works only with Human class of objects, that is specified automatically and cannot be disabled.

Running detector settings window is represented in Figure 209.

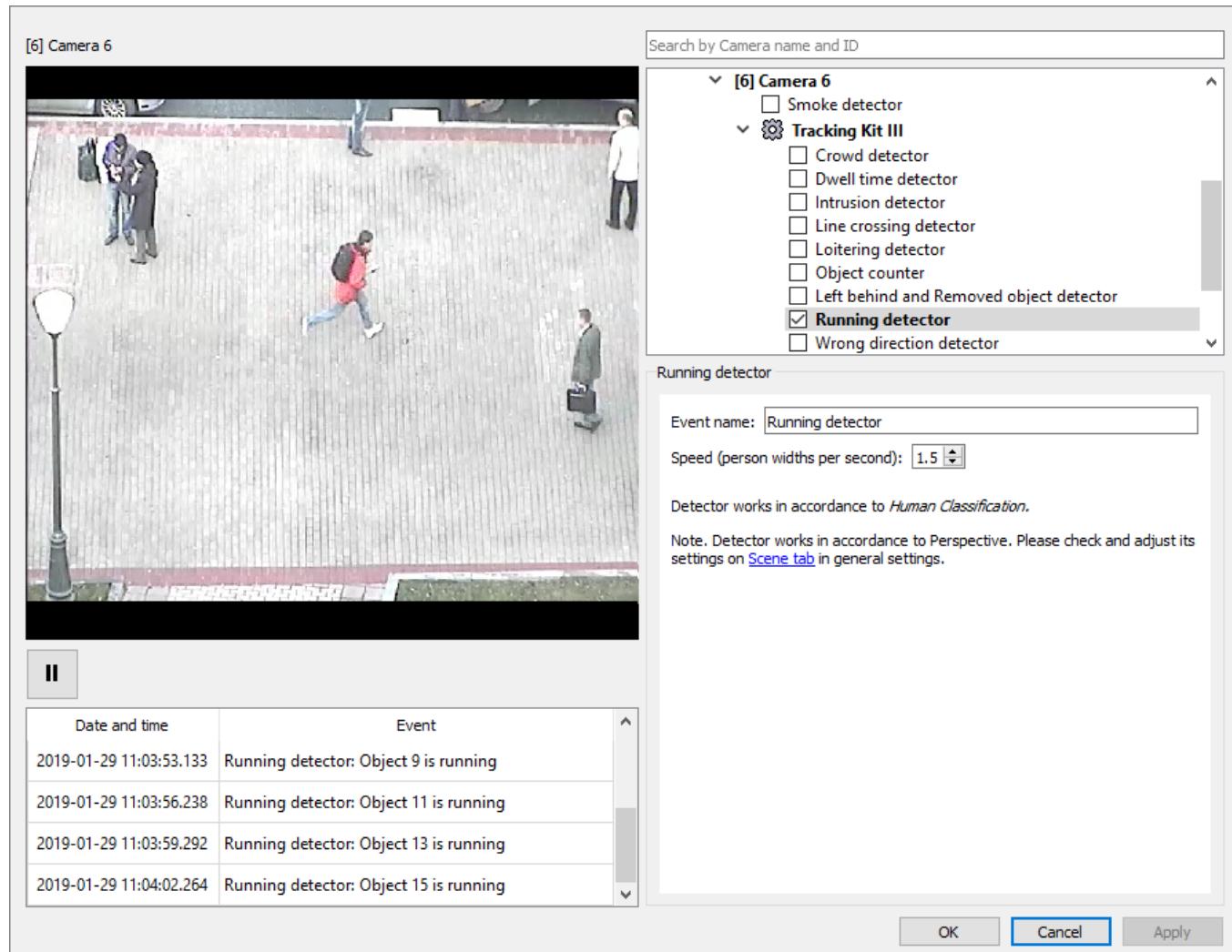


Figure 209. Running detector settings window

Table 75. Running detector settings

Parameter	Description
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> if a person's speed within the controlled area exceeds specified value.
Speed (person width per second)	Specify speed (in relative units) above which a person will be considered running. Note. Speed is specified on the base of the person's width calculated at the moment when a person is captured by detector (below an reference width). If length of trajectory, that a person passes per 1 second is Speed time greater than the reference width, then a person is considered running. Thus, depending on the trajectory, the reference width changes with the perspective.

Warning! The Perspective must be configured to use this detector (see [Scene Tab](#)).

12.2.1.2.3 Left Behind and Removed Object Detector

The detector is intended to identify object left in camera's field of view or removed from it. An item is considered left behind if it has been separated from another tracked moving object and stayed motionless within the controlled zone. A removed object is an object that has disappeared from the camera's field of view. At the same time, to be detected as removed this subject must be considered the background of the controlled area until the moment of disappearance. Controlled area and operation mode are configurable parameters of the detector.

Note. An object is considered to be within the controlled zone if the area of the object and controlled zone crossing is not less than 50% of calculated area of detected object.

Linear sizes of the left behind/removed object should not be less than 5% of frame size. For best performance of the detector, the overlapping of the objects should be minimal (moving objects should not overlap object left behind). Thus, the "top view" camera angle is optimal. Perspective view (angle view) is allowed only when the camera mounting height is sufficient and the camera's optical axis is directed down with sufficiently sharp angle. At the same time, detection of the left behind/removed objects is most reliable if the detected object is located near the camera. Objects located far from the camera can significantly overlap each other.

An essential condition for the reliable operation of the detector is stable and good lighting, which can be reached, if the camera is installed indoors. If the camera is installed in the street, the number of false positives can increase.

Left behind and Removed object detector settings window is represented in Figure 210.

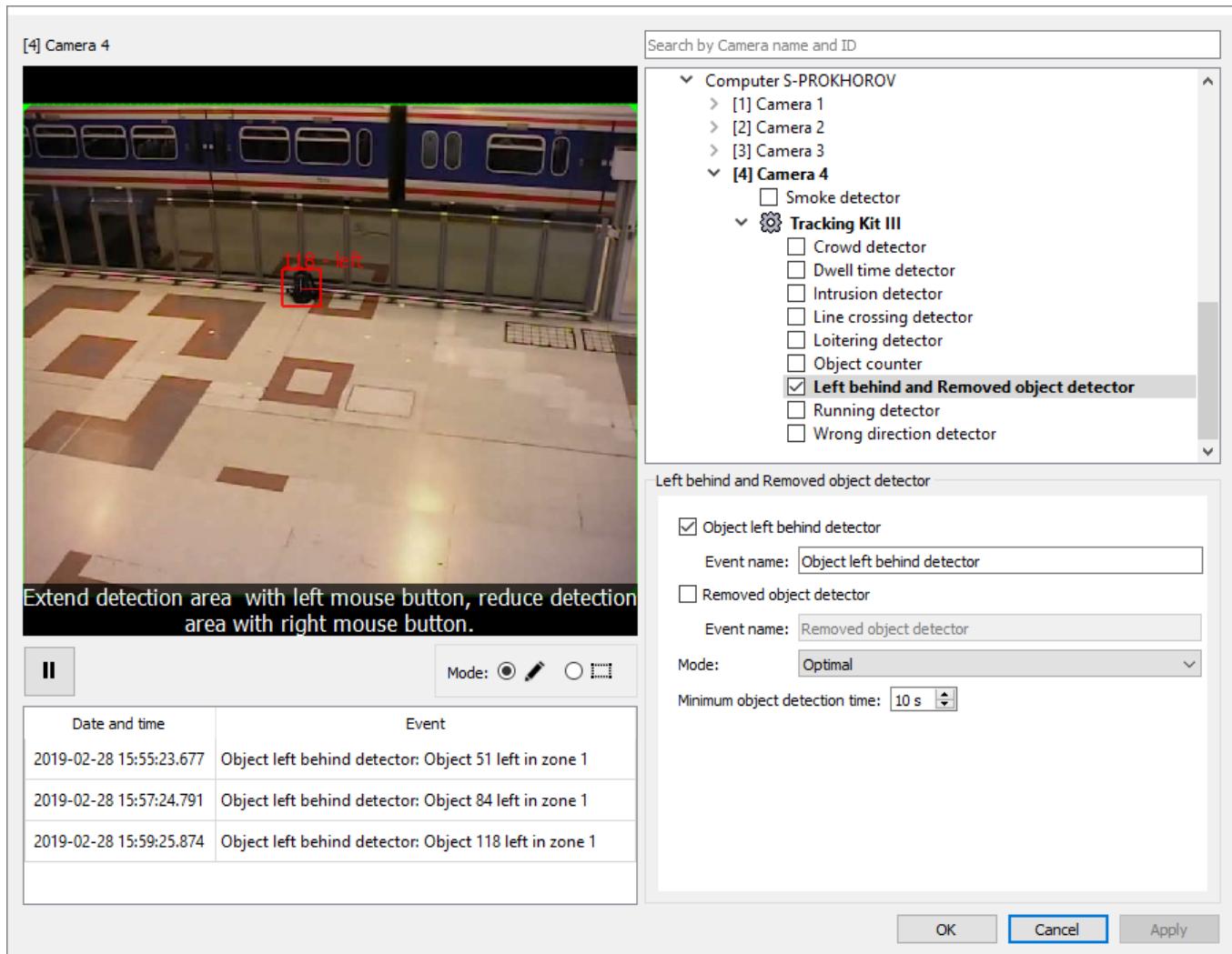


Figure 210. Left behind and Removed object detector settings window

Table 76. Left behind and Removed object detector settings

Parameter	Description
Object left behind detector	Select this checkbox to detect objects left behind in the controlled area.
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> if an object remains in the controlled area longer than the time period specified below.
Removed object detector	Select this checkbox to detect objects removed from the controlled area. By default it is deselected.
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> if an object disappeared from the camera's field of view.

Parameter	Description
Mode	<p>Select required detector mode:</p> <ul style="list-style-type: none"> • Optimal – optimal mode that provides a balance between false alarms and missed events; • Minimize false alarms – number of false positive detections is minimal, but it increases the probability of missing detection events; • Maximize true detections – number of the missing detection events is minimal, but it increases the probability of false positives.
Minimum object detection time	<p>Specify duration of the period (in seconds). An object will be considered left behind/removed when specified value will exceeded:</p> <ul style="list-style-type: none"> • for the left behind objects – the time the object was in the controlled area from the moment it appeared. In this case, the object must remain motionless during specified time period; • for the removed objects – the time elapsed after the disappearance of the object from the controlled area. At the same time, it is believed that until the moment of disappearance, the object was a part of the controlled area background. <p>Warning! If specified parameter value exceeds specified value of the Stop tracking stationary objects after (see Tracker Tab) an object will not be detected as left behind.</p>

12.2.1.2.4 Loitering Detector

Loitering is when a person stays within a controlled area for a specified time period. Controlled area and duration are the configurable parameters of the detector.

Also the object's minimum and maximum sizes must be specified or it is necessary to ensure that there are no stopped vehicles within the controlled area. For best detector performance especially in complex scenes where the simultaneous presence of a large number of people is expected it is necessary to use "top view" camera position. If the number of people within the scene is known to be not great, it is also allowable to use perspective camera view (angle view), but only when camera mounting height is sufficient and camera's optical axis is directed down with sufficiently sharp angle.

Loitering detector settings window is represented in Figure [211](#).

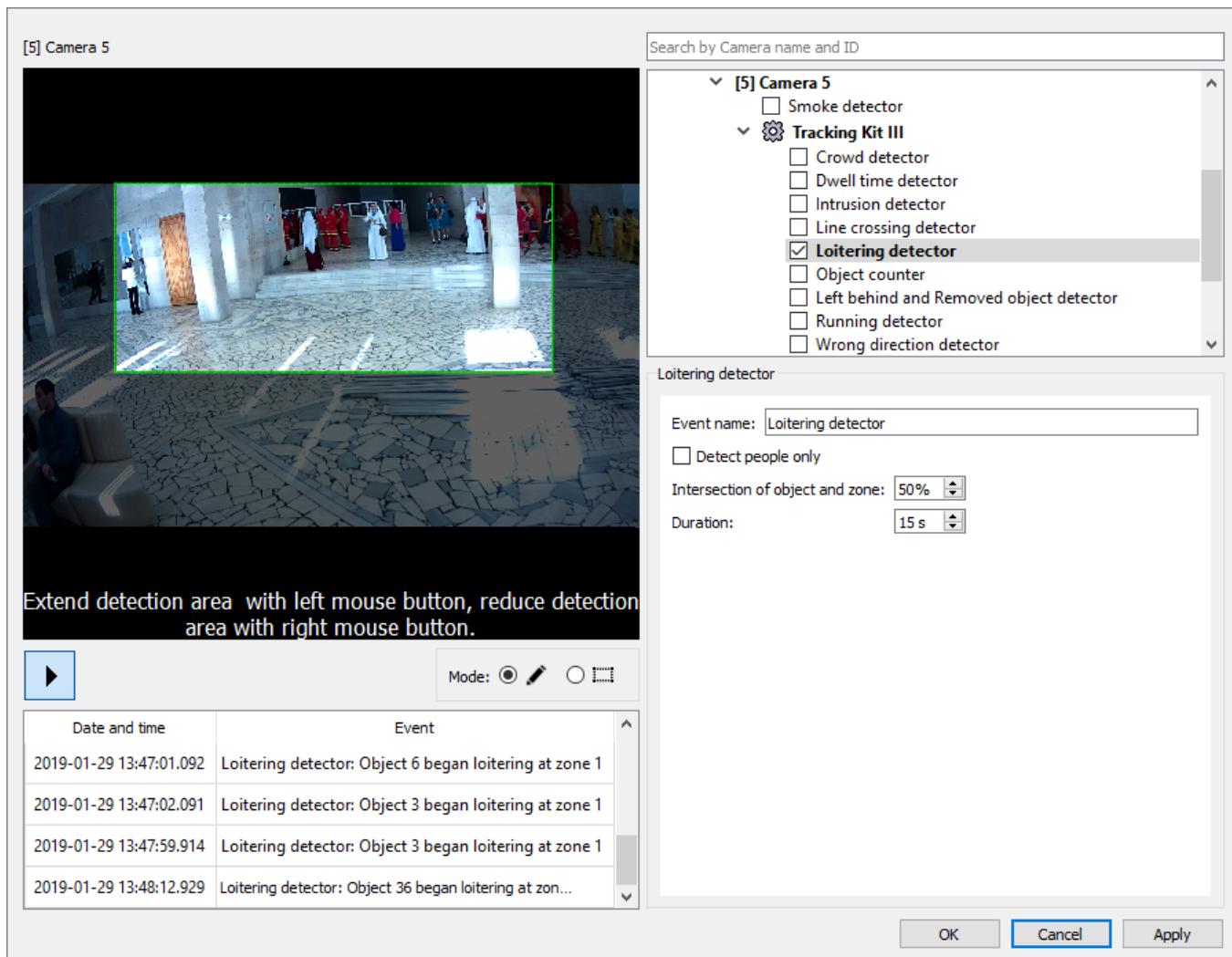


Figure 211. Loitering detector settings window

Table 77. Loitering detector settings

Parameter	Description
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> if a person stays in the controlled area for a specified time period.
Detect people only	Select this check box if only Human class of objects must be detected. Otherwise objects of any class will be detected. For more information about object classes see Classification Tab .
Intersection of object and zone	Specify intersection of the detected object and the controlled zone (in percents of the calculated area of the detected object). If this value will be exceeded, the object will be considered as entered into the controlled area.
Duration	Specify the time of a person staying in a controlled area (in seconds), that if exceeded will be considered loitering.

12.2.1.2.5 Intrusion Detector

Intrusion into an controlled area is considered as a movement (traveling or passing) of a tracked object from outside into the controlled area. The controlled area and type of the object that cause an alarm (person, vehicle or animal) are adjustable parameters of the detector.

The best performance of the detector is reached if the camera is installed above the controlled area (camera's angle is "top view") or at an angle to the controlled area ("angle view"). An angle view is allowed only when the camera mounting height is sufficient and camera's optical axis is directed down with sufficiently sharp angle. In other words, the camera angle view has to be such that the foreground objects will not obscure the controlled area.

The number of false positives can be high when there are strong (and, especially, lengthy) shadows as well as a presence of light reflections (e.g. from car headlights) in the dark.

Intrusion detector settings window is shown in Figure 212.

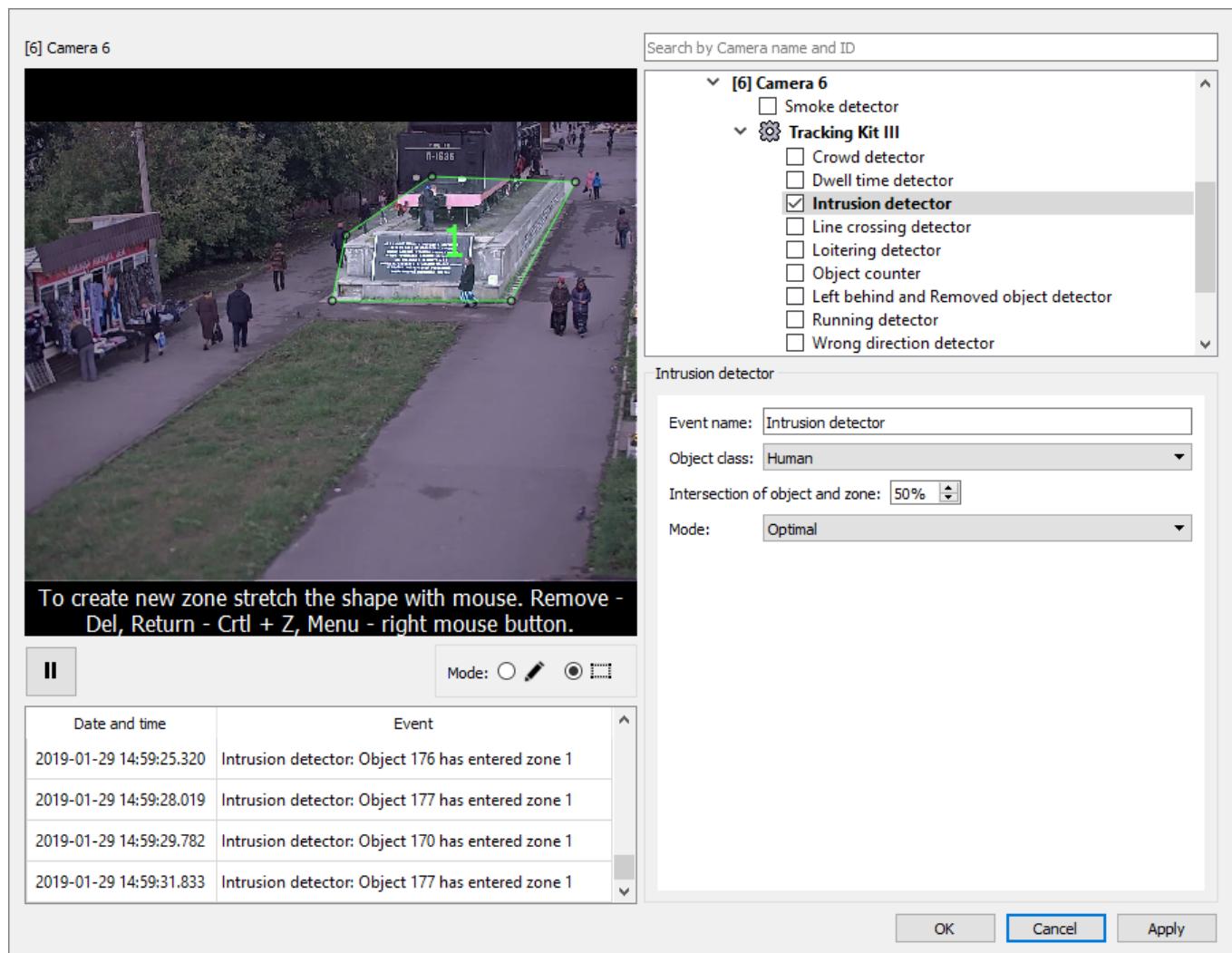


Figure 212. Intrusion detector settings window

Table 78. Intrusion detector settings

Parameter	Description
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> if object of the selected class crossed the border of the controlled area.
Object class	Choose from the list a class of the detected object. Possible values: <ul style="list-style-type: none"> • Don't use classification – all objects will be analyzed; • Vehicle – only objects classified as "vehicle" will be analyzed; • Human – only objects classified as "human" will be analyzed; • Vehicle and human – only objects classified as "vehicle" and/or "human" will be analyzed; • Animal – only objects classified as "animal" will be analyzed.
Intersection of object and zone	Specify intersection of the detected object and controlled zone (in percents of the calculated area of the detected object). If this value will be exceeded, the object will be considered as entered into the controlled area.
Mode	Select required detector mode: <ul style="list-style-type: none"> • Optimal – optimal mode that provides a balance between false alarms and missed events; • Minimize false alarms – number of false positive detections is minimal, but it increases the probability of missing detection events; • Maximize true detections – number of the missing detection events is minimal, but it increases the probability of false positives.

12.2.1.2.6 Crowd Detector

In video analytics, a crowd refers to a number of people that are simultaneously located in a controlled area during a specified time interval. The shape of the controlled area, the number of people and the time interval are configurable parameters of the detector.

Vehicle traffic within the controlled area is highly undesirable. For best performance of the detector, the camera should be installed above the controlled area (camera's angle is "top view"). A perspective view (angle view) is allowed only when the camera install height is sufficient and the camera's optical axis is directed down with sufficiently sharp angle.

Crowd detector settings window is shown in Figure 213.

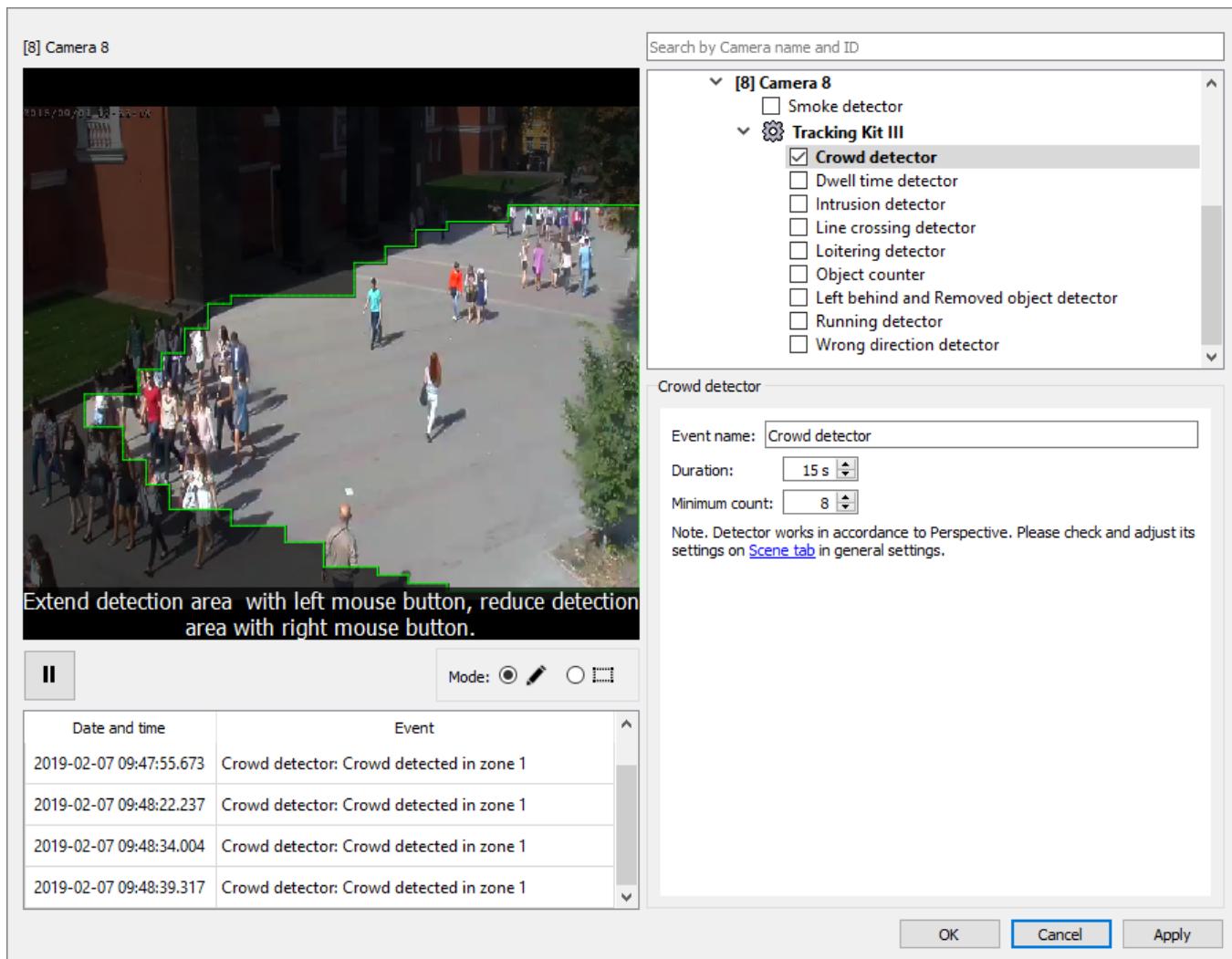


Figure 213. Crowd detector settings window

Table 79. Crowd detector settings

Parameter	Description
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> if a crowd is detected in the controlled area and it's duration in the controlled area exceeds the specified value.
Duration	Specify crowd duration in the controlled area (in seconds) which will cause detector triggering if exceeded.
Minimum count	Specify minimum number of people which will cause detector triggering if exceeded.

Warning! The Perspective must be configured to use this detector (see [Scene Tab](#)).

12.2.1.2.7 Object Counter

This detector is designed to count objects that cross the control line. Counting is performed separately for the objects that cross the control line in opposite directions. Working with several control lines is supported. In this case the counting is performed both separately for each control line and in total for all detector's control lines.

The best detection quality is reached when using "top view" camera angle. Perspective view (angle view) is allowed only when camera mounting height is sufficient and camera's optical axis is directed down with sufficiently sharp angle. The number of objects will be counted correctly only if moving objects can be visually separated within the frame. In other words, objects should not overlap each other or be moving in heavy traffic.

Object counter settings window is represented in Figure 214.

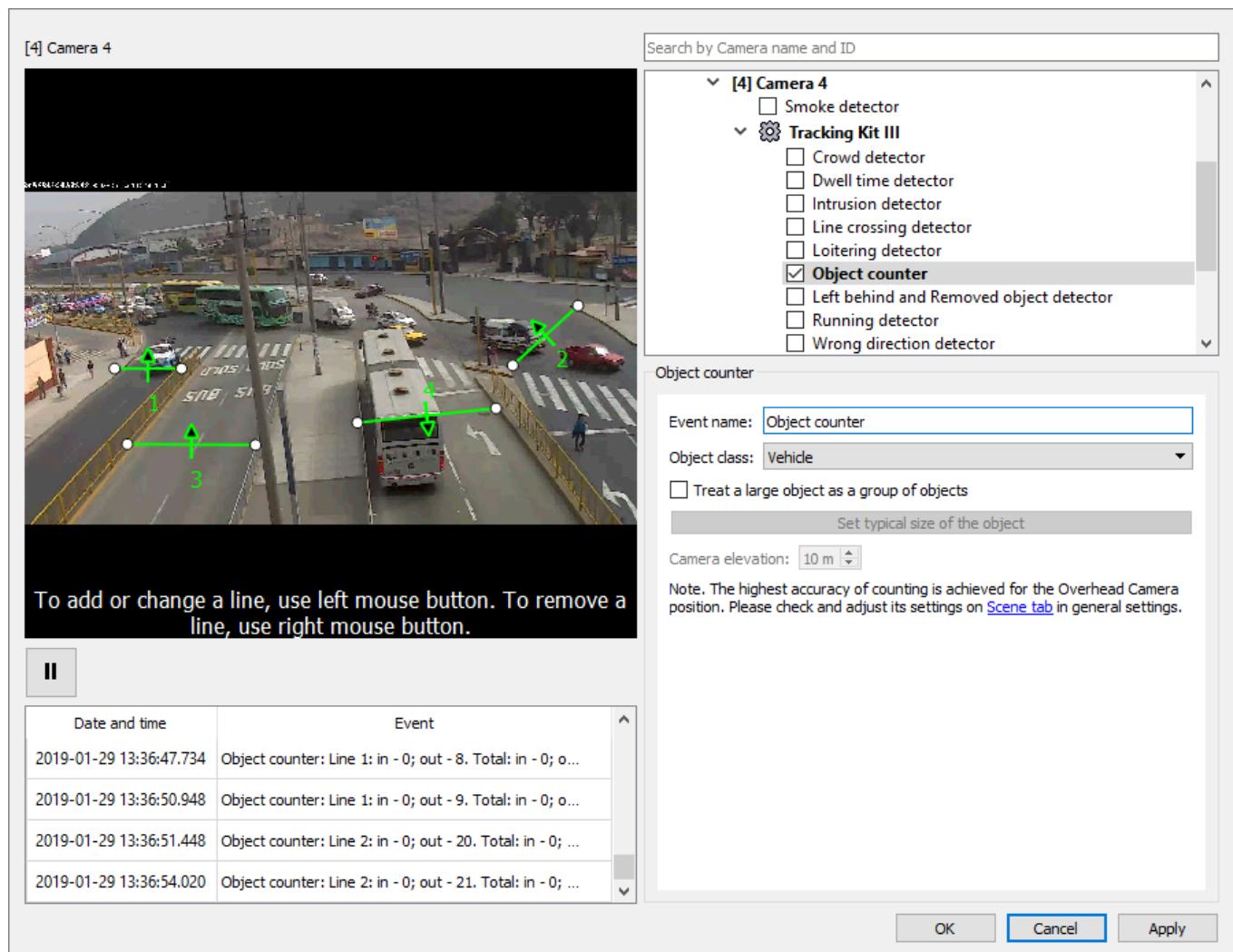


Figure 214. Object counter object settings window

Table 80. Object counter settings

Parameter	Description
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> if an object has crossed the control line.

Parameter	Description
Object class	<p>Choose from the list a class of the detected object. Possible values:</p> <ul style="list-style-type: none"> • Don't use classification – all objects will be analyzed; • Vehicle – only objects classified as "vehicle" will be analyzed; • Human – only objects classified as "human" will be analyzed; • Vehicle and human – only objects classified as "vehicle" and/or "human" will be analyzed. <p>Warning! If the Treat a large object as a group of objects check box is selected (see below) this parameter is not displayed.</p>
Treat a large object as a group of objects	Select this check box if the objects in the frame cannot be visually separated. If this check box is selected, the algorithm for dividing a large object into the separate objects will be applied when calculating the number of objects.
Parameters described below are enabled if the Treat a large object as a group of objects check box is selected.	
Set typical size of the object	Click the button to specify character sizes of the object on the frame. Character sizes allow to separate "large" objects and all other detected objects within the frame. If the size of the object in the frame exceeds the upper limit of the specified range of sizes, such an object will be considered "large". Character sizes of the object are specified in the same way as the sizes of the detected object in the frame are specified (see Scene Tab , the Object size limits parameter). The range of character sizes of an object should lie within the range of sizes of detected objects.
Camera elevation	Specify <i>Camera</i> elevation under the controlled scene.

When configuring object counter it is necessary to draw one or several *Control lines*. All objects of the specified class, that cross a specified *Control line*, which sizes are within range specified in the global plugin (see **Scene Tab**) settings will be detected and counted.

Warning! The maximum number of the *Control lines* is limited.

To draw a *Control line* on the frame image, move mouse pointer to the required point on the frame and click the left mouse button. Holding mouse button pressed, draw a line in the required direction. A line will be added onto the frame. Incoming direction will be labeled with directed arrows. Objects that cross the line in the given direction will be considered "incoming" and in reverse direction - "outgoing". "Incoming" and "outgoing" objects are counted separately. Number of counted objects of each type will be displayed in the **Comment** field of the *Event Viewer*.

Note. Direction of arrows on the control line depends on how the line is drawn (left-to-right or right-to-left).

To remove a line right click it and select the **Remove line** command in the context menu.

Note. The last line remaining in the frame can not be deleted.

12.2.1.2.8 Line Crossing Detector

This detector is designed to count objects that cross the control line. The total number of line crossings is calculated regardless of the direction of the object movement. Working with several control lines is supported. In this case, the counting is performed both separately, for each control line, and in total, for all detector's control lines.

The highest counting accuracy is achieved when contrast between the object and the background is good enough. When weather is bad and there is water on the asphalt local interference may occur that interfere with the detection of objects as a result of which the detector may not trigger.

Line crossing detector settings window is represented in Figure 215.

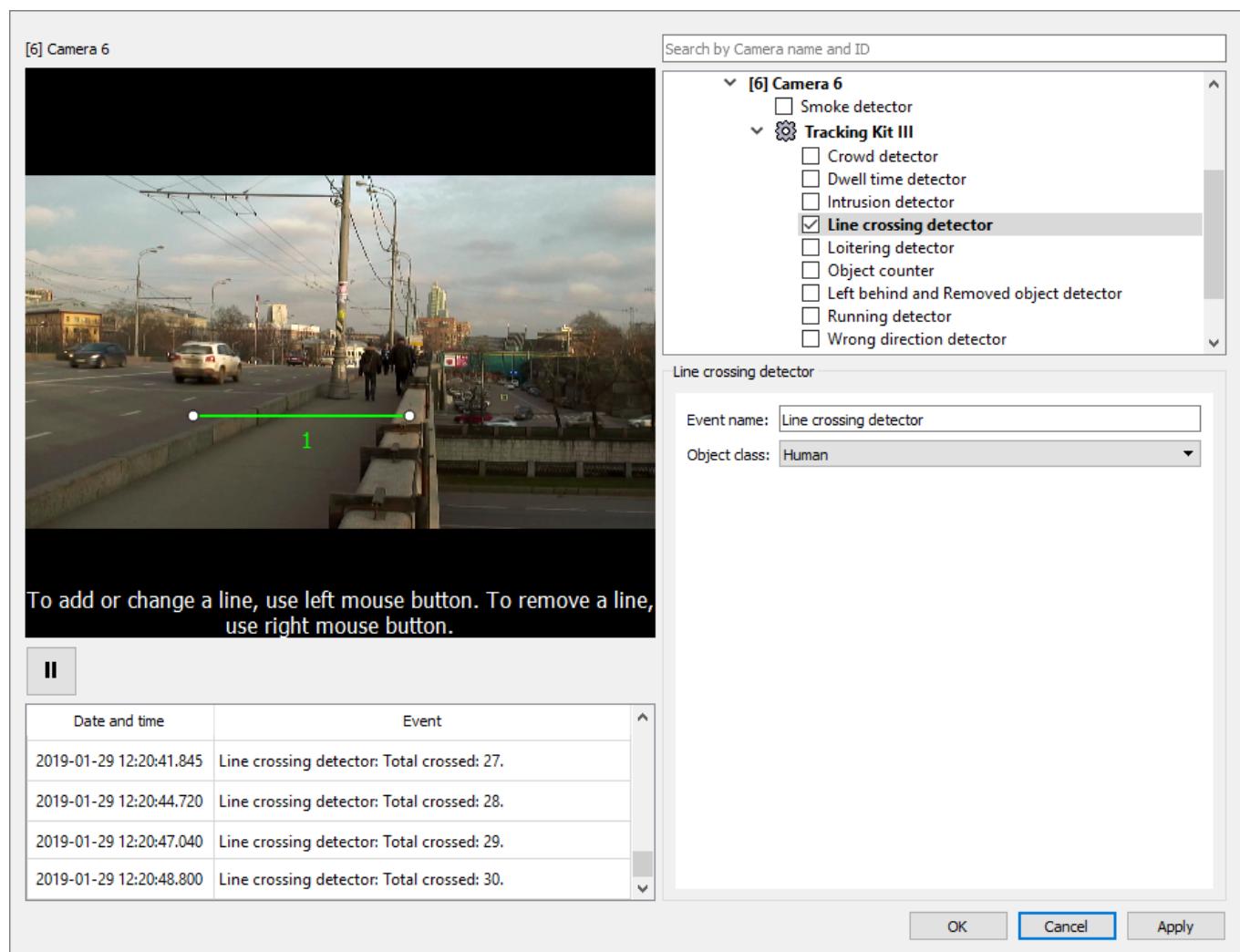


Figure 215. Line crossing detector settings window

Table 81. Line crossing detector settings

Parameter	Description
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> if an object has crossed the control line.

Parameter	Description
Object class	<p>Choose from the list a class of the detected object. Possible values:</p> <ul style="list-style-type: none"> • Don't use classification – all objects will be analyzed; • Vehicle – only objects classified as "vehicle" will be analyzed; • Human – only objects classified as "human" will be analyzed; • Vehicle and human – only objects classified as "vehicle" and/or "human" will be analyzed.

When configuring object counter it is necessary to draw one or several *Control lines*. All objects of the specified class, that cross a specified *Control line*, which sizes are within range specified in the global plugin (see [Scene Tab](#)) settings will be detected and counted.

Warning! The maximum number of the *Control lines* is limited.

To draw a *Control line* on the frame image, move mouse pointer to the required point on the frame and click the left mouse button. Holding mouse button pressed, draw a line in the required direction. A line will be added onto the frame. The total number of objects will be displayed in the **Comment** field of the *Event Viewer*.

To remove a line right click it and select the **Remove line** command in the context menu.

Note. The last line remaining in the frame can not be deleted.

12.2.1.2.9 Dwell Time Detector

This detector is designed to collect statistics about long/short-term stay of people in a particular place. Controlled area and threshold of the long/short term staying in the zone are configurable parameters of the detector. Working with one rectangular or several polygonal zones is supported (for the details see [Configuring Controlled Zone](#)).

The object must be continuously recognized throughout its stay in the zone.

Also the object's minimum and maximum sizes must be specified or it is necessary to ensure that there are no stopped vehicles within the controlled area. For best detector performance especially in complex scenes where the simultaneous presence of a large number of people are expected it is necessary to use "top view" camera position. The number of false positives can be high when there are strong (and, especially, lengthy) shadows as well as a presence of light reflections (e.g. from car headlights) in the dark.

The highest counting accuracy is achieved when contrast between the object and the background is good enough. When weather is bad and there is water on the asphalt local interference may occur that interfere with the detection of objects as a result of which the detector may not trigger.

Dwell time detector settings window is shown in Figure 216.

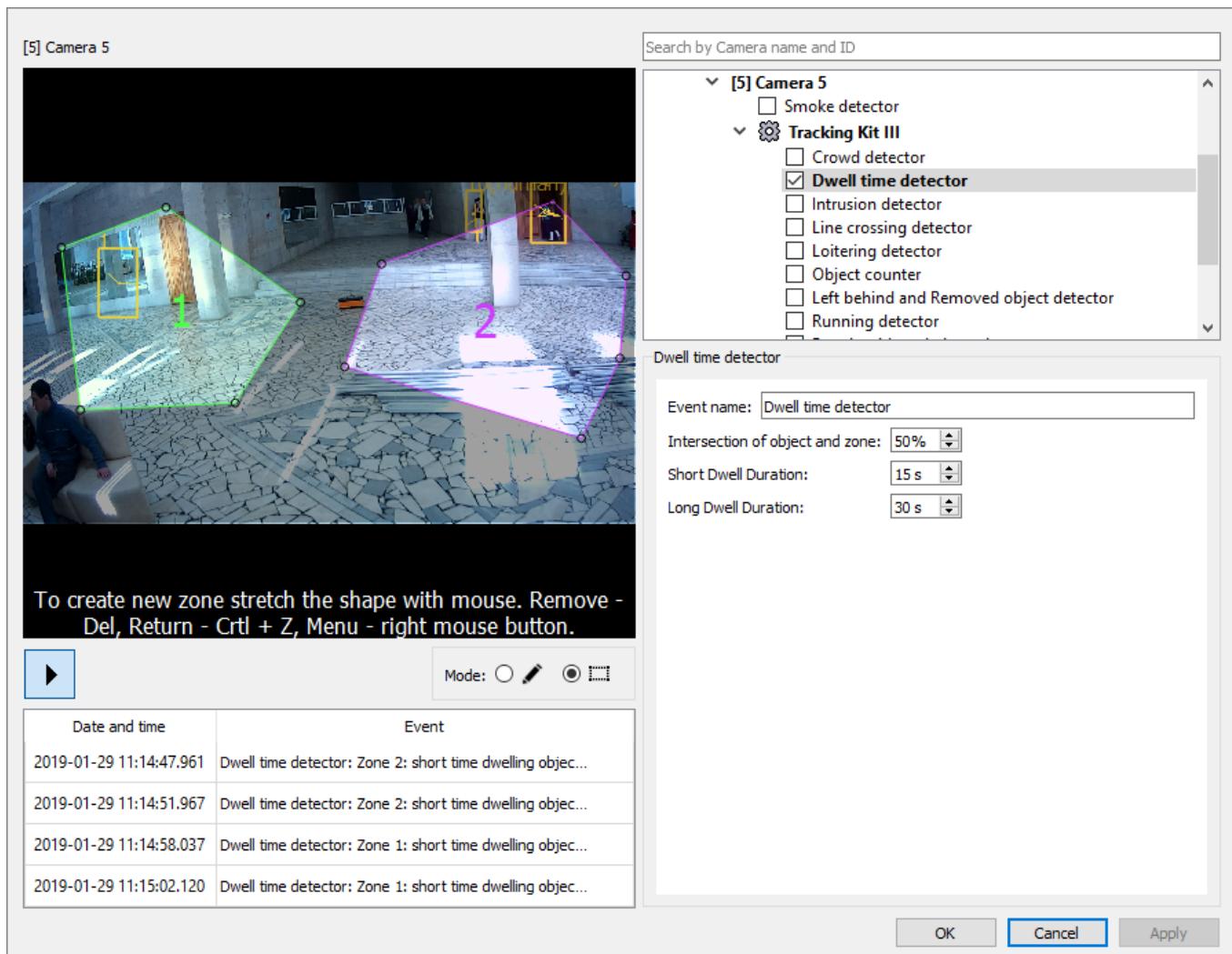


Figure 216. Dwell time detector settings window

Table 82. Dwell time detector settings

Parameter	Description
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> if thresholds of staying in the zone are exceeded.
Intersection of object and zone	Specify intersection of the detected object and the controlled zone (in percents of the calculated area of the detected object). If this value will be exceeded, the object will be considered as entered into the controlled area.
Short Dwell Duration	Set the duration of the object's stay in the zone (in seconds). If this value is exceeded the object's stay in the zone will be considered <i>Short-term</i> .
Long Dwell Duration	Set the duration of the object's stay in the zone (in seconds). If this value is exceeded the object's stay in the zone will be considered <i>Long-term</i> .

When configuring the detector it is necessary to draw one or several *Control zones*. It is not recommended to choose large areas. If there are several zones specified then object counting will be performed independently for each zone.

The following information is displayed in the protocol as a result of detector working:

- The number of objects short-term staying in the zone at the moment of the event generation.
- The number of objects short-term staying in the zone from the beginning of the detector working.
- The number of objects long-term staying in the zone at the moment of the event generation.
- The number of objects long-term staying in the zone from the beginning of the detector working.

12.2.1.2.10 Wrong Direction Detector

This detector is designed to detect a movement in the wrong direction.

For successful detector triggering, an accurate determination of the object's trajectory is necessary. The object must be continuously recognized over a certain time period.

The highest counting accuracy is achieved when contrast between the object and the background is good enough. When weather is bad and there is water on the asphalt local interference may occur that interfere with the detection of objects as a result of which the detector may not trigger.

Wrong direction detector settings window is shown in Figure 217.

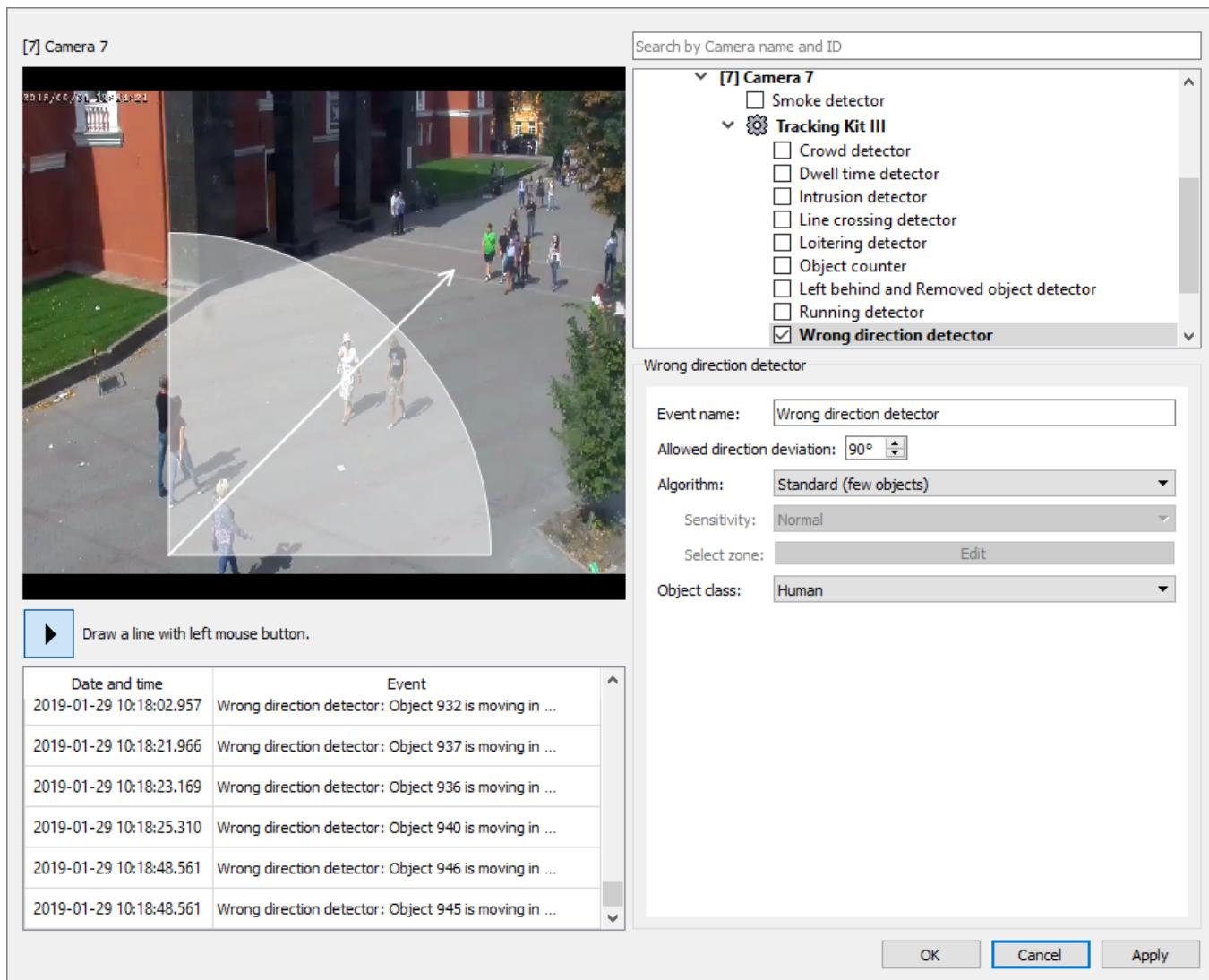


Figure 217. Wrong direction detector settings window

Table 83. Wrong direction detector settings

Parameter	Description
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> when an object moving in the wrong direction will be detected.
Allowed direction deviation	Specify the deviation sector (in degrees) from the specified vector of the wrong direction, within which it will be assumed that the object also moves in the wrong direction.
Algorithm	Select required detection algorithm depending on the controlled scene. Possible values: <ul style="list-style-type: none"> • Standard (few objects) – the number of objects in the frame is small. Objects can be visually separated; • Advanced (crowd) – the number of objects in the frame is large. Objects cannot be visually separated.

Parameter	Description
Object class	Choose from the list a class of the detected object. Possible values: <ul style="list-style-type: none"> • Don't use classification – all objects will be analyzed; • Vehicle – only objects classified as "vehicle" will be analyzed; • Human – only objects classified as "human" will be analyzed; • Vehicle and human – only objects classified as "vehicle" and/or "human" will be analyzed.
Parameters below are enabled only when the Advanced (crowd) Algorithm is used	
Sensitivity	Specify sensitivity of the detection algorithm. Possible values: <ul style="list-style-type: none"> • Low – number of false positive detections is minimal but it increases the probability of missing detection events; • Normal (is the default value) – optimal mode that provides a balance between false alarms and missed events; • High – number of the missing detection events is minimal, but it increases the probability of false positives.
Select zone	In the frame draw a <i>Control zone</i> within which the Advanced (crowd) algorithm will be applied. Procedure for detection area configuration is described in Configuring Controlled Zone .

When configuring the detector it is necessary to set the vector of the wrong direction of movement and the angle of deviation within which the direction of movement will also be considered wrong. This angle deviation is displayed automatically depending on specified value of the **Allowed direction deviation** parameter (see Figure 217).

To draw a vector of wrong direction move mouse pointer to the required point on the frame and click the left mouse button. Holding mouse button pressed, draw a line in the required direction. The line with arrow, indication the wrong direction, and the deviation sector will be drawn on the frame. Information about objects moving in wrong direction will be displayed in the **Comment** field of the **Event Viewer**.

12.2.2 Representation of video analytics detector operation results

When SecurOS video analytics detector is triggered, the system forms an event, that may be processed by *VB/JavaScript program* (see [SecurOS Programming Guide](#)) or tracked by operator on the *Event viewer*. Event is being formed by *Camera* object, for which the video analytics detector is created, and has **Video analytics event** title (`VCA_EVENT`) irrespective to detector type. Meanwhile on the *Event viewer* will be displayed name, that is set in the detector settings (**Event name** parameter).

Note. If not set, then default value that matches the detector name is used.

If necessary, operator can react to detection event. For example, one can switch from *Event Viewer* window to *Media Client* or send an *Emergency ticket* to *Emergency service* (see [SecurOS Quick User Guide](#)).

12.3 Smoke Detector

This detector is designed to detect smoke. Controlled area and sensitivity are configurable parameters of the detector.

In SecurOS a separate instance of *Smoke detector* corresponds to each *Camera*. Each detector is configured independently of the Tracking Kit III plugin and its detectors. To configure detector select the *Computer Vision* object in the SecurOS *Object Tree*, then select required *Camera* in the camera list and select the check box for the child *Smoke detector* object. The system activates the detector's parameters settings window.

Smoke detector settings window is represented in Figure 218.

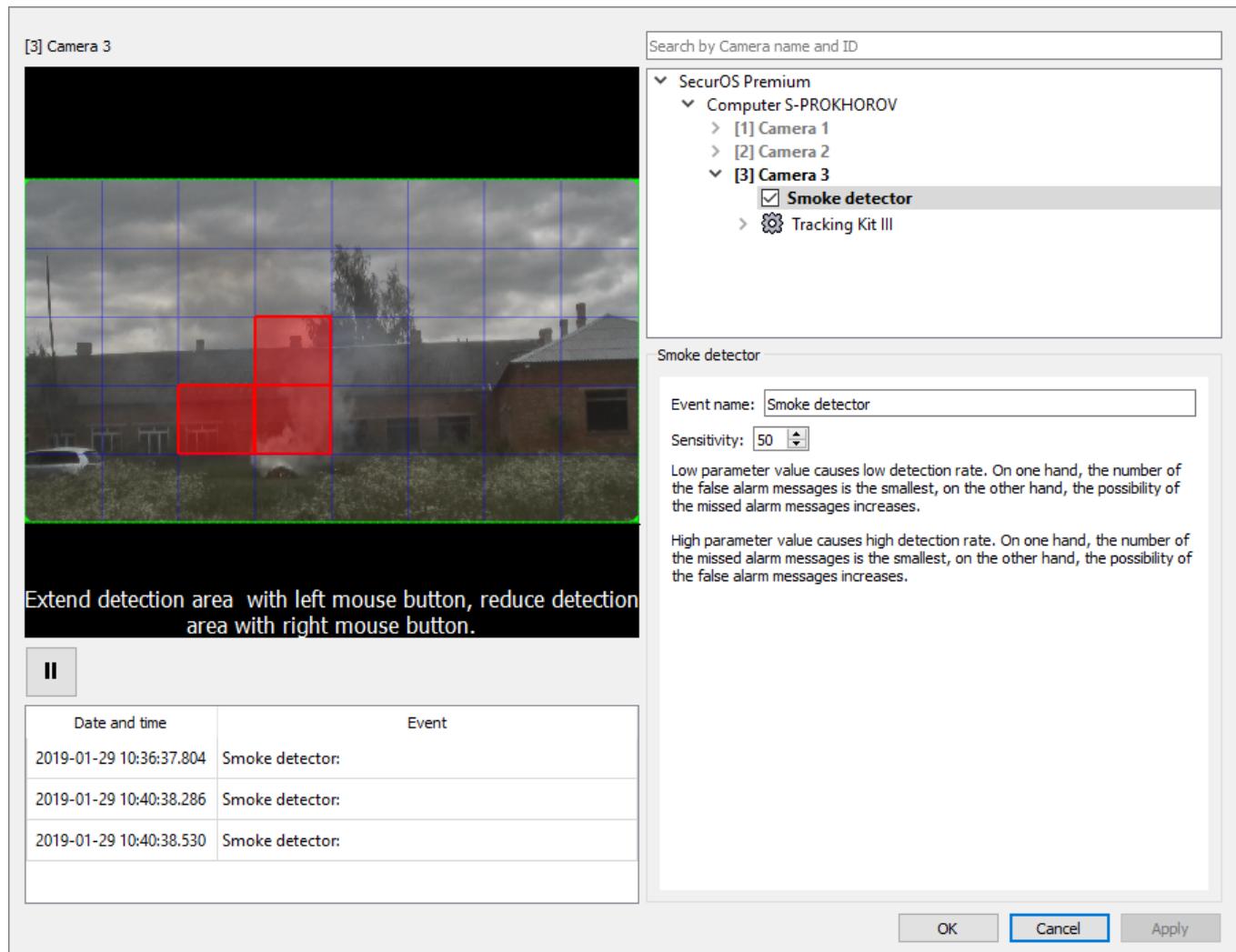


Figure 218. Smoke detector settings window

Table 84. Smoke detector settings

Parameter	Description
Event name	Specify a name of the event that will be registered in the <i>Event Viewer</i> if a smoke is detected within the controlled area.
Sensitivity	Specify detector's sensitivity (in relative units). Sensitivity affects the speed of the detector triggering when the detection event occurs. A detailed description of the detector's working algorithm depending on the specified value is provided on the parameter settings tab.

Detection area can be limited. Procedure for detection area configuration is described in [Configuring Controlled Zone](#).

12.3.1 Recommendations on Camera Configuration for Smoke Detector

Below are the additional requirements for the scene, cameras, and light source locations that must be followed to solve smoke detection video analytics task. If these requirements are not met this may result in false positive or false negative detector triggering.

1. Minimum allowed frame resolution is 640x480 pixels. Maximum resolution is not limited in a whole.
2. Minimum FPS value: 5 fps. FPS of the video stream must be stable otherwise correct working of the detectors is not guaranteed.
3. Linear sizes of the smoked area should not be less than 10% of frame size.

For other recommendations on setting up and positioning cameras, see [General Recommendations on Camera Configuration and Location](#).

13 Monitoring & Control Center

This functionality is available in the *SecurOS Monitoring & Control Center* only.

SecurOS MCC Edition allows to build a common regional *Monitoring & Control Center* that can work with several territorially separated security systems.

Note. Further the *SecurOS Monitoring & Control Center* will be referred as a *Monitoring Center*.

There are three types of the *Monitoring Center*, that differ by the method of the connection to the *Remote system*:

- SecurOS MCC Direct Connect – direct connection.
- SecurOS MCC VC Connect – connection via *Video Concentrator* (further will be referred to as VC-connection).
- SecurOS MCC VR Connect – connection via *Video Repeater* (further will be referred to as VR-connection).

Warning! Correct work of the SecurOS MCC is guaranteed if version number of SecurOS, installed in the *Remote system*, is equal or less than SecurOS MCC version number. At the same time, version compatibility is limited. For more information contact Intelligent Security Systems Technical Support Team.

VC-connection must be used when both no integration with SecurOS Auto is required and one of the following is required:

- interaction with the *Remote system*, where version of the installed SecurOS software is below 9.1.
- video gate feature is desirable.

Note. When video gate feature is used, then each video stream queried from the *Remote system* is transmitted to the *Monitoring Center* only once, regardless of how many users of that video stream are in the *Monitoring Center*.

VR-connection must be used when no integration with SecurOS Auto is required and video stream from cameras of the *Remote system* must be recorded locally in the *Monitoring Center*.

Direct connection must be used in all other cases, including video gate feature.

Working with remote objects is only possible when the *Remote system* configurations are downloaded into the SecurOS MCC. Features of the configuration downloading procedure are described in the **Direct Connection** and **VC/VR-connection** sections.

Different types of connection can be used in the same SecurOS MCC server both separately and simultaneously, complementing each other in the last case. Features of the *Monitoring Center* for different connection types are described in Table 85.

Table 85. Features of the SecurOS MCC for different connection types

SecurOS MCC Features	Connection type		
	Direct	VC	VR
SecurOS Editions supported in Remote systems			
SecurOS Xpress	•	•	•
SecurOS Professional	•	•	•
SecurOS Premium	•	•	•
SecurOS Enterprise	•	•	•
Supported versions of the SecurOS Editions			
9.1 and above	•	•	•
below 9.1		•	•
Integration with Intelligent Modules installed in the Remote Systems			
SecurOS Auto	•		
Working with Remote System Configuration			
Automatic Update Configuration in SecurOS MCC	•		
Manual Update Configuration in SecurOS MCC		•	•
Partial Downloading of <i>Remote System</i> Configuration to SecurOS MCC		•	•
Working with Remote System Cameras with the Help of Media Client			
Multi-Streaming Support	•	•	
Video Gate	•	•	•
Viewing Live Video	•	•	•
Viewing Video Archive from <i>Remote System</i>	•	•	
Viewing Archive Video Recorded in <i>Monitoring Center</i>			•
Viewing Long-term Archive Recorded in <i>Remote System</i>	•		
Managing Archive Recording in <i>Remote System</i>	•		
Managing Archive Recording in <i>Monitoring Center</i>			•
Alarm Mode Control	•		

Digital Zoom	•	•	•
Wiper Control	•		
Washer Kit Control	•		
Working with Camera Speaker	•		
Exporting Frames	•	•	•
PTZ Control	•	•	•
Separate Telemetry Control Support	•	•	•
Adding and Storing Bookmarks	•	•	•
Searching Bookmark	•	•	•
Searching Alarms	•		
Smart Search	•		
Searching Video Fragments by Date	•	•	•
Exporting Primary Video Archive	•	•	•
Exporting Long-term Video Archive	•		
Integration with WebView			
Supporting WebView Server	•	•	•
Viewing live and archive video, recorded with the help of the <i>Cameras</i> of the <i>Remote System</i> , with the help of <i>WebView Monitor</i>	•	•	•
Integration with WebConnect			
Viewing live and archive video, recorded with the help of the <i>Cameras</i> of the <i>Remote System</i>	•	•	•
Searching and viewing <i>Alarms</i> registered by the <i>Cameras</i> of the <i>Remote System</i>	•	•	•
Controlling PTZ of the <i>Cameras</i> of the <i>Remote System</i>	•	•	•
Working with the <i>Presets</i> of the <i>Cameras</i> of the <i>Remote System</i>	•	•	•
Exporting <i>Primary archive</i> from the <i>Cameras</i> of the <i>Remote System</i>	•	•	•
Working with Remote System Microphones with the Help of Media Client			

Listening to live sound from <i>Microphones</i> linked to the <i>Remote System Cameras</i> (when viewing a video)	•			
Listening to live sound from independent <i>Microphones</i> of the <i>Remote System</i>	•			
Controlling video (with audio)/audio archive recording mode in <i>Remote System</i>	•			
Listening to archive sound from <i>Microphones</i> linked to the <i>Remote System Cameras</i> (when viewing a video)	•			
Listening to archive sound from independent <i>Microphones</i> of the <i>Remote System</i>	•			
Exporting <i>Remote System</i> video archive (with audio)	•			
Exporting <i>Remote System</i> audio archive	•			

Working with Remote System Events with the Help of Event Viewer

Receiving All Events	•			
Receiving Server State Changing Events	•	•		•
Receiving Cameras State Changing Events		•		
Monitoring Events	•	•		•
Filtering Events	•	•		•
Viewing Event in <i>Media Client</i>	•	•		•

Working with Remote System Objects with the Help of Other Interface Subsystem Objects

Self-Diagnostic of State of Downloaded Objects of Remote Systems with the Help of <i>Health Monitor Module</i>	•			
Self-Diagnostic of State of Local Proxy-Object of Remote Systems with the Help of <i>Health Monitor Module</i>		•		•
Remote System Objects Control with the Help of <i>Map Window</i>	•			
Complex Object Control with the Help of <i>VB/JScript programs</i>	•			
Telemetry Control with the Help of <i>VB/JScript programs</i>		•		•

13.1 Direct Connection

With a direct connection, the *Monitoring Center* center can be configured to work with remote archives only.

13.1.1 Limitations

There are a few limitations that ensure correct operation of the *Monitoring Center* when direct connection is used:

1. Versions of the SecurOS MCC and SecurOS installed in the *Remote systems* should not be lower, than 9.1.
2. Regional settings, specified in the operation system parameters, should be the same on the SecurOS MCC's servers and *Remote systems* SecurOS's servers.
3. Intelligent Modules installed in the *Remote system* must also be installed in the SecurOS MCC.

13.1.2 Setting Up Direct Connection

To set up direct connection of the *Monitoring Center* do the following:

Note. Setting up procedure can be performed on any computer where SecurOS MCC is installed.

1. Create an configure the **Remote system** object (see [The location and names of the Remote system's objects](#)) in the *Monitoring Center's Object Tree*.

Warning!

1. Only SecurOS MCC's superuser (see [SecurOS Users](#)) can create and configure the *Remote system* object.
2. If it is necessary to limit number of messages transmitted to the *Monitoring Center* from the *Remote system*, choose the preliminary created [Event Filter](#) in the object settings.

2. In the **User Rights** object settings specify the required access rights to the *Cameras* of the *Remote system* for the operators of the *Monitoring Center*.

Note. By default, after downloading the configuration to the *Monitoring Center*, operator does not have access to the *Remote system* object and all children objects.

When configuration is downloaded, the separate *Objects Visibility Tree* for each connected *Remote system* is created in the *Monitoring Center's Object Tree*. This tree is located on the same hierarchy level as the *Monitoring Center's System* object (see Figure 219). Only the following objects of the *Remote system* are displayed in the *Objects Visibility Tree*:

1. *Databases*;
2. *Computers*;
3. *Cameras*;
4. *Microphones*;
5. *Zones*;

6. Sensors;
 7. Relays;
 8. Archivers.

Note. "Visibility" of the *Remote system*'s objects in the SecurOS MCC means the possibility of direct interaction with these objects. In this case, the operator's access to the settings and other operations with these objects in the *Object Tree* (Disable/Rename/Delete) is prohibited.

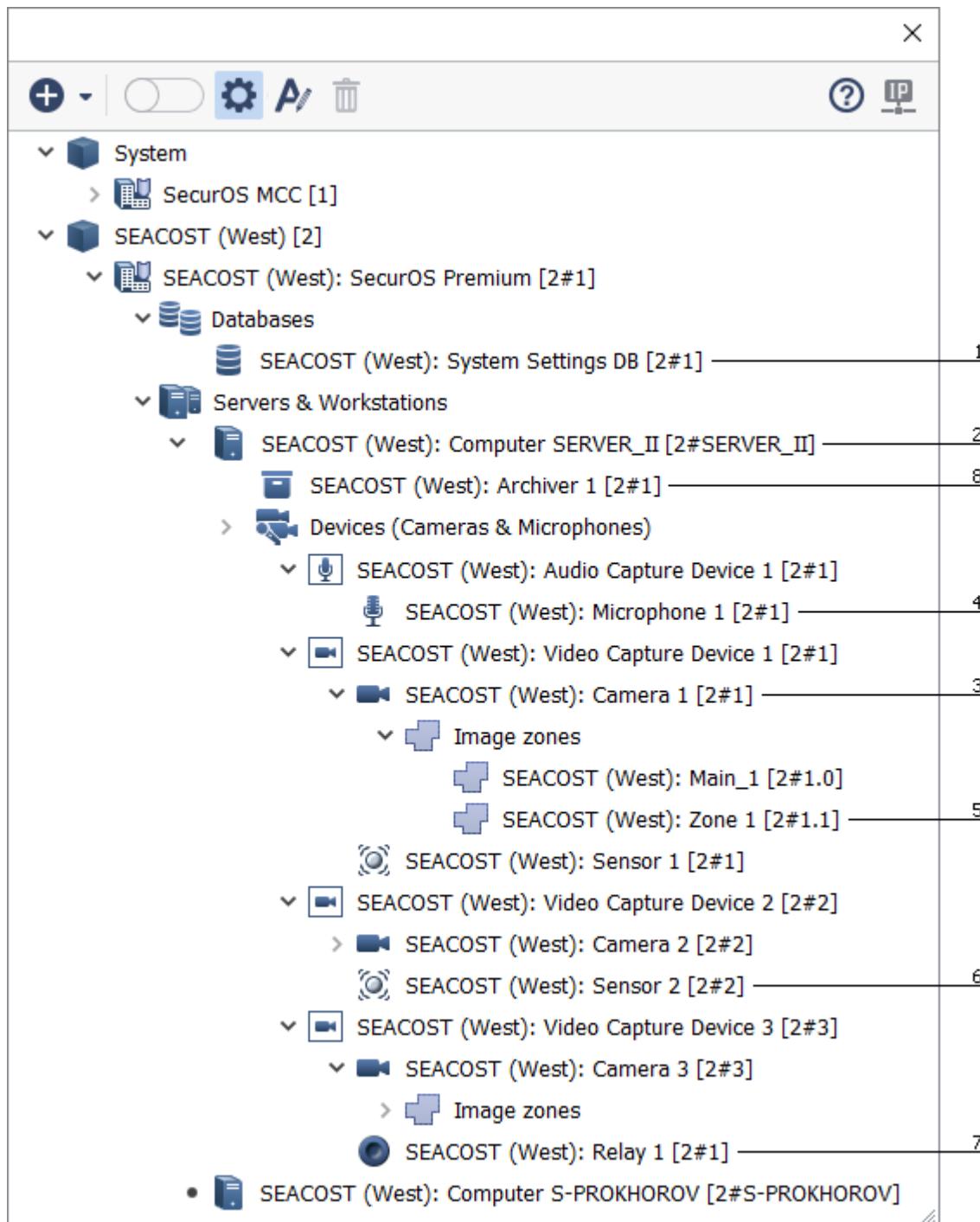


Figure 219. Configuration of the Remote system displayed in the Monitoring Center's Object Tree

The location and names of the Remote system's objects

Remote system object is created in the *Object Tree* on the same hierarchy level, as the *System* object of the *Monitoring Center*. **Name** and **ID**, which are assigned to the remote system when you create it, bring, as a rule, useful information. For example, where this *Remote system* is located. After the configuration is downloaded, the **Names** and **IDs** of the following format are assigned to the objects of the *Remote system*:

- **Object Name:** <Remote system Name>:<space><Remote system object Name>
- **Object ID:** <Remote system ID>#<Remote system object ID>

13.1.2.1 Remote System

This functionality is available in the *SecurOS Monitoring & Control Center* only.

The object is used to provide a connection between current (*Monitoring Center*) and *Remote SecurOS* security system.

To create this object select the **System** object in the SecurOS MCC's *Object Tree*, then click the **Create** button and select the *Remote System* item.

SecurOS MCC provides the video gate feature when receiving video from the *Remote System*. When using the video gate feature only one video stream will be requested from the *Remote System* regardless of the number of the consumers of this stream in the SecurOS MCC. Thus, the use of the video gate feature allows significantly reduce the network traffic.

To use the video gate feature do the following:

1. In the SecurOS MCC *Object Tree* select arbitrary *Video Server* that will be used as the video gate.
2. For the selected *Video Server* create a *MCC DC Gateway* child object.
3. Choose created gateway in the *Remote System* object settings (see Figure 220 and Table 86).

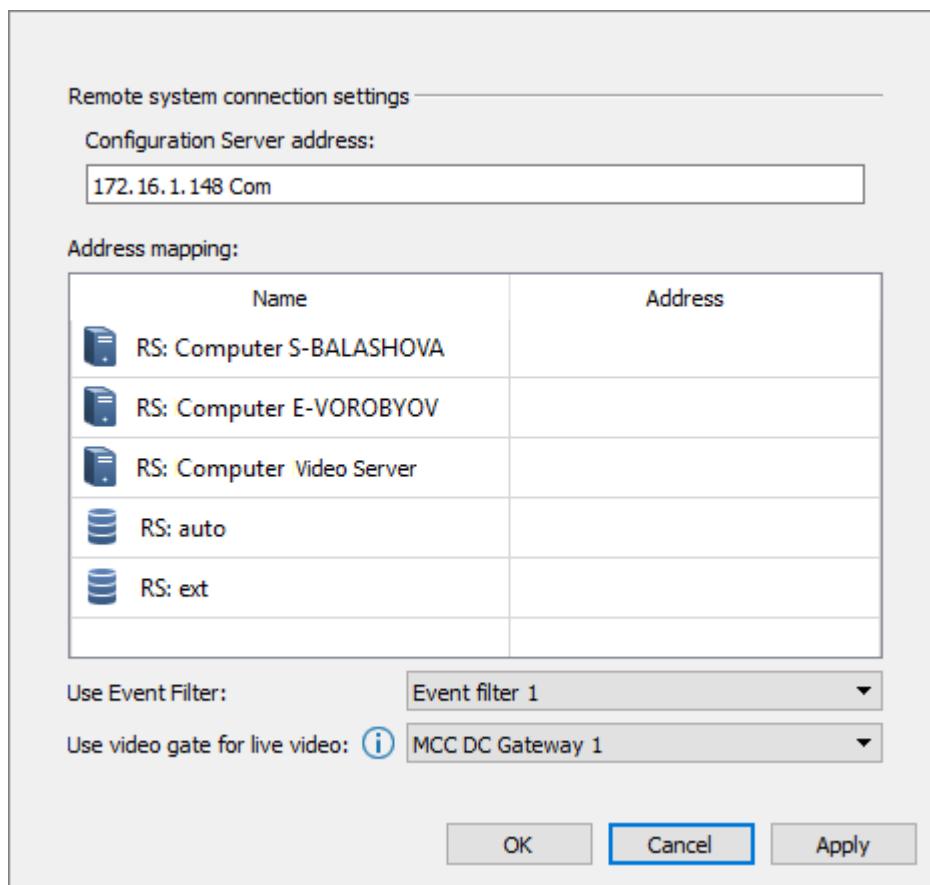


Figure 220. Remote system object settings window

Table 86. Remote system object settings

Parameter	Description
Configuration address	Specify the IP address of the <i>Configuration Server</i> of the SecurOS <i>Remote system</i> .
Address mapping	Table of correspondence between the names of the <i>Computers</i> and the <i>Database</i> of the <i>Remote system</i> and their public IP addresses. This parameter is specified if necessary, for example, if <i>Monitoring Center</i> and <i>Remote system</i> are connected via VPN, or they are located in different provider's networks, etc.
Use Event filter	<p>Specify one of the Event filters created and configured within <i>Monitoring Center</i> to limit number of messages that are being sent from the <i>Remote system</i> to the <i>Monitoring Center</i>.</p> <p>Warning! If such a filter does not exist or is not configured, then all messages generated within <i>Remote system</i> will be transmitted to the <i>Monitoring Center</i>. This can cause overloading of the communication channel and unstable work of the monitoring center.</p>

Parameter	Description
Use video gate for live video	Select from the drop-down list one of the MCC DC Gateways created in the <i>Monitoring Center</i> if it is necessary to reduce the loading of the communication channel between the <i>Remote System</i> and the <i>Monitoring Center</i> . Warning! When using the video gate feature, working with the <i>Camera</i> speaker in the <i>Monitoring Center</i> is not supported.

13.1.3 Setting Up to Work with SecurOS Auto

When working with SecurOS Auto operator of the *Monitoring Center* can get access to the results of the license plate recognition, that is performed in the *Remote system*. For this, configure *Monitoring Center* as follows (see Figure 221):

Note. On the figure in the SecurOS MCC Object Tree some *Object groups* are removed.

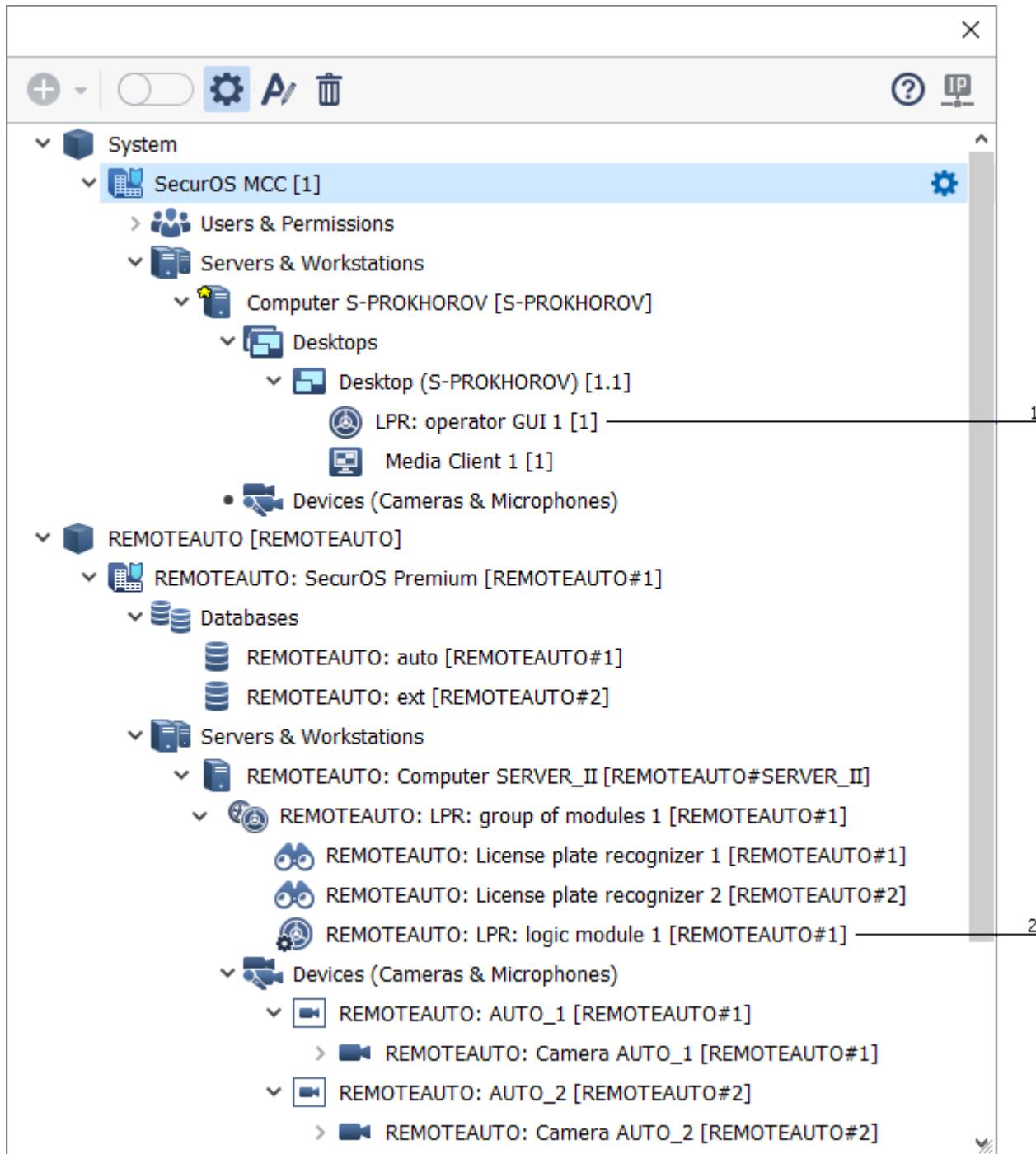


Figure 221. Monitoring Center Object Tree to work with remote SecurOS Auto

1. Create *LPR: operator GUI* object.
2. In the *LPR: operator GUI* settings select the *LPR: logic module 1* that belongs to *Remote system* (see Figure 222).

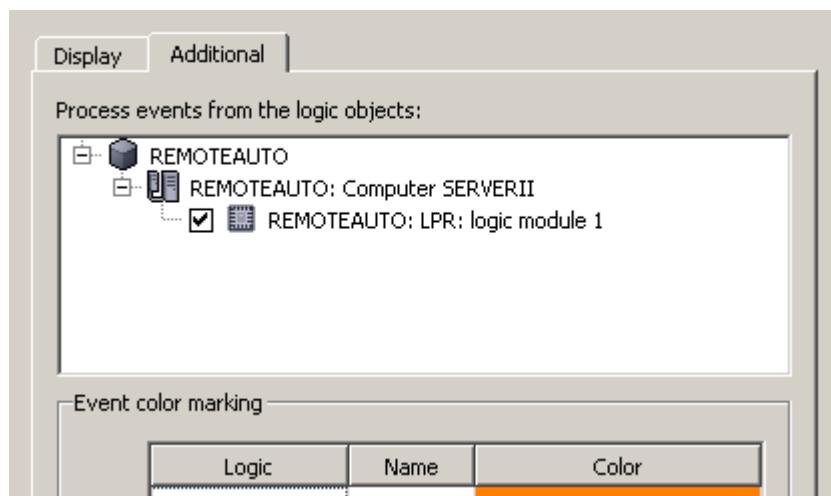


Figure 222. LPR: operator GUI object settings in SecurOS MCC

3. Check a possibility to connect to the SecurOS Auto database in the *Remote system*: network routing rules and PostgreSQL RDBMS configuration files `postgresql.conf` and `pg_hba.conf` (see [SecurOS Auto User Guide](#)).
4. In case, if local IP address of the SecurOS Auto remote database server differs from the public one, specify public IP address of the server in the *Remote system* object settings (see Figure 223). In example below this is the REMOTEAUTO: auto and REMOTEAUTO: ext databases.

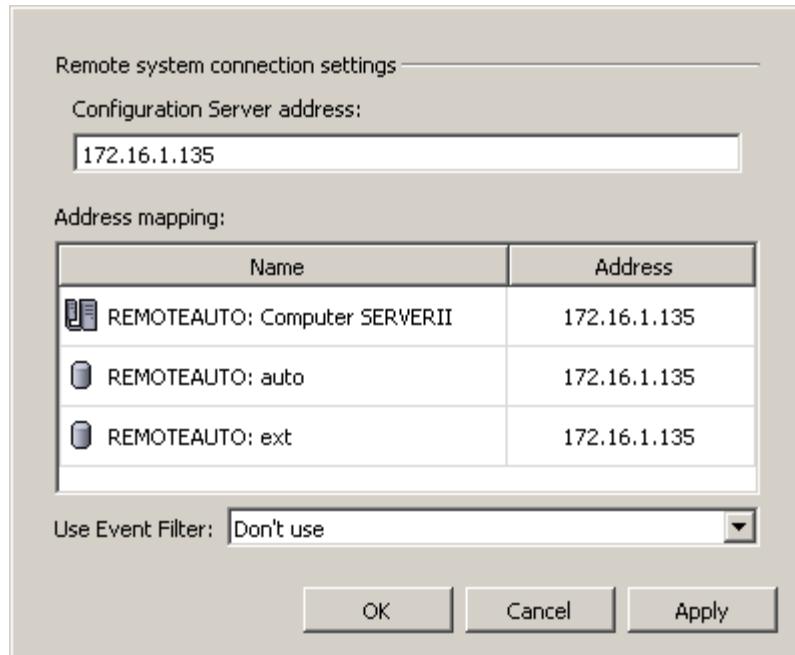


Figure 223. Remote system object settings in SecurOS MCC

13.2 VC/VR-connection

When using VC/VR-connection then the intermediary object created in the SecurOS – *Concentrator* or *Repeater* is used to work with *Remote system's Cameras*. In this case *Monitoring Center* can work both with remote and local archives.

When using VC-connection of the *Monitoring Center* then video stream from *Remote system's Camera* is available only in viewing mode. *Monitoring Center* can access archive recorded on the *Remote system's server*.

When using VR-connection of the *Monitoring Center* then video stream from *Remote system's Camera* is available both in viewing and recording mode. Archive of the *Remote system's Camera* can be recorded locally on the *Monitoring Center's server*. Access to the video archive created directly on the remote system's *Camera* is denied.

In other words, when VR-connection is used a *Monitoring Center* allows the operator to control video streams, coming from the remote server's *Cameras* in the same way as if they were set within the local SecurOS security network.

For the VR-connection the main requirement is the availability of the TCP/IP channel with large carrying capacity. When VC-connection is used a performance of the *Monitoring Center* mainly depends on the hardware of the server on which it is deployed (see [Video Server System Requirements](#)).

13.2.1 Setting Up VC/VR-connection

Setting up the SecurOS MCC for each case is described in appropriate section:

- [Setting Up VC-connection of the Monitoring Center to Work with Remote Archives](#).
- [Setting Up VR-connection of the Monitoring Center to Work with Local Archives](#).

Setting Up VC-connection of the Monitoring Center to Work with Remote Archives

To set up the VC-connection of the *Monitoring Center* to work with remote archives do the following:

1. Provide configuration of the **Monitoring center agent** object on one of the servers of the *Remote system*.
2. Configure the **Remote system** object on the *Configuration Server* of the *Monitoring Center*. Click the **Update configuration** button in the **Remote system** object settings window.

Warning! To update configuration, it is necessary that the **Server IP address** parameter was set in the each *Video Server* of the *Remote system*. Otherwise an error message is displayed.

The following objects will be created in the *Object tree* of the SecurOS MCC after configuration is downloaded (see Figure 224):

1. *Proxy-computers* - "copies" of all of the *Computer* objects existing within the remote security system. These objects are children to the **Remote system** object. Names of these objects will be in the following format: <Remote system Name>:<Computer Name>.
2. *Video Capture Devices* with **ISS Video Concentrator** device type (see [Video Capture Device](#)), related to remote *Video Servers*. **IP address** parameter of the *Video Capture Device* will possess the IP address of the appropriate remote server. All created objects are children of the *Monitoring Center's Video Server* and have names of the following format: <Remote system Name>:<Remote Computer Name>.
3. *Cameras*, which will correspond to the *Cameras* existing on the remote server. *Cameras* have names of the following format: <Remote system Name>:<Camera Name>.

Note. No Motion Detection Zones are created for the *Cameras* downloaded from the *Remote system*.

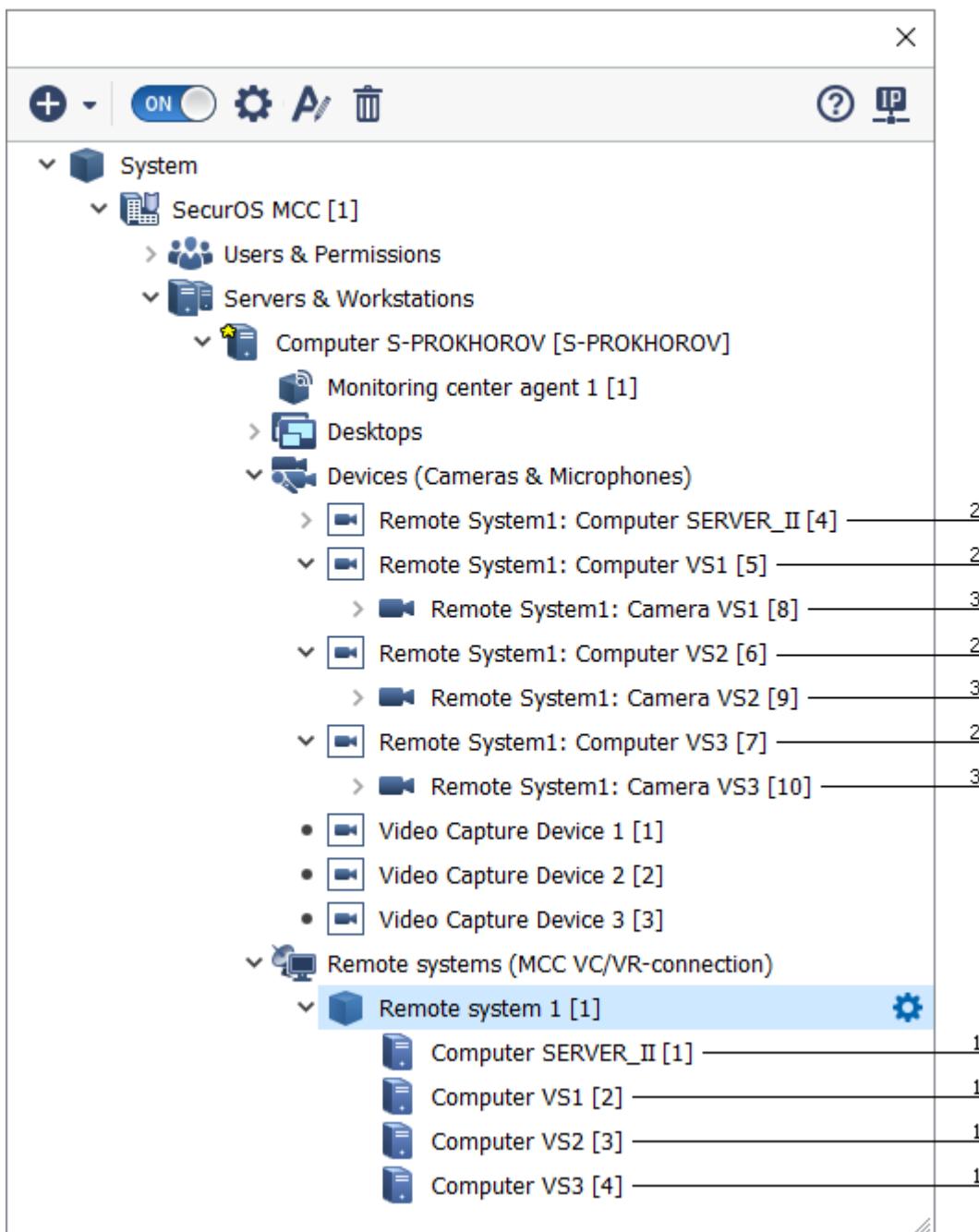


Figure 224. Configuration of the Remote system displayed in the Monitoring Center's Object Tree

Note. On the figure in the SecurOS MCC Object Tree some *Object groups* are removed.

Setting Up VR-connection of the Monitoring Center to Work with Local Archives

To set up VR-connection of the Monitoring Center to work with local archives, change the type of the created Video Capture Devices. To do this, choose the Video Repeater value in each Video Capture Device object settings (see [Video Capture Device](#)), then apply new settings.

After Video Capture Device type is changed it allows the operator to work with Cameras of the remote servers in the same way as if they were set within the local SecurOS network.

In any type of connection the operator of the *Monitoring Center* will have the opportunity to monitor the events generated by remote *Camera* or *Computer* with the help of the *Map Window*, *Media Client* and *Event Viewer*.

13.2.1.1 Remote System

This functionality is available in the *SecurOS Monitoring & Control Center* only.

This object is used to connect *Monitoring Center* to the *Remote system*.

Parent object – *Computer\Remote systems (MCC VC/VR-connection)* group.

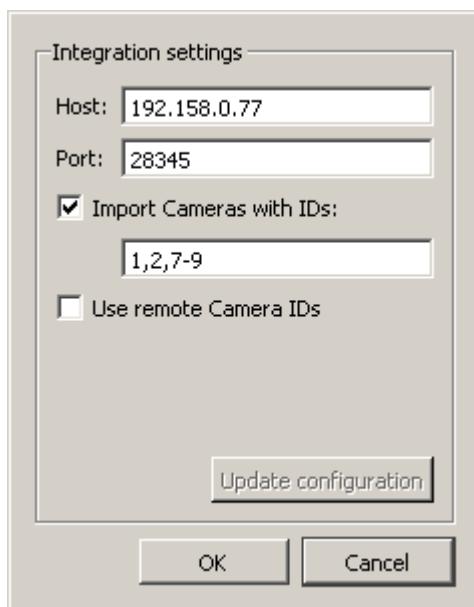


Figure 225. Remote system object settings window

Table 87. Remote system object settings

Parameter	Description
Integration settings	
Host	This parameter is used to select the <i>Computer</i> within <i>Remote system</i> , to which <i>Monitoring Center</i> will be connected. Specify the IP address. Required parameter.
Port	Port number to connect <i>Monitoring Center</i> to the <i>Remote system</i> . Mandatory parameter. Default value is 28345. The same value must be specified in the Monitoring center agent object settings on the <i>Remote system</i> side.
Import Cameras with IDs	Select this checkbox to specify a list or range of <i>Cameras</i> to import from remote system. Warning! If parameter is used with the current configuration of the remote system, imported to the <i>Monitoring Center's</i> server, then all <i>Cameras</i> , that are not listed will be removed when updating configuration.

Parameter	Description
Use remote Camera IDs	Select this checkbox to import <i>Cameras</i> and keep the IDs, assigned to the objects in remote system.
Update configuration (button)	Update configuration on the <i>Monitoring Center's</i> server in accordance with specified parameters. Warning! This button became enabled after applying the current settings.

13.2.1.2 Monitoring Center Agent

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*, *SecurOS Xpress*.

Monitoring center agent is used to connect *Monitoring Center* to the *Remote system*.

Parent object – **Computer**.

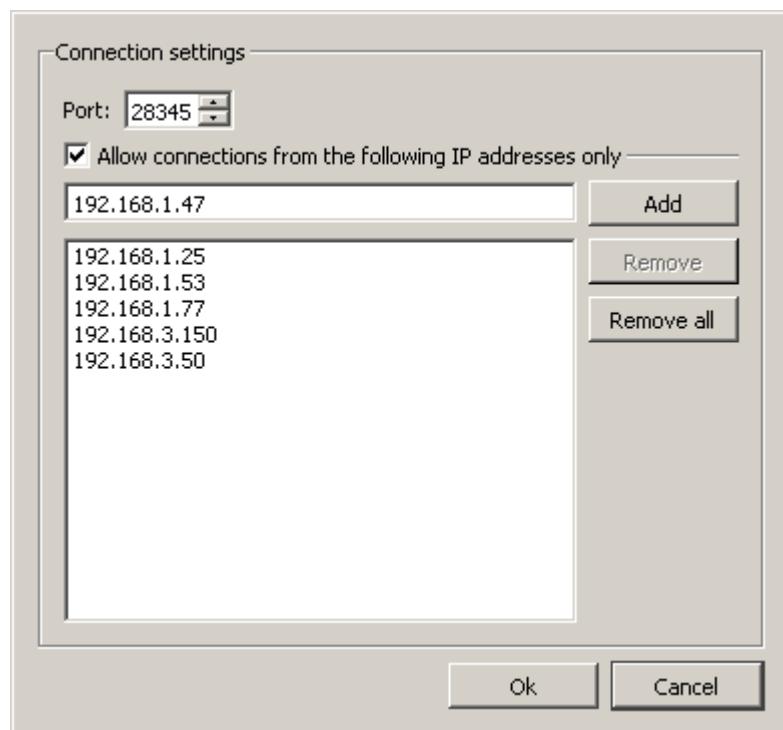


Figure 226. Monitoring center agent object settings window.

Table 88. Monitoring center agent object settings

Parameter	Description
Connection settings	
Port	Port number to connect <i>Remote system</i> to the <i>Monitoring Center</i> . Mandatory parameter. Default value is 28345. Specified value must much the number, specified on the <i>Monitoring Center</i> side (see Remote System).

Parameter	Description
Allow connections from the following IP addresses only	Check this box to allow only <i>Computers</i> with listed IP addresses to connect to security system. Optional parameter.
List of allowable IP addresses	<p>List of the IP addresses of computers, that are allowed to connect to the given SecurOS security system.</p> <hr/> <p>Note. To add IP address to the list of available addresses enter its value into the text box above the list, and then click the Add button.</p>

14 Redundancy

This sections describes methods to provide SecurOS servers redundancy. There are two such methods:

- **Failover Cluster.**
- **Redundant Servers Cluster.**

14.1 Failover Cluster

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

In order to provide additional reliability of SecurOS security network and to simplify hardware upgrade process, *Video Servers* could be integrated into failover cluster. Failover cluster represents the group of computers that is able to sustain servers malfunction with help of backup servers.

14.1.1 Cluster Structure

Cluster represents a logic structure that consists of following elements:

- **Host** – any physical computer with SecurOS *Video Server* software installed. Such computer only counts in cluster configuration that is independent from SecurOS configuration. It is not displayed in SecurOS *Object Tree*;
- **Node** – abstract entity that is represented in SecurOS *Object Tree* by *Computer* object with *Video Server* role. Unlike independent *Video Servers Node* is not bound to specific physical computer and may be run by and *Host* in cluster. For this purpose *Node* has virtual IP address that remains unchanged no matter on which *Host* it runs on.

Note. Independent *Video Server* represents physical computer with fixed IP address and SecurOS software installed but it is not a member of cluster and can be found in *Object Tree*. SecurOS configuration may include both independent *Video Servers* and *Nodes* at the same time.

Warning! When cluster is implemented SecurOS *Configuration Server* role is assigned to one of cluster *Hosts*.

Schematic view of cluster structure is provided on figure 227.

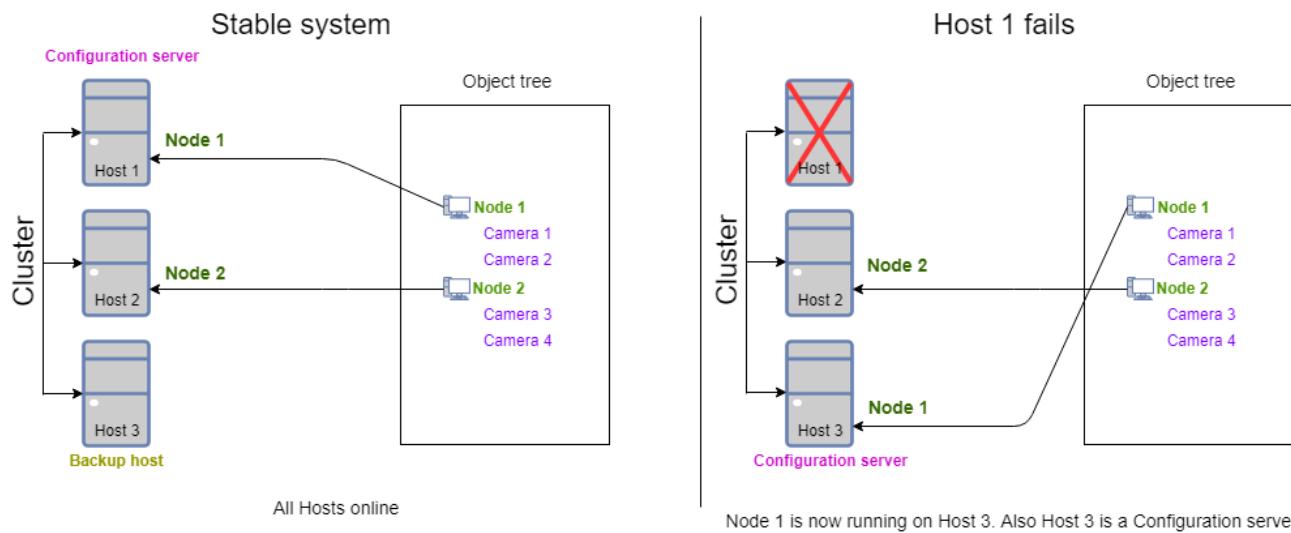


Figure 227. Cluster structure

14.1.1.1 Cluster Configuration

Information about *Hosts* and *Nodes* (their names, parameters and state) represents cluster configuration. It exists independently from SecurOS configuration and controlled by stand-alone utility (see [Configuring Cluster](#)).

14.1.1.2 Cluster Operation. Quorum

In order cluster could provide backup function, number of *Hosts* must be greater than number of *Nodes*. *Hosts* could be in two different states:

- **Operating host** – on such *Hosts* there are *Nodes* running. Running the *Node* means starting all processes that are required for SecurOS to operate. One *Host* can run only one *Node* at the same time.
- **Backup host** – such *Hosts* are in standby state. When operating *Host* fails the *Node* that was running on it starts running on a backup *Host*. Backup *Host* is being selected automatically.

If the failed *Host* restores at the moment when all *Nodes* are already allocated, it switches itself to backup state. *Configuration Server* role can also be automatically assigned to other *Host* if needed. Such behavior can be changed with help of service mode (see [Service mode](#)).

Configuration Server role can be assigned both the active and backup hosts.

Cluster keeps working while its *Hosts* (both operating and backup ones) maintain the quorum state. Quorum state exists while more than the half of all *Hosts* are online.

Quorum loss

The loss of the quorum within the cluster causes the following consequences:

- All *Hosts*, including those that have remained operational, will not be able to function. Whole cluster will stop operating and will be waiting for quorum state restoration (see [Resolving Common Issues](#)). This situation will not affect those *Video Servers* in SecurOS configuration that are not members of the cluster.

Note. Such behavior is typical for most cluster structures and is not a feature of SecurOS.

- Most of the cluster configuration commands can not be executed.

Example

In following configurations the quorum state loss will happen if:

- Cluster of 2 Hosts. Quorum will be lost, if one *Host* will failed (see [Redundant Servers Cluster](#) section that describes how to create effective cluster consisting of two *Hosts*).
- Cluster of 3 Hosts. Quorum state will be lost if 2 *Hosts* fail.
- Cluster of 4 Hosts. Quorum state will be lost if 2 *Hosts* fail.
- Cluster of 5 Hosts. Quorum state will be lost if 3 *Hosts* fail.

Behavior of the system in states of quorum loss and restoration is provided on figure 228.

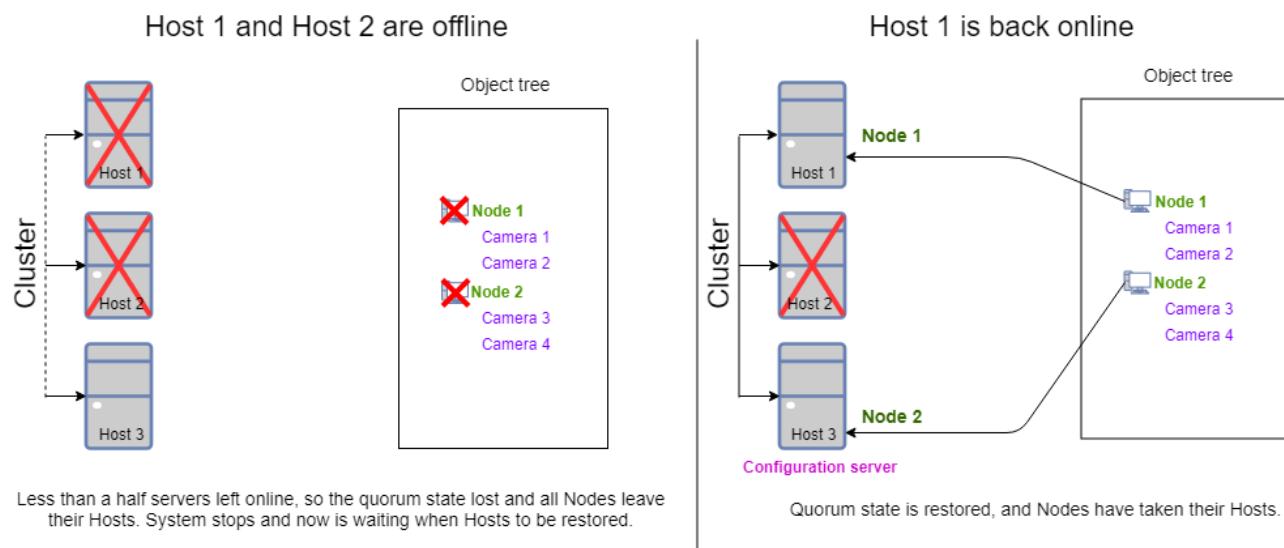


Fig. 228. Quorum loss and restoration for configuration of three Hosts

14.1.1.3 Recommendations

It is recommended to use isolated network interface for server communication (see [Changing Network Interface for Virtual IP Addresses](#)).

It is recommended to use centralized data storage. To store video data one may use shared folders (access by CIFS (SMB) protocol) or iSCSI drive. For other data one may use iSCSI storage (see [iSCSI Drive](#)).

Warning! To provide interaction of the *Host* within cluster it is necessary to ensure the availability of the network ports (see [Appendix 4. TCP/IP Ports Used by SecurOS](#)).

14.1.2 Configuring Cluster

For working with cluster it is recommended to use the [SecurOS Server Manager](#) utility. It has a user-friendly graphical interface that allows to perform all necessary operations with the cluster and monitor its work in real time.

To configure and control the cluster alternatively one can use `clustercli.exe` console utility, that is located in SecurOS root directory.

Warning! Executing commands with utility requires Windows administrator rights.

Operations of creating and configuring cluster from the command prompt are described in following sections:

- [Creating Cluster;](#)
 - [Creating Cluster within Existing SecurOS Configuration;](#)
 - [Creating Cluster and SecurOS Configuration From the Scratch;](#)
- [Getting Current Cluster Configuration;](#)
- [Creating Security Zone;](#)
- [Adding Host;](#)
- [Removing Host;](#)
- [Switching to Video Server Mode;](#)
- [Adding Node;](#)
- [Removing Node;](#)
- [Getting Node List;](#)
- [Setting Preferred Host for the Node;](#)
- [Moving Node to the Host Manually;](#)
- [Recreating Cluster;](#)
- [Restoring SecurOS Configuration from File;](#)
- [Setting Configuration Server;](#)
- [Converting Independent Video Server to Cluster Node;](#)
- [Service Mode;](#)
- [Changing Network Interface for Virtual IP Addresses.](#)

14.1.2.1 Creating Cluster

Warning! Before starting create cluster it is recommended to save current SecurOS configuration (see [System](#)).

To create a cluster execute the following command on one of the *Hosts*:

```
Clustercli.exe create <heartbeat_nic> <virtual_ip_nic> <config_server_virt_ip>
```

where:

- `heartbeat_nic` - given computer's IP address, at which it will be available for data exchange with other *Hosts*;
- `virtual_ip_nic` - IP address of network interface on this computer, which virtual IP addresses will be assigned to;

Note. If computer has only one network adapter, you must duplicate the value of the `heartbeat_nic` parameter. This address can be changed further with the help of separate command (see [Changing Network Interface for Virtual IP Addresses](#)).

- `config_server_virt_ip` - virtual IP address, which the *Configuration Server* will be available at. This address must be unique in local area network and will be assigned to the network interface on a *Host* that will play role of *Configuration Server*. In case of such *Host* failure this IP address may migrate to other *Hosts*.

After successful command execution the cluster will be ready to start operation. It will consist from one *Host*, that is also a *Configuration Server*.

Warning! If the command was executed not on current SecurOS *Configuration Server*, then at this moment there are two competing configurations. The elimination of this problem is described in details in the [Creating Cluster in Existing SecurOS Configuration. Example](#).

Depending on whether there is an existed SecurOS configuration on computers being added to cluster, next steps differ. See details in following section:

- [Creating Cluster in Existing SecurOS Configuration](#);
- [Creating Cluster and SecurOS Configuration From the Scratch](#).

14.1.2.1.1 Creating Cluster in Existing SecurOS Configuration

Execute `create` command on a computer that is already a part of SecurOS security network with existed configuration. After that to start configuring system do the following:

1. If some *Video Servers*, including previous *Configuration Server*, must stay independent (namely they should not be added to cluster), configure them to work with new *Configuration Server*. To do this use *Server Role Manager* utility (see [ISS Server Role Manager utility](#)) and specify IP address of the new *Configuration Server* - `config_server_virt_ip` parameter, that was used in cluster creation command.
2. Create at least one *Node*, which the *Operator Workstation* will be able to connect to (see [Adding Node](#)). If it is required, one can convert one of *Video Servers* existed in current configuration to a *Node* (see [Converting independent Video Server to cluster Node](#)).

14.1.2.1.2 Creating Cluster and SecurOS Configuration From the Scratch

If it is required to create cluster and SecurOS network with new configuration simultaneously, execute `create` command at any computer with SecurOS software installed. Now, to start configuring system, do the following:

1. Create *Security Zone* (see [Creating Security Zone](#)).
2. Create at least one *Node*, which the *Operator Workstation* will be able to connect to (see [Adding Node](#)).

Detailed process of how to create cluster when there is no configuration yet is described in section [Creating and setting up cluster example](#).

14.1.2.2 Getting Current Cluster Configuration

To check current cluster configuration execute the following command on any *Host*:

```
Clustercli.exe state
```

Console will display the following information:

1. *Configuration Server* virtual IP address.

2. List of *Nodes* with following description:

- SecurOS configuration revision for the moment of *Node* creation.

Note. Configuration revision is a number that matches the count of changes made in this configuration.

- Virtual IP address of the *Node*.

- Preferred *Host* for that *Node* (if set).

3. Name of the *Host*, that serve as *Configuration Server*.

4. List of couples of *Nodes* and *Hosts*, which these *Nodes* running on.

5. List of *Hosts* with their IP addresses and current configuration revision.

6. List of the servers connected to the cluster (see **Redundant Servers Cluster**) indicating the current revision of the configuration.

7. List of the local drives added on this *Host* (see **Storing Video Archive on the Host's Local Drives**).

Warning! In case of quorum loss state (see **Cluster Operation. Quorum**) it is unable to check cluster state.

Command execution result in provided on figure 229:

```
C:\Program Files (x86)\ISS\SecurOS>clustercli.exe state
Settings: {
    "csIp": "172.16.7.80",
    "nodes": {
        "NODE1": {
            "crRev": "579",
            "ip": "172.16.7.61",
            "prefHost": "V-FIH7-2"
        }
    }
}

CS host: V-FIH
State: {
    "nodes": {
        "NODE1": "V-FIH7-2"
    }
}
Hosts:
    V-FIH(http://172.16.1.93:2380) csRevision=632
Supplementary hosts online:
    V-FIH7-2 csRevision=632, nocs

C:\Program Files (x86)\ISS\SecurOS>
```

Figure 229. Cluster state

14.1.2.3 Creating Security Zone

If cluster is being configured in system without any SecurOS configuration, one must create *Security Zone* first. To do this execute the following command on any host:

```
Clustercli.exe node createzone <zone_id>
```

where:

- `zone_id` - *Security Zone ID*.

The *System* object will be created if there was none.

14.1.2.4 Adding Host

To set up computer as cluster *Host*, execute the following command on it:

```
Clustercli.exe join <heartbeat_nic> <virtual_ip_nic> <other_host_ip>
```

where:

- `heartbeat_nic` - given computer's IP address, at which it will be available for data exchange with other *Hosts*;
- `virtual_ip_nic` - IP address of network interface on this computer, which virtual IP addresses will be assigned to;

Note. If computer has only one network adapter, you must duplicate the value of the `heartbeat_nic` parameter. This address can be changed further with the help of separate command (see [Changing Network Interface for Virtual IP Addresses](#)).

- `other_host_ip` - IP address of one of cluster *Hosts*.

Warning! Entering wrong or not available IP address as `this_real_ip` parameter may cause quorum loss (see [Resolving Common Issues](#)).

After executing command SecurOS service will restart and after that it will be working in cluster *Host* mode.

Warning! If the computer that is being added to the cluster stores any SecurOS configuration it will be overwritten.

14.1.2.5 Removing Host

To remove *Host* from cluster configuration execute the following command on any *Host*:

```
Clustercli.exe remove <host_to_remove_ip> <other_host_ip>
```

where:

- `host_to_remove_ip` - IP address of the *Host*, that must be removed from cluster;
- `other_host_ip` - IP address of one of cluster *Hosts*.

Note. To return computer to regular mode it is not enough only to remove it from cluster. It must be also switched to *Video Server* mode (see [Switching to Video Server mode](#)).

14.1.2.6 Switching to Video Server Mode

To completely switch computer to independent *Video Server* mode, one must execute the following command on this computer:

```
Clustercli.exe leave [-f]
```

where:

- [-f] – optional parameter for forced execution.

This command works in two steps:

1. It sends command to remove *Host* from cluster (see [Removing Host](#)).
2. Switches computer to independent *Video Server* mode.

In case if first step can not be executed, for example, due to quorum loss (see [Cluster Operation. Quorum](#)), the second step will not be executed. If it is needed to switch computer to *Video Server* mode anyway, skip the first step. To do this use -f parameter, that allows to perform forced command execution.

14.1.2.7 Adding Node

To add a *Node* to cluster configuration execute the following command on any *Host*:

```
Clustercli.exe node create <node_name> <node_virt_ip> <zone_id>
```

where:

- node_name – name and ID of the *Node* to be created;
- node_virt_ip – virtual IP address, which the *Node* will be available at. This address must be vacant in local area network and unique;
- zone_id – ID of *Security Zone*, which is parent to the *Node*.

Note. Unlike independent *Video Servers*, ID of a *Node* does not have to match computer's domain name, that it will be running on.

A new *Nodes* also can be added via SecurOS *Object Tree*. To do this perform the following steps:

1. Connect to the working *Node* using client application (see [Connecting Operator Workstations to the Cluster Servers](#)).
2. In the configuration create *Computer* object that has *Video Server* role.
3. In settings of this *Computer* object tick the **Enable failover of the Video server and add to the cluster** checkbox.
4. Enter virtual IP address of the *Node* into the **IP address** field.

Virtual IP address is now assigned to the *Node* and it will be available at this address despite of what *Host* it is running on.

14.1.2.8 Removing Node

To remove *Host* from cluster configuration execute the following command on any *Host*:

```
Clustercli.exe node remove <node_name>
```

where:

- *node_name* – ID of the *Node* to be deleted.

Warning! Removing the *Node* results into deleting all *Cameras* and other child objects as well.

14.1.2.9 Getting Node List

To get list of all *Nodes* in the configuration execute the following command:

```
Clustercli.exe node list
```

List of all *Nodes* with ID and virtual IP address for each will be displayed.

Command execution result in provided on figure 230:

```
C:\Program Files (x86)\ISS\SecurOS>clustercli node list
Security Zone: SecurOS Enterprise[1]
    Node: NODE1 172.16.7.101
    Node: NODE2 172.16.7.102
```

Figure 230. Node List

14.1.2.10 Setting Preferred Host for the Node

If it required to make specific *Node* always run on a specific *Host* (due to its higher performance, for example), execute the following command:

```
Clustercli.exe node set <node_name> pref_host=<host_name>
```

where:

- *node_name* – name of the *Node*, which the preferred *Host* is being set for;
- *host_name* – name of the *Host*, that will become preferred for specified *Node*.

Note. To cancel *Host*'s priority for the *Node*, execute command with empty *pref_host* parameter value. For example, Clustercli.exe node set Node_1 pref_host=.

Nodes that have preferred *Hosts* fall under the following rules:

1. *Node* will be trying to take its preferred *Host* at the earliest opportunity.
2. If any *Host* is set to be preferred for several *Nodes* at one moment, the one that will take it will be selected automatically. Thus it can not be displaced from this *Host* automatically.
3. When setting up preferred *Host* for a *Node* it will immediately replace the *Node* currently running on the *Host* (if current *Node* is not running on preferred *Host*). The displaced *Node* will take first vacant *Host* if there are any.

14.1.2.11 Moving Node to the Host Manually

To manually move *Node* to required *Host* execute the following command:

```
Clustercli.exe node set <node_name> pref_host=<host_name>
```

where:

- *node_name* – ID of the *Node* to be moved;
- *host_name* – name of the *Host* that will run specified *Node*;

Process of manual moving the *Node* to a *Host* falls under the following rules:

1. If there is another *Node* running on specified *Host* already, it will be displaced.
2. If the displaced *Node* was the one, for which that *Host* is set to be preferred, further behavior will be determined by rules for *Nodes* with preferences.

Note. It is not recommended to use manual *Node* transferring to configure cluster. Proper setup of *Nodes* preferences allow to achieve better results (see [Setting Preferred Host for the Node](#)).

14.1.2.12 Recreating Cluster

In case when one needs to reassemble the cluster without losing its configuration (see [Cluster Configuration](#)) except for list of *Hosts*, execute the following command on any *Host*:

```
Clustercli.exe recreate <heartbeat_nic> <virtual_ip_nic>
<config_server_virt_ip>
```

where:

- *heartbeat_nic* – given computer's IP address, at which it will be available for data exchange with other *Hosts*;
- *virtual_ip_nic* – IP address of network interface on this computer, which virtual IP addresses will be assigned to;

Note. If computer has only one network adapter, you must duplicate the value of the *heartbeat_nic* parameter. This address can be changed further with the help of separate command (see [Changing Network Interface for Virtual IP Addresses](#)).

- *config_server_virt_ip* – virtual IP address, which the *Configuration Server* will be available at. This address must be unique in local area network and will be assigned to the network interface on a *Host* that will play role of *Configuration Server*. In case of such *Host* failure this IP address may migrate to other *Hosts*.

After executing this command cluster will contain only one *Host*. Other hosts must be added to cluster again (see [Adding Host](#)).

Note. Recreating cluster is a way to solve the quorum loss problem (see [Resolving Common Issues](#)).

14.1.2.13 Restoring SecurOS Configuration from File

If SecurOS configuration was initially saved into a file, it can be used to restore one. To do this execute the following command on any *Host*:

```
Clustercli.exe xmlrestore <path_to_file>
```

where:

- *path_to_file* – absolute or relative path to file with saved configuration.

Note. When executing this command cluster *Hosts* list is not restored. If necessary, hosts must be added to the cluster manually (see [Adding Host](#)).

Before executing command, current SecurOS configuration is being saved to `ISS\Sys_config\cluster_backup.xml`, path to which is defined by `%ProgramData%` variable.

Warning!

1. Version of the backup copy should comply with version of the currently installed SecurOS, otherwise it is not applicable.
2. Configuration backup file is stored on the *Host* that was in *Configuration Server* role at the moment of command execution.
3. The current password of the superuser (see [SecurOS Users](#)) will not change after restoring the configuration.

14.1.2.14 Setting Configuration Server

If it is required to set *Configuration Server* role to a specific *Host* in cluster, execute the following command on any *Host*:

```
Clustercli.exe set cs=<new_cs_host>
```

where:

- *new_cs_host* – name of the *Host* that will be set as new *Configuration Server*.

Notes:

1. In case when *Host* set to be a *Configuration Server* fails, new *Configuration Server* will be assigned automatically. Such behavior can be changed with help of service mode (see [Service Mode](#)).
2. *Configuration Server* role can be assigned only to cluster member.

14.1.2.15 Converting Independent Video Server to Cluster Node

If cluster is being created based on existed SecurOS configuration, one must convert regular *Video Servers* into *Nodes* after. To do this execute the following command on any *Host*:

```
Clustercli.exe node update <videoserver_id> <node_virt_ip>
```

where:

- *videoserver_id* – ID of the *Video Server* in SecurOS *Object tree* that required to be converted into a *Node*;

- `node_virt_ip` - virtual IP address, which the *Node* will be available at.

Note. Same command may be used for changing virtual IP address of existed *Node*.

14.1.2.16 Service mode

Service mode allows to perform hardware and software upgrade without losing cluster configuration (see [Cluster configuration](#)). There are types of service mode:

- Fixed *Configuration Server* – in this variation *Configuration Server* role can not be assigned to other *Host* automatically.
- Full fixation – in this variation not only the *Configuration Server* role but also *Nodes* are not changing *Hosts* automatically.

To enter service mode execute the following command on any *Host*:

```
Clustercli.exe set service_mode=<service_mode_name>
```

where:

- `service_mode_name` – type of service mode:
 - `fixed_cs` – fixed *Configuration Server*;
 - `fixed_all` – full fixation.

To exit service mode execute the following command on any *Host*:

```
Clustercli.exe set service_mode=
```

This command removes current service mode value so *Nodes* and *Configuration Server* role will start to transfer automatically again.

14.1.2.17 Changing Network Interface for Virtual IP Addresses

Operator Workstations connect to security network via virtual IP addresses of *Nodes*. Network load depends on *Host*'s network interface, which virtual IP addresses are assigned to. It is recommended to assign virtual IP addresses to a network interface that differs from the one that is used by *Hosts* to communicate with each other.

To change network interface, to which you want to assign virtual IP addresses, execute the following command:

```
Clustercli.exe set virtual_ip_nic=<ip_address>
```

where:

- `ip_address` – IP address of network interface on this computer, which virtual IP addresses will be assigned to.

14.1.3 Connecting Operator Workstations to the Cluster Servers

Operator Workstations can connect to the SecurOS servers, that work within cluster. To connect to such server specify **virtual IP address** of one of the *Nodes* in authorization window. If *Host* fails, the client application will automatically reconnect to the same *Node* after it is launched on the new *Host*.

Note. If there is no *Node* in cluster yet, use IP address of one of the *Hosts* to configure SecurOS.

Limiting connection of client applications running on cluster Hosts

Security Zone object settings allows to limit connections of the client applications to the SecurOS servers (see [Connection Restrictions Tab](#)). If cluster *Host* is used as *Operator Workstation* at the same time, not only IP address of this computer must be added to the white list of the IP addresses, but also virtual IP addresses of all cluster *Nodes* and virtual IP address of the *Configuration Server*.

14.1.4 Storing Data in Cluster

While working with cluster, special attention should be given to video archive and databases storage organization.

Following types of storage can be used for storing video archive:

- **Shared folder (CIFS)** – the most **safe** type of centralized storage.
- **iSCSI drive** – the most **fast** type of centralized storage (see [iSCSI Drive](#)).

Warning!

1. Versions of Windows OS installed on all *Hosts* that use iSCSI drives must match.
2. For proper iSCSI drive connection on Windows 10, update your operation system to build 1709 or above.
3. Each iSCSI drive must contain one partition formatted in NTFS.
4. Simultaneous recording on iSCSI drive may lead to data corruption. To provide additional data safety it is recommended to use storages with support of iSCSI target connection exclusivity control.

Besides storing video archive iSCSI drives may be used for storing databases. For example, databases of *Event viewer*, recognition modules, etc (see [Movable PostgreSQL](#)).

- **Local drives** allow to store video archive directly on the cluster's *Hosts*. Records stored on all *Hosts* are available to operator as transparent archive. In case of *Host* failure, the corresponding part of the archive will be temporarily unavailable.

Note. Local drives for archive recording can be set on the *Host* where the *Node* works (see [Advanced Cluster Host Settings](#)). In this case the archive will be first written on these drives, even if there are other directories for archive recording specified in the *Node* own settings.

This type of storage is recommended to use in [Redundant Servers Cluster](#) due to its restrictions. Details of the configuration procedure are described in the [Storing Video Archive on the Host's Local Drives](#).

14.1.4.1 iSCSI Drive

Warning! Before using iSCSI drive make sure that all *Hosts* in the cluster are running Windows service named **Microsoft iSCSI Initiator Service** and type of run is set to **Automatically**.

This object is a mediator between SecurOS and Windows iSCSI initiator, that provides credentials to establish connection. To add iSCSI drive to SecurOS configuration create *iSCSI drive* object, child of the *Computer* object (*Node*).

Note. To record video archive on the *Node* one can use only those *iSCSI drives*, that are child to this *Node*.

Parent object – **Computer**.

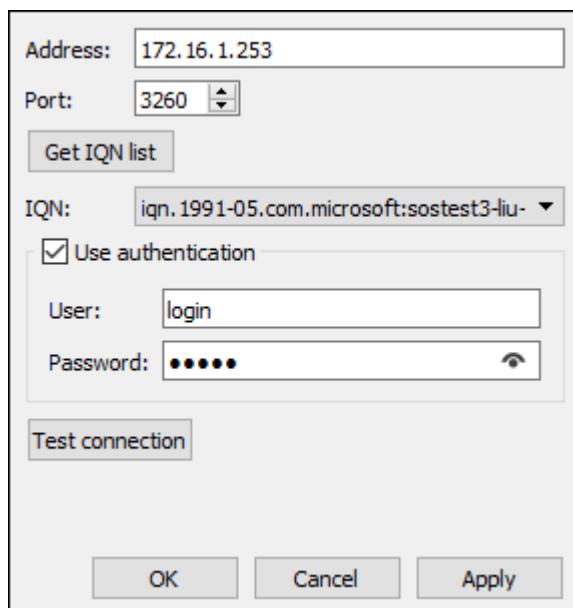


Figure 231. iSCSI drive object settings window

Table 89. iSCSI drive object settings

Parameter	Description
Address	Enter IP address in IPv4 format or domain name of the server where disk is located.
Port	Enter network port that is used to establish connection. Default value: 3260.
Get IQN list (button)	Press the button to get list of IQN available on the portal.
IQN	List of IQNs, to which the connection can be established. Select desired value.
Use authentication	Select this checkbox if there is authentication required on the portal.
User and Password	Enter credentials for authentication.

Parameter	Description
Test connection (button)	Press the button to make sure that connection with selected IQN works properly. In case if all settings are correct, the Connection established message will appear next to the button. Otherwise the Connection refused message will appear.

14.1.4.2 Using iSCSI Drive for Storing Video Archive

Warning! Using **Save space** mode when archive recording can negatively affect the data safety on the iSCSI storage. It is recommended to use **Optimal performance** mode (see [Select archive recording mode](#)).

To record archive on *iSCSI drive*, one must set it up first (see [iSCSI Drive](#)). After that it can be selected in settings of *Computer* object. To perform that do the following:

1. Open *Computer* object settings.
2. Press the **Add directory** button at the **Archive** section.
3. Select **iSCSI drive** option and find required *iSCSI drive* in the drop-down list.
4. Click the **Add** button.

Note. Setting up *Archiver* for storing long-term archive on *iSCSI drive* can be performed in the same way (see [Archiver](#)).

14.1.4.3 Movable PostgreSQL

In order to increase fault tolerance of databases, they can be located on *iSCSI drives*. It will make databases available at fixed IP address in case of *Host* failure.

Parent object – [iSCSI drive](#).

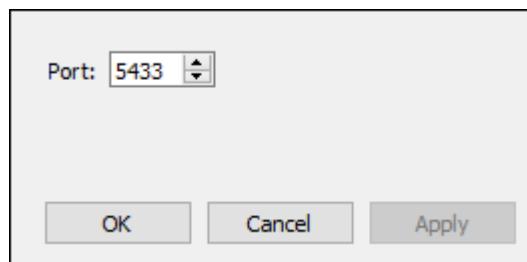


Figure 232. Movable PostgreSQL object settings window

Table 90. Movable PostgreSQL object settings

Parameter	Description
Port	Enter network port at which movable DBMS will be available. Default value: 5433.

To create such fail safe database, do the following:

1. Create *Movable PostgreSQL* object child to *iSCSI drive* object.
2. At object settings enter the port at which the database will be available.

One must configure access from outer IP addresses on selected PostgreSQL server.

To do this edit `postgresql.conf` and `pg_hba.conf` configuration files. In `postgresql.conf` there must be `listen_addresses = '*' option`, and `pg_hba.conf` must include permissions for *Operator Workstations* or *Video Servers*.

Generally the line must look like this:

```
host all all 0.0.0.0/0 md5
```

Notes:

1. `postgresql.conf` and `pg_hba.conf` files can be found in `%ProgramData%/ISS/iscsi_drives/[iscsi_drive_id]/pg_data` directory.
 2. To check remote DB accessibility at *Operator Workstation* one can use the **Test connection** button in the *Database* object settings window or pgAdmin utility.
-

3. Connect to the movable database using PGAdmin utility. For connection specify virtual IP address of the *Node*, which are parent for the *Movable PostgreSQL*.
4. Use PGAdmin to create new database.
5. Markup created database with the help of **Database Update Utility**.
6. Create *Database* object child to *Security Zone* object (see **Database**).
7. Configure the *Database* object. To do this enter *iSCSI drive*'s parent *Node* virtual IP address as Host, and *Movable PostgreSQL* port value as Port.

Now this *Database* can be selected in settings of the object it is intended for.

14.1.4.4 Storing Video Archive on the Host's Local Drives

Local hard drives of the cluster's *Hosts* can be used to store video archive. Each *Host* is configured separately.

Warning! It is strongly recommended to configure the cluster in that way, so that the preferred *Host* is selected for each *Node* (see **Setting Preferred Host for the Node**).

To configure *Host*'s local drive to store video archive use the `clustercli.exe` utility (see **Configuring Cluster**). This utility provides the following commands to work with the drives:

- **Adding Drive;**
- **Removing Drive;**
- **Getting Drive List.**

Adding Drive

Note. Writing to the drives that have been added in such way is performed with higher priority than to the iSCSI drive/network folder specified in the *Computer* object settings.

To add a *Host*'s drive as a video archive storage execute the following command on the appropriate *Host*:

```
Clustercli.exe drive add <drive_letter> <min_free_space> <read_write>
```

where:

- `drive_letter` - drive letter. The following formats are allowed: C:, D:\, E:/.
- `min_free_space` - minimum allowable amount of free disk space in percent. When the amount of free space is reduced to the specified value, the recording in the "ring" mode will start. Possible values: [1; 20].
- `read_write` - drive access level. Possible values:
 - `rw` - read and write;
 - `r` - read only. In the last case one can view an archive existed on this drive, but a new files will not be recorded.

Note. If the drive marked with specified letter has been already added its settings will be re-written.

As a result of the command execution will be a message about successful or failure drive adding.

Removing Drive

To remove previously added *Host*'s drive execute the following command on the appropriate *Host*:

```
Clustercli.exe drive remove <drive_letter>
```

where:

- `drive_letter` - drive letter. The following formats are allowed: C:, D:\, E:/.

As a result of the command execution will be a message about successful or failure drive removing.

Getting Drive List

To get list of all drives added on this *Host* execute on it the following command:

```
Clustercli.exe drive list
```

As a result of the command execution will be a list of drives and their settings.

14.1.5 Cluster Creating and Setting Up Examples

This section describes main operations for cluster creating and configuring:

- [Creating Cluster and SecurOS Configuration From the Scratch. Example.](#)
- [Creating Cluster in Existing SecurOS Configuration. Example.](#)

14.1.5.1 Creating Cluster and SecurOS Configuration From the Scratch. Example

This section describes steps required to create new SecurOS configuration based on cluster.

14.1.5.1.1 Task

The task is to create a new SecurOS configuration and cluster. Cluster would consist of three *Hosts* and one *Operator Workstation* for monitoring needs (see [Cluster structure](#)). Two *Hosts* will run *Nodes* and one *Host* would serve as backup one.

14.1.5.1.2 Requirements

To create cluster described above one will need 3 computers with SecurOS installed with *Video Server* role, and 1 computer to be an *Operator Workstation*.

As recommended (see [Recommendations](#)), computers that considered to be *Hosts* must have two different network interfaces for *Hosts* communication (connection name, for example, NIC_CLUSTER) and for *Operator Workstation* connection (connection name, for example, NIC_VIDEO). Connection names may differ from specified ones.

For computer that is selected to be an *Operator Workstation*, one network interface will be enough.

Note. All commands described below must be executed from the command line with Windows administrator rights.

14.1.5.1.3 Computers Parameters

In this example computers have following parameters:

- **Computer 1**

- Domain name: Host1.
- Network interface NIC_CLUSTER: 192.168.0.101.
- Network interface NIC_VIDEO: 172.16.1.101.

- **Computer 2**

- Domain name: Host2.
- Network interface NIC_CLUSTER: 192.168.0.102.
- Network interface NIC_VIDEO: 172.16.1.102.

- **Computer 3**

- Domain name: Host3.
- Network interface NIC_CLUSTER: 192.168.0.103.
- Network interface NIC_VIDEO: 172.16.1.103.

- **Computer 4**

- Domain name: Operator.
- Network interface NIC_VIDEO: 172.16.1.104.

14.1.5.1.4 Steps

Cluster creation procedure consists of the following steps:

1. Creating cluster, *Security Zone* and *Nodes*.
2. Adding the second *Host*.
3. Adding the third *Host*.
4. Connecting *Operator Workstation* and further configuration of the SecurOS.

To create cluster do the following with the help of `clustercli.exe` utility (see [Configuring Cluster](#)):

1. Switch to **Computer 1** (first *Host*).

1.1. Create Cluster by executing following command

```
clustercli.exe create 192.168.0.101 172.16.1.101 172.16.20.1
```

Cluster will be created. There will be one *Host* in cluster configuration, that also will be *Configuration Server* which virtual IP will be 172.16.20.1.

Virtual IP addresses of this *Host* will be assigned to the `NIC_VIDEO` (172.16.1.101) network interface. *Operator Workstations* will receive video through that interface.

1.2. Create Security Zone by executing command

```
clustercli.exe node createzone 1
```

This *Security Zone* will have ID **1**.

1.3. Create Node by executing following command

```
clustercli.exe node create node1 172.16.20.101 1
```

It will start running on the recently created *Host*. *Node* will look like *Computer* object with *Video Server* role and ID **node1**, child to *Security Zone* with ID **1**. Now **Computer 1** is a *Configuration Server* with virtual IP address 172.16.20.1, and it has *Node* with virtual IP address 172.16.20.101 running on it.

1.4. Create second Node by executing following command

```
clustercli.exe node create node2 172.16.20.102 1
```

Second *Node* is not running right now and is waiting for new *Hosts*.

2. Switch to **Computer 2** (second *Host*).

2.1. Add Computer 2 to the cluster by executing following command

```
clustercli.exe join 192.168.0.102 172.16.1.102 192.168.0.101
```

Now *Hosts* are connected through `NIC_CLUSTER` network interface. As soon as this *Host* added to the cluster the *Node* with ID **node2** will start running on it.

Virtual IP addresses of this *Host* will be assigned to the `NIC_VIDEO` (172.16.1.102) network interface.

3. Switch to **Computer 3** (third, backup *Host*).

3.1. Add Computer 3 to the cluster by executing following command

```
clustercli.exe join 192.168.0.103 172.16.1.103 192.168.0.101
```

Last *Host* has joined the cluster. It will serve as backup *Host*.

Virtual IP addresses of this *Host* will be assigned to the `NIC_VIDEO` (172.16.1.103) network interface.

3.2. Check cluster state by executing following command on any of cluster members

```
clustercli.exe state
```

Cluster state will show that there are three *Hosts* with two running *Nodes*.

4. Switch to **Computer 4 (Operator Workstation)**.

- 4.1. Start operator interface and specify 172.16.20.101 (one of *Nodes* virtual IP address) as IP address to connect.
- 4.2. Log on as superuser (see [SecurOS Users](#)).

14.1.5.2 Creating Cluster in Existing SecurOS Configuration. Example

This section describes steps required to reconfigure SecurOS so that independent Video Servers may work in cluster.

14.1.5.2.1 Task

Transform an existed SecurOS configuration to work in cluster. Current configurations contains two *Video Servers* and one *Operator Workstation* that is used for monitoring. It is planned to use an additional computer that will be a backup server.

14.1.5.2.2 Requirements

In accordance to recommendations (see [Recommendations](#)), each of *Video Servers* and proposed backup server must be provided with two network interfaces. One of them will be used to provide interaction with cluster *Hosts* (connection name, for example, NIC_CLUSTER), the second one will be used to connect *Operator Workstations* (connection name, for example, NIC_VIDEO). Connection names may differ from specified ones.

For computer that is selected to be an *Operator Workstation*, one network interface will be enough.

Note. All commands described below must be executed from the command line with Windows administrator rights.

14.1.5.2.3 Computers Parameters

Security Zone which ID is 1 already exist within SecurOS configuration.

Computers that belong to existed configuration have the following parameters:

- **Video Server 1**

- Domain name: Server1.
- Role: Configuration Server.
- Network interface NIC_CLUSTER: 192.168.0.101.
- Network interface NIC_VIDEO: 172.16.1.101.

- **Video Server 2**

- Domain name: Server2.
- Role: Peripheral Server.
- Network interface NIC_CLUSTER: 192.168.0.102.
- Network interface NIC_VIDEO: 172.16.1.102.

- **Operator Workstation**

- Domain name: Operator.
- Network interface NIC_VIDEO: 172.16.1.104.

Computer, that will be used as a **backup server**:

- Domain name: Backup.
- Network interface NIC_CLUSTER: 192.168.0.103.
- Network interface NIC_VIDEO: 172.16.1.103.

14.1.5.2.4 Steps

Updating SecurOS configuration to work in cluster consists of the following steps:

1. Creating cluster on the *Configuration Server*.
2. Adding the second *Video Server* to the cluster.
3. Updating old configuration to work in cluster.
4. Adding backup server to the cluster.
5. Connecting *Operator Workstation* and confirmation of the operation ability.
6. Switch to the use of centralized storage.

Do the following with the help of `clustercli.exe` utility (see [Configuring Cluster](#)):

1. Switch to the **Video Server 1** (Configuration Server).

1.1. Create Cluster by executing following command

```
clustercli.exe create 192.168.0.101 172.16.1.101 172.16.20.1
```

Cluster will be created. There will be one *Host* within cluster configuration, that will continue to be *Configuration Server*. 172.16.20.1 virtual IP address will be used as IP-address of this *Configuration Server*. SecurOS configuration is saved unchanged.

At this stage the peripheral server will continue to work, having lost the connection with its old *Configuration Server*. Actually, it will work with its current SecurOS configuration until it is added to the cluster.

Virtual IP addresses of this *Host* will be assigned to the NIC_VIDEO (172.16.1.101) network interface. *Operator Workstations* will receive video through that interface.

2. Switch to the **Video Server 2** (old Peripheral Server).

2.1. Add Video Server 2 to the cluster by executing following command

```
clustercli.exe join 192.168.0.102 172.16.1.102 192.168.0.101
```

This *Video Server* also became cluster *Host*. Now *Hosts* are connected through NIC_CLUSTER network interface. SecurOS configuration is synchronized.

Virtual IP addresses of this *Host* will be assigned to the NIC_VIDEO (172.16.1.102) network interface.

3. Transform Computer objects to cluster Nodes by executing the following commands:

```
clustercli.exe node update Server1 172.16.20.101
```

```
clustercli.exe node update Server2 172.16.20.102
```

If commands terminates successfully, then *Computer objects* are the cluster *Nodes* for now. Each of commands cab be executed on any of two *Hosts*. *Nodes* will have the 172.16.20.101 and 172.16.20.102 virtual IP addresses, respectively.

4. Switch to **Computer 3** (third, backup server).

4.1. **Add Computer 3 to the cluster** by executing following command

```
clustercli.exe join 192.168.0.103 172.16.1.103 192.168.0.101
```

Last *Host* has joined the cluster. It will serve as backup *Host*.

Virtual IP addresses of this *Host* will be assigned to the `NIC_VIDEO` (172.16.1.103) network interface.

4.2. **Check cluster state** by executing following command on any of cluster members

```
clustercli.exe state
```

Cluster state will show that there are three *Hosts* with two running *Nodes*.

5. Switch to **Operator Workstation**.

5.1 Start operator interface and specify 172.16.20.101 (one of *Nodes* virtual IP address) as IP address to connect.

5.2 Authorize.

6. Configure *Computer* objects that correspond to cluster *Nodes*, so that the archive recording is kept on a centralized storage (see [Storing Data in Cluster](#)).

14.1.6 Resolving Common Issues

This section describes following problems:

- [Quorum Loss](#).
- [Restoring Operating System from Backup](#).
- [Unable to Connect Operator Workstation](#).

14.1.6.1 Quorum Loss

Quorum loss (see [Cluster Operation. Quorum](#)) may happen due to following reasons:

- Half or more *Hosts* in cluster fails;
- There was a mistake while adding *Host* to cluster.

As far as cluster configuration cannot be changed without quorum, adding new *Hosts* is impossible and will not solve the problem. There are two ways to restore quorum state:

1. Restore failed *Hosts*.
2. Recreate cluster with only working *Hosts* in it (see [Recreating Cluster](#)).

Second way allows to partially restore system's functionality and also opens ability to add new *Hosts*.

14.1.6.2 Restoring Operating System from Backup

Restoring *Host*'s operating system from backup may cause negative impact on cluster state. In this regard, dependently on current cluster state, the procedure can be performed in different ways:

- **In quorum state** – in this case cluster functionality will not be interrupted. One can restore from backup without any concerns.
- **Quorum state lost** – in this case *Hosts* that were restored from backup may damage cluster

configuration after returning to quorum state. It is recommended to perform cluster recreation procedure (see [Recreating Cluster](#)) before restoring from backup. Follow these steps:

1. Execute cluster recreation command on one of live *Hosts*.
2. Restore failed *Hosts* operating systems from backup.
3. Add all *Hosts* back to cluster.

14.1.6.3 Unable to Connect Operator Workstation

Operator Workstations may lose ability to connect to *Video Servers* due to following reasons:

- **Situation 1:** Security settings do not allow servers to accept connection from *Operator Workstations*.
In this case the solution will be to connect as superuser (see [SecurOS Users](#)) and change settings.
- **Situation 2:** There no running *Nodes* or working *Video Servers* that *Operator Workstation* can connect to.
If the license key allows, one can create one more *Node* (see [Adding Node](#)) and connect to it. If it is not possible then one can convert failed *Video Server* to *Node* (see [Converting Video Server to Cluster Node](#)). If converting to a *Node* is not a suitable solution, one can delete this *Video Server* and create a *Node* instead.

14.1.6.4 Updating Software and Hardware within Cluster System

To update software/hardware in cluster configuration do the following:

1. Update procedure must be started on computers that are the members of cluster. Switch cluster to the `fixed_cs` service mode (see [Service mode](#)). This mode will not allow other *Host* to get the *Configuration Server* role during system updating procedure. Otherwise system configuration can be corrupted.
2. Find out which of the cluster *Hosts* is the *Configuration Server* (see [Getting Current Cluster Configuration](#)). If it is necessary, assign the *Configuration Server* role to the *Host* that is more convenient for updating (see [Setting Configuration Server](#)).
3. Execute all required software/hardware update operations on the *Configuration Server*.
4. Update all other *Hosts* of the cluster.
5. Turn service mode off.
6. Update computers that are not members of the cluster.

14.1.7 Limitations

Using cluster in SecurOS configuration has following limitations:

- Cluster can only be deployed under 64 bit OS.
- Only one cluster in configuration.
- *Configuration Server* role can be assigned only to cluster member.
- One *Host* can run only one *Node* at the same time.
- System time on all *Hosts* must be synchronized;
- The following Modules will not work on the cluster's *Hosts*:

- POS;
 - WebView;
 - SNMP;
 - SecurOS UVSS.
- Use of *Archiver* on cluster *Hosts* in **Continuous** and **Scheduled** modes (see [Archiver](#)) is not supported. To provide continuous access to the created *Long-term archive* it is recommended to use *Network folders* or iSCSI drive.
 - Detailed *Mobile Server* configuration is described in [SecurOS Mobile Quick Start Guide](#).
 - Detailed *ActiveMedia Kit* configuration is described in [SecurOS ActiveMedia Kit Guide](#).
 - SecurOS objects, concerning with computer settings or files, located on this computer, must be duplicated on all *Hosts* of the cluster.

iSCSI storage limitations:

- iSCSI Target can have only one LUN.
- MPIO (Multipath I/O) is not supported.

14.2 Redundant Servers Cluster

In some cases hardware requirements to the configuration do not allow to use classic cluster to provide redundancy. In these cases a **Redundant servers cluster** can be created.

This approach is based on the ability of the cluster to act as a redundant group for non-cluster servers. Number of such servers can significantly exceed the number of cluster members. Thus, most of the time *Nodes* are working outside the cluster. The most common scenarios for using a redundant servers cluster are the following:

1. The configuration consists of two computers (1+1) and one of them is redundant (see example in the [Creating "1+1" Cluster from Existing SecurOS Configuration. Example](#)).
2. Distributed configuration where SecurOS is working on the computers that do not have stable connection with the cluster.

Warning! Redundant servers cluster does not support working with the centralized data storage. Use computer's local hard drives to store archive and databases.

14.2.1 Creating Configuration on the Base of Redundant Servers Cluster

To organize redundancy based on a redundant servers cluster perform the following steps:

1. Determine which of the servers will be redundant.
2. Create cluster (see [Creating cluster](#)) and integrate these redundant servers in it (see [Adding Host](#)).
3. Use operator interface and create required number of *Nodes* (see [Connecting Operator Workstations to the Cluster Servers](#)). Number of *Nodes* must match the number of computers that you plan to connect to the redundant servers cluster.
4. Add to the cluster the computers on which the *Nodes* will run in the normal mode (see [Adding Computer to the Redundant Servers Cluster](#)).
5. For each *Node* specify preferred *Host* from the list of the computers added to the cluster (see [Setting Preferred Host for the Node](#)).

After completing these steps, the system is operational, and the cluster provides redundancy.

14.2.2 Adding Computer to the Redundant Servers Cluster

To add computer to the redundant servers cluster execute the following command on this computer:

```
Clustercli.exe attach <virtual_ip_nic> <hosts_list>
```

where:

- `ip_address_nic` - IP address of network interface on this computer, which virtual IP addresses will be assigned to;
- `hosts_list` - list of the IP addresses of the *Hosts* of the redundant servers cluster, separated by space. It is recommended to specify IP addresses of all *Hosts*.

After executing the command, SecurOS service will restart.

Warning! If the computer that is being added to the cluster stores any SecurOS configuration it will be overwritten.

Immediately after adding computer to the cluster it must be set as preferred for one of the *Nodes* (see [Setting Preferred Host for the Node](#)).

Such a server cannot be disconnected from the cluster using the `remove` command. Execute `leave` command (see [Switching to Video Server Mode](#)) on this computer to stop cluster from taking it into account when distributing *Nodes*.

14.2.3 Creating "1+1" Cluster from Existing SecurOS Configuration. Example

This section describes steps required to organize redundant system in SecurOS configuration containing only one *Video Server*.

14.2.3.1 Task

Transform an existed SecurOS configuration to work in "1+1" cluster. Current configuration includes one *Video Server*. It is planned to use additional computer to provide redundancy.

14.2.3.2 Computers Parameters

Security Zone which ID is 1 already exist within SecurOS configuration.

Computer that belongs to existed configuration has the following parameters:

- Domain name: `Server1`.
- IP address: `192.168.0.101`.

Computer that you plan to add to the cluster **to provide redundancy**:

- Domain name: `Server2`.

- IP address: 192.168.0.102.

The SecurOS must be installed on the computer being added.

14.2.3.3 Steps

Updating SecurOS configuration to work in cluster consists of the following steps:

1. Creating redundant servers cluster on the base of the existing *Video Server*.
2. Adding the second computer to the redundant servers cluster.
3. Updating old configuration to work in cluster.
4. Selecting new server as preferred to work with SecurOS;
5. Performance verification.

Do the following with the help of `clustercli.exe` utility (see [Configuring cluster](#)):

1. **Jump to the Server1** (*Video Server*, where SecurOS is now working).

Create Cluster by executing following command:

```
clustercli.exe create 192.168.0.101 192.168.0.101 172.16.20.1
```

The cluster will be created. There will be one *Host* within the cluster configuration, that will continue to be the *Configuration Server*. 172.16.20.1 virtual IP address will be used as IP-address of this *Configuration Server*. SecurOS configuration is saved unchanged.

Virtual IP addresses of this *Host* will be assigned to the network interface that has the 192.168.0.101 address – the same interface, that is selected to provide connection with the other *Hosts*.

2. Jump to the **Server2** (new computer).

Attach Server2 to the cluster by executing the following command:

```
clustercli.exe attach 192.168.0.102 192.168.0.101
```

Now this computer is attached to the cluster. SecurOS configuration is synchronized.

Virtual IP addresses of this *Host* will be assigned to the network interface that has the 192.168.0.102 IP address.

3. **Transform Computer objects to cluster Node** by executing the following commands:

```
clustercli.exe node update Server1 172.16.20.101
```

If commands terminates successfully, then *Computer object* is the cluster *Node* for now. It will has the 172.16.20.101 virtual IP address.

4. **Make attached server preferred for the Node** by executing the following command:

```
clustercli.exe node set Server1 pref_host=Server2
```

After that SecurOS will start working on the server connected to the cluster. If Server2 fails the it work will be continued on the Server1.

5. **Make sure** that the system is working.

5.1 Start operator interface on any computer and specify 172.16.20.101 (*Node* virtual IP address) as IP address to connect.

5.2 Authorize.

15 Interaction with External Systems

This section describes algorithm and sequence of the SecurOS configuration procedure to provide interaction with different external systems.

15.1 Interaction with External Emergency Service

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

Using SecurOS security system one can inform external Emergency service about incident or emergency situation. Message is sent as *Emergency ticket* that contains detailed information about event. Further message processing is performed by Emergency service operator.

Emergency ticket can be created with the help of [Event Viewer](#) or [Media Client](#).

The following object must be configured in SecurOS to create and send the *Emergency ticket*:

- **Emergency service** – this object prepare data that can be transferred in *Emergency ticket*:
 - http address of the Emergency service.
 - list of cameras for which it is possible to create *Emergency ticket* and addresses of their physical location.
 - parameters for creation links to the video related to the incident. Using created link an Emergency service can download video. Both live and archive video can be downloaded. [RTSP Server](#) or [WebView](#) module are used to download video (see [SecurOS WebView User Guide](#)).
 - incident types list. Create and download to the SecurOS incident types list, that is required to send *Emergency ticket* (see [Incident Types List. File Format](#)).
- **Event Viewer** – possibility to create and send the *Emergency ticket* ([Send Ticket to Emergency Service](#) parameter) is configured. Using protocol entries relevant to the *Camera* object operator can watch live or archive video of the event in the *Media Client* and/or create and send *Emergency ticket*.
- **Media Client** – possibility to create and send the *Emergency ticket* ([Send Ticket to Emergency Service](#) parameter) is configured.

After system is configured it operates as follows:

1. Using an [Event Viewer](#) or a [Media Client](#) operator controls beginnings of the incidents or emergency situations.
2. If appropriate entry is added to the *Event Viewer* operator watches the video and makes a decision if a message must be sent to external Emergency service. When working with video using a *Media Client* operator controls the situation visually.
3. If decision is made operator creates and sends *Emergency ticket*. *Emergency ticket* can be created and sent both with the help of [Event Viewer](#) and [Media Client](#) (see [SecurOS Quick User Guide](#)).

Emergency ticket contains two part of data: the first part is displayed in the interface window and is visible to the operator (see Table 91), and the second part is not (see Table 92). Data are sent to the Emergency service in JSON format.

Table 91. Parameters of the message that are displayed in the Emergency ticket

Parameter	Description
Incident Time	Incident Time. When sending an <i>Emergency ticket</i> from the <i>Event Viewer</i> is filled with event time. When sending an <i>Emergency ticket</i> from the <i>Media Client</i> is filled with frame time.
Incident Place	Address of the incident place. In the <i>Emergency ticket</i> interface window is displayed as a <i>Camera's ID</i> and name. At the same time in the transferred message body these data are replaced by physical address of the camera location specified in the Emergency service settings.
Incident coordinates	Coordinates of the camera, that recorded the incident video (see General Tab).
Incident Type	Choose incident type from the list.
People in danger	Select this checkbox if an incident poses a threat to people.
Additional Info	Text comment on the incident. Is filled automatically by system (if the Comment field of the <i>Event Viewer</i> table contains entry) or can be filled manually by operator.

Table 92. Parameters of the message that are not displayed in the emergency ticket

Parameter	Description
Source of information	<p>Personal data of the operator (Name and Phone number) who create and sent an <i>Emergency ticket</i>, where:</p> <ul style="list-style-type: none"> • Name — Name of the User account from the <i>Object tree</i>; <hr/> <p>Note. Data are sent as the <Last name><First name><Middle name> structure that are created from the Name string as follows: the <Last name> field is filled in by the first part (substring) of the object's Name. the <First name> field is filled in by the second part (substring) of the Name string, that is separated from the first part by space. the <Middle name> field is filled in by the third part (substring) of the object's Name, that is separated from the second part by space, too. If there are no parts (substrings) separated by space in the object's Name, then whole sting is substituted for the <Last name> field. Other fields remain empty. For example, the Name of the object is specified by the following string: Jameson John. In this case the Jameson value will be substituted for the <Last name> field and the John value — for the <First name> field. The <Middle name> will be empty.</p> <hr/> <ul style="list-style-type: none"> • Phone number — is the Phone parameter value from the User account object.

Parameter	Description
Links to watch video	<p>Links to connect to the RTSP or WebView servers to watch video.</p> <hr/> <p>Note. To create these links the parameters specified in the Emergency service object settings are used.</p> <hr/>

16 Light Integration

This section describes light integration of SecurOS with the external FAAC (Fire Alarm/Access Control) and radiation monitoring systems.

16.1 General Description

SecurOS allows to integrate some FAAC (Fire Alarm/Access Control) – **Bolid** and **FortNet**. The interaction model presumes that the external module transfers some events to SecurOS where these events can be processed.

Note. The list of the external system events supported by SecurOS is specified within the program code of the Bolid and FortNet internal module of integration.

Processing of the events generated by the external system can result in the changing state of the external system object placed on *Map*, displaying SecurOS form that requires an operator's action (for example, displaying short message window to call police) or sending a control action to the external system modules (only for which this possibility is specified in external system).

Program interface with the external system is provided by SecurOS internal executor, that corresponds to Bolid and FortNet integration.

The root *<integration_name> integration* object is used to describe and control the external system from inside SecurOS. The integration object tree (external system modules tree) is built automatically on the base of the file, that describes external system configuration (see [Integration Point](#)).

After object tree is built any of its entries can be placed on *Map*. Further operation with objects of the external system placed on *Map* is similar to operations with typical SecurOS objects placed on the *Map*.

One of the following methods can be used to transfer control actions to the external module:

- using *Macro* (see [Macro](#));
- executing *VB/JScript program* (see [VB/JScript program](#));
- as a result of operation executed with the object placed on *Map* (see [Map](#)).

Logging of interactions between SecurOS and the external system and operations with the integration object tree is performed separately - events generated by the external system are stored in the SecurOS log, while operations with the external system object tree are stored in an independent log-file.

16.2 Integration Point

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

This object is designed to integrate external custom application into SecurOS. This is an API that implements the description of an external system in SecurOS and interacts with it using messages that use SecurOS *Events* and *Commands*.

Using this interface one can do the following:

1. Connect external system and SecurOS and control connection state;
2. Represent the configuration of the external system in the SecurOS *Object Tree* as a hierarchical structure;
3. Represent and control external system objects with the help of SecurOS user interfaces ([Map Window](#), [Macroses](#));
4. Display events of the external system in the [Event Viewer](#) and states of external system objects on the [Map](#).

Parent object – *Computer\Integration and Automation* group.

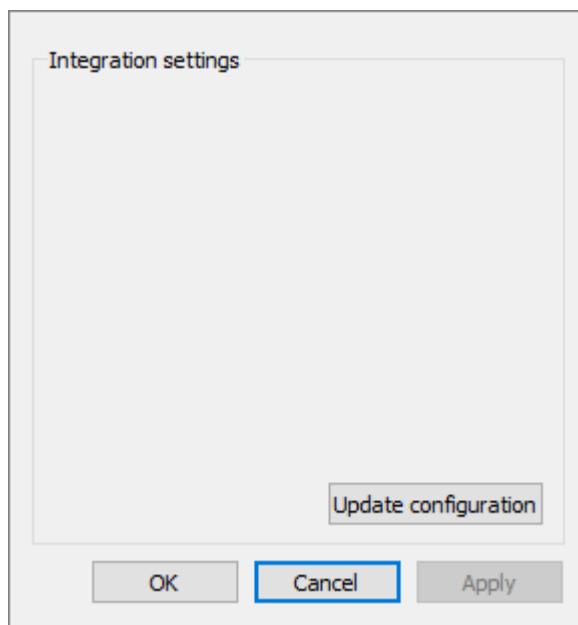


Figure 233. Integration point object settings window

Table 93. Integration point object settings

Parameter	Description
Update configuration (button)	Click this button to build configuration of the external system in the SecurOS <i>Object Tree</i> as hierarchical structure of objects.

Refer to [UinP User Guide](#) for a detailed explanation of how to configure system and use the *Integration point* object.

Note. **UinP User Guide** is not included into common documentation package and is provided by request.

16.3 SecurOS Integrations

SecurOS software distributive contains the dynamic link libraries that provide integration with the following external systems:

- **Bolid;**
- **FortNet.**

Intelligent Security Systems ensures stable operation of the integration for the following versions of the external system software:

- Bolid – ORION Pro version 1.11, release 2, build 1908;
- FortNet – APM 1.4.2.15.

16.3.1 Bolid

Bolid integration object is used to provide integration with the FAAC (Fire Alarm/Access Control) Bolid system.

Parent object – *Computer\ACS* group.

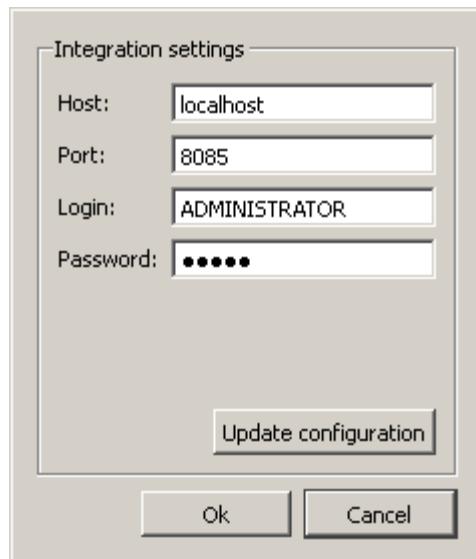


Figure 234. Bolid integration object settings window

Table 94. Bolid integration object settings

Parameter	Description
Host	IP address or network name of the computer where the Bolid integration internal executor is running. Default value is localhost.

Port	Communication port for interaction between the external system and the Bolid integration internal executor. Default value is 8085.
Login	User name to log into the Bolid system. Default value is ADMINISTRATOR.
Password	User's password to log into the Bolid system. Default value is ORION.
Update configuration	Receiving configuration data from the external system and rebuilding the external system's object tree within SecurOS.
OK (Cancel)	Save/discard changes.

SecurOS supports the following Bolid system's objects (modules):

- *Bolid controller;*
- *Bolid device;*
- *Bolid reader;*
- *Bolid loop;*
- *Bolid relay.*

Additional Information

Modules of the external system can be controlled with the help of *Macros*, *VB/JScript Programs* and *Map* object control commands. *Map* or *Event Viewer* objects are used to monitor object states.

16.3.2 FortNet

FortNet integration object is used to provide integration with the AC (Access Control) FortNet system.

Parent object – *Computer\ACS* group.

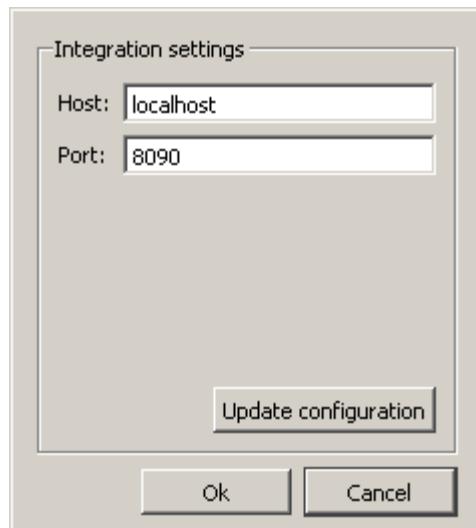


Figure 235. FortNet integration object settings window

Table 95. FortNet integration object settings

Parameter	Description
Host	IP address or network name of the computer where the FortNet integration internal executor is running. Default value is localhost.
Port	Communication port for interaction between the external system and the FortNet integration internal executor. Default value is 8090.
Update configuration	Receiving configuration data from the external system and rebuilding the external system's object tree within SecurOS.
OK (Cancel)	Save/discard changes.

SecurOS supports the following FortNet system's objects (modules):

- *FortNet computer;*
- *FortNet controller;*
- *FortNet controller loop;*
- *FortNet controller card reader;*
- *FortNet controller relay;*
- *FortNet check point;*
- *FortNet check point card reader;*
- *FortNet loop group;*
- *FortNet loop;*
- *FortNet relay group;*
- *FortNet relay.*

Additional Information

Modules of the external system can be controlled with the help of *Macros*, *VB/JScript Programs* and *Map* object control commands. *Map* or *Event Viewer* objects are used to monitor object states.

17 Keyboard Shortcuts

This section describes shortcuts used to perform actions on different SecurOS objects.

17.1 Administration Toolbar

Table 96. Shortcuts for working with SecurOS objects

Shortcut	Description
Delete	Delete the selected object
Enter	Open the selected object properties window
Space	Disable/enable selected object or all <i>Group</i> children objects
Ctrl+N	Displaying the menu for objects creation or for all <i>Group</i> children objects creation
*	Open all children branches for the selected object (plus additional level on each key button pressed)
+ (Num Pad)	Open a child branch for the selected object (one level)
- (Num Pad)	Close a child branch for the selected object
Ctrl+F	Open the search object window in object tree.
Enter	Look for the next object with the search parameters.
F1	In the Administration mode: <ul style="list-style-type: none">• if object settings window is opened it calls the help topic associated with this object;• if object settings window is closed it calls the help topic associated with the <i>Administration Center</i>.
F2	Rename the selected object
Esc	Close object settings window or SecurOS <i>Object Tree</i> window

18 Appendixes

This section contains a description of system utilities and other additional information useful to configure and operate the system.

18.1 Appendix A. Upgrading/Uninstalling Software

This section describes SecurOS upgrading and uninstalling specifics.

18.1.1 Upgrading Software

To upgrade software do the following:

1. Start the installation program by launching the setup file of the new software version.
2. Further installation steps are similar to ones for the first installation (see [SecurOS Installation and Update](#)).

18.1.2 Uninstalling Software

Uninstalling SecurOS is done in two steps:

- uninstalling software;
- removing video/audio archives and configuration database (optional).

To uninstall SecurOS software do one of the following:

- Launch the setup file of the currently installed software version. The system will display the [Program Maintenance](#) window (see figure 236)

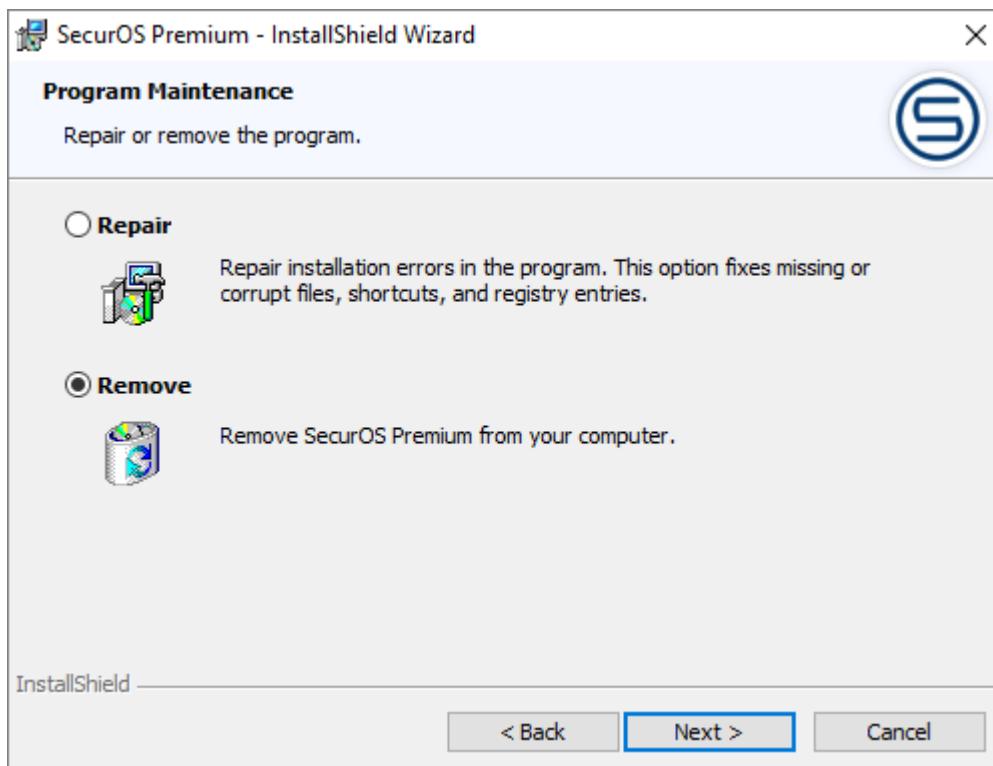


Figure 236. Program Maintenance Window

Select **Remove** option to uninstall the software, click **Next** button to continue.

- In the **Start** Windows menu choose the following menu options **All Programs** → **SecurOS** → **Uninstall SecurOS**.

SecurOS software will be uninstalled automatically.

Aside from uninstalling the software, you may want to delete all video and audio archives as well as the configuration database, all of which are not deleted automatically by the InstallShield Wizard.

Thus, this step should be done manually: to delete archives, delete any `\Video` and `\Audio` folders located in the root directory of your logical drive(s) (`C:\Video`, `C:\Audio`, `D:\Video`, `D:\Audio` etc.).

To delete the configuration database (PostgreSQL) launch the `uninstall-postgresql.exe` file from the `C:\Program Files\PostgreSQL\X.Y` directory, or use **Add or Remove Programs** option. The PostgreSQL directory in `C:\Program Files\` will have to be deleted as well.

18.1.3 SecurOS Version Upgrade Features

This section describes upgrade features of the following SecurOS versions:

- **Release 9.3 and Earlier Updating Procedure;**
- **Release 9.6 and Earlier Updating Procedure;**
- **Release 10.0 and Earlier Updating Procedure;**
- **Release 10.1 and Earlier Updating Procedure;**
- **Release 10.2 and Earlier Updating Procedure;**
- **Release 10.3 and Earlier Updating Procedure.**

18.1.3.1 Release 9.3 and Earlier Updating Procedure

Some changes, which should be noted during the update, have been made in SecurOS 9.4:

- [Running SecurOS server part as OS service.](#)
- [Administrating SecurOS from Operator Workstation.](#)
- [Archive recording.](#)

Running SecurOS server part as OS service

Starting from Release 9.4 *Server part* runs only as OS service. *Client part* implements operator GUI and runs as stand-alone application.

If you previously ran the *Server part* as an application, pay special attention to the following:

1. By default, *Server part* is running as Local System system user. This can cause the network folders mounted as network drives and previously selected for archive recording in the [Computer](#) object settings will be unavailable. To record an archive to shared network resource use network folders instead of mounted drives in the [Computer](#) object settings.
2. Notification about *Server part* crashes with the help of OS information messages displayed in separate windows is discontinued. Information about such crashes one can find in the OS log ([Event Viewer](#) → [Applications and Services Logs](#) → [SecurOS](#)). Information about *Server part* starting failures is saved into the `securos_svc.log` file, located in the `%ProgramData%\ISS\logs` folder.

Administrating SecurOS from Operator Workstation

Support of the *Computers*, role of which is *Administrator Workstation* has been discontinued. SecurOS administration features have been moved to the *Operator Workstations*.

When updating pay special attention to the following:

1. All *Administrator Workstations* are transformed into *Operator Workstations*.

Note. **Servers to connect** list for each transformed *Operator Workstation* will be empty. This means that *Operator Workstation* can connect to any *Video Server* within network. For the connection details refer to [Servers to Connect Tab](#) section.

2. Components of all SecurOS Intelligent Modules that are used within the system must be installed on each *Video Server* and *Operator Workstation* (see *User Guide* for the corresponding Module for the details).
3. Versions of the SecurOS and SecurOS Intelligent Modules must be the same on all *Computers* within network (see [SecurOS Update Order](#)).

Archive recording

The archive is recorded into files of specified size, which allows to reduce their fragmentation and, as a consequence, to increase the disk writing speed. Efficiency of this mechanism depends of free disk space.

Note. Intelligent Security Systems recommends to use 10%. This value is also recommended by Microsoft Corporation for NTFS partitions. One can change this value in the [Computer](#) object settings.

When working with SecurOS 9.4 pay special attention to the following:

1. When updating to version 9.4 free disk space will be automatically recalculated for each disk. Calculated value will be offered by default. This value can be changed with **Archive recording** slider (see [Archive](#)).
2. After updating the **Save space** mode is set automatically (see [Archive](#)).

18.1.3.2 Release 9.6 and Earlier Updating Procedure

Some changes, which should be noted during the update, have been made in SecurOS 10.0:

- [Connecting Operator's Workstations to Video Servers without additional settings. Access limitation.](#)
- [Operator Workstation Profiles.](#)
- [Using additional network ports.](#)

Connecting Operator Workstations to Video Servers without additional settings. Access limitation

Starting from Release 10.0 *Client part* can be launched on any computer, even it is not represented in the SecurOS *Object Tree*.

Settings for limit access of *Operator Workstation* to the *Video Servers* are located in the *Security Zone* object settings window now. **Servers to Connect Tab** allows to limit connections to specific servers (see [Servers to Connect Tab](#)) to provide automatic load balancing and automatic reconnection. **Connection Restrictions Tab** allows to create white list of the computers, that can connect to the *Video Servers* within the system (see [Connection Restrictions Tab](#)).

Operator Workstation Profiles

A new feature – *Operator Workstation Profiles* has been designed for making unified operator interfaces, that may be used on many computers simultaneously. Details and restrictions of working with profiles are described in the [Operator Workstation Profiles](#).

Using additional network ports

To provide SecurOS working it is necessary to open 21112 network port, that provides communication between *Client* and *Server parts*.

18.1.3.3 Release 10.0 and Earlier Updating Procedure

Starting from Release 10.0 the SecurOS configuration may include a cluster (see [Failover Cluster](#)). Sequence of steps to update such a configuration is described in the [Updating Software and Hardware within Cluster System](#).

18.1.3.4 Release 10.1 and Earlier Updating Procedure

In Release 10.2 the cluster was powered with the extended capability for storing video archive on the local drives of the *Hosts*. At the same time, the procedure for configuring disks has been changed. If local drives have been used to store video archive in cluster they must be reconfigured (see [Storing Video Archive on the Host's Local Drives](#)).

18.1.3.5 Release 10.2 and Earlier Updating Procedure

In Release 10.3 user access to the camera's wiper and camera's illumination is controlled via *User Rights* object settings. Operator must have **Control** or above access level to the *Camera* object to control its wiper or illumination.

Events redirection functionality has been updated. When updating SecurOS up to the version 10.3 it is necessary to redefine rules for events redirection between the computers that have been set for the version 10.2 or below (see [Servers to Connect Tab](#)).

18.1.3.6 Release 10.3 and Earlier Updating Procedure

In the Release 10.4 there are some differences in the operation of the *Core*, *Audio* and *Video Subsystems* objects described in the following subsections:

- [Core Subsystem Operation Features](#).
- [Video Subsystem Operation Features](#).
- [Audio Subsystem Operation Features](#).

Core Subsystem Operation Features

When using SecurOS some service files on the *Peripheral Servers* and *Operator Workstations* can be edited locally and differ from the same files on the *Configuration Server*. After upgrading software to the version 10.4 all such files on all *Peripheral Servers* and *Operator Workstations* within SecurOS network will be automatically replaced by files from the *Configuration Server*. For the list of files to be updated see [SecurOS Files Synchronization](#).

Video Subsystem Operation Features

Automatic rearrangement of the date and time of the beginning and end of the fragment when playing the archive in the opposite direction is not supported anymore. In the version 10.4 the order of the date setting during reverse playback is defined by the system settings (for more details see the [RTSP Server](#) section).

Audio Subsystem Operation Features

In the version 10.4 the new format of the audio files for the archive records is supported. As a result of this, after upgrading to version 10.4 it is necessary to take into account the following features of SecurOS operation:

- Video archive recorded in the SecurOS version 10.3 and below, will be played back by default without audio in the version 10.4. To provide playing back the video archive together with the recorded sound, one must convert the accompanying audio file to a new format (see [Outdated Audio Archive Updater Utility](#)).

Note. To playing back in SecurOS MCC the archive with soundtrack recorded in the *Remote systems* no conversion of such archives in the *Remote Systems* is required.

- When playing back an archive recorded with the soundtrack the case when frames are played back with no sound is possible. When deleting files "in a ring" mode in case of expiration of their storage period, the lower time boundary of the oldest remaining files may differ. This feature is specific only for the first hour of the entire time period of the archive.
- New format of the audio files is not supported by the [ISS Media Export Utility](#).
- **SoundMixer Audio Capture Device** is no longer supported. When upgrading to the version 10.4 the

Type field in the settings of all existing devices of such type will be cleared.

18.2 Appendix B. Quick Video Subsystem Configuration

By default, the system object tree consists of the following objects after SecurOS installation and starting with empty database: *System*, *SecurOS*, *Computer*, *Desktop*, *Media Client*.

To create and configure a basic object of the video subsystem:

1. Configure *Computer* object parameters:

- **IP address** – click [<>] button near the field (127.0.0.1 value is set when there is no network connection).
- **Disk** – choose Read/Write from the list in **Video** and **Audio** column of the table in **Archive** tab. Then video and audio archive will be recorded on to selected drives.

Note. It is not recommended to select system drive with Operating System installed for read/write settings.

2. Create the *Video Capture Device* object(s). This object represents the device the video signal is coming from (IP camera, IP encoder, etc.). Configure the *Video Capture Device* parameters:

- **Type** – select device type corresponding to the device where video is coming from:
 - If video is coming from an IP camera/encoder, select the corresponding manufacturer of the IP camera/encoder.
 - For use of IP devices using standards protocols, the ONVIF, or Generic RTSP options can be used. The Device must support these Protocols.
 - To play pre-recorded videos (for demo or testing purposes) the Virtual or Player AVI options can be used.
- **IP Address, User, Password** – if using IP devices set these parameters accordingly.

3. Create the *Camera* object (child object of the *Video Capture Device* object). This object represents a single video stream. Specify the camera identifier in the **ID** field (you can begin with 1 and keep incrementing by 1), then specify its **Name** (e. g. Office, Street, Home etc.). You may also use default ID/Name.

Notes:

1. For single lens IP cameras, one *Video Capture Device* object will have one *Camera* child object.
 2. For cameras with more than one lens, one *Camera* object will be created for each lens. The *Camera* objects will be child objects of the same *Video Capture Device*.
 3. For cameras connected to IP encoders, one *Video Capture Device* object will have as many *Camera* child objects as cameras connected to the encoder.
-

Configure the *Camera* object parameters:

- **Channel number** – select from spin box:
 - If this camera is a single lens IP camera, then default value of 1 can be used.
 - If camera with more than 1 lens is being used, then one *Camera* object will be created for each lens. The *Camera* objects will have different channel numbers, incrementing from 1.
 - If this camera is connected to an IP encoder, then the number should correspond to the port the

camera is connected to.

- **Pan/Tilt/Zoom** – select Use for IP cameras with built-in PTZ device.
- **Image Settings** – specify parameters on the **Advanced** tab.

4. Select the mode of the *Media Client* operation with *Cameras*:

- Work with all cameras – default mode. Image from all system *Cameras* will be displayed on the *Media Client* (checkbox **Use only selected Cameras** is not selected).
- Use only selected Cameras – configurable mode. Image from selected *Cameras* only will be displayed on the *Media Client*. To activate this mode select the **Use only selected Cameras** checkbox, then in the *Object tree* select checkboxes on the left of that *Cameras* which will be used.

18.3 Appendix C. System Utilities

SecurOS software comes with several helper utilities. You can find them in the \Tools sub-folder of SecurOS installation folder or in SecurOS installation folder itself:

- **SecurOS Server Manager** utility (`ServerManager.exe`) allows to monitor *Configuration servers* states, to create and control cluster (see [SecurOS Server Manager Utility](#)).
- **ISS Hardware Report Utility** (`HardwareReportUtility.exe`) reports all installed Guardant keys (see [ISS Hardware Report Utility](#)).
- **ISS System Report Utility** (`ISSInfo.exe`) collects system and network information required by Intelligent Security Systems Technical Support (see [ISS System Report Utility](#)).
- **ISS Media Export Utility** (`Backup.exe`) plays archived video/audio, exports selected parts of archive to AVI, ASF and BMP files (see [ISS Media Export Utility](#)).
- **DSAdmin** utility (`dsadmin.exe`) creates and stores database connection parameters (see [DSAdmin Utility](#)).
- **Database Update Utility** (`ldb.exe`) defines access to database: to update and configure (see [Database Update Utility](#)).
- **ISS SecurOS Registration Files Editor** (`DDI.exe`) edits SecurOS object types database (not the actual database itself) (see [ISS SecurOS Registration Files Editor](#)).
- Video archive index repair utility (`MediaIndexRepairer.exe`) is used to work with the SecurOS video archive index files (see [Video Archive Index Repair Utility](#)).
- Audio archive converter utility (`AudioArchiveConverter.exe`) is used to convert SecurOS audio archive of an outdated format to the new one (see [Outdated Audio Archive Updater Utility](#)).
- **Certificate Generator** utility (`CertificateGenerator.exe`) is intended for creating trial SSL certificates (see [Certificate Generator Utility](#)).
- **AuditClient** utility (`audit_client.exe`) is intended for obtaining SecurOS audit data (see [AuditClient Utility](#)).

18.3.1 SecurOS Server Manager Utility

This utility is intended for centralized monitoring and controlling SecurOS server (hosts) states. Using it one can perform all operations for cluster creating and configuring (see [Redundancy](#)). One can manage multiple configurations at once.

Warning!

1. The utility interacts with the *SecurOS Control Service* on the remote hosts. If service on the host is stopped it won't be available for management.
2. To provide module working it is necessary to open TCP ports in the firewall settings (see [Appendix D. TCP/IP Ports Used by SecurOS](#)).
3. The utility supports working with servers that running Microsoft Windows operating system only.

Main purposes of the utility are the following:

- Monitoring the host's states;
- Creating a failover cluster;
- Clear visual representation of the cluster state;
- Configuring cluster.

Warning! To create cluster nodes and change their parameters one should use SecurOS *Object Tree* (see [Adding Node](#)).

Location:

<SecurOS root folder>\ServerManager.exe

Launching from the Start menu:

Start → Programs → SecurOS → SecurOS Server Manager

Appearance of the main window is represented on Figure 237.

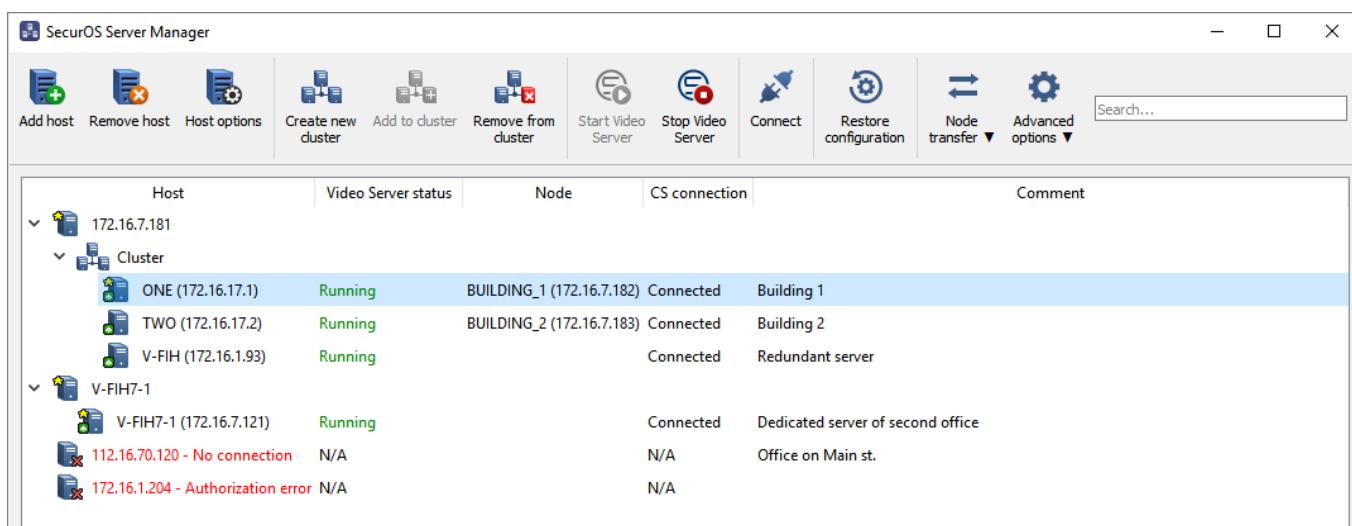


Figure 237. Server Manager Utility window

At the top of the utility window a control panel consisting of buttons and a search bar is located (see [Control Toolbar](#)).

Below the toolbar the hosts table is located. This table displays states of all hosts added to the utility list and grouped by *Configuration Server* (see [Hosts Table](#)).

18.3.1.1 Control Toolbar

Appearance of the *SecurOS Server Manager* control toolbar is represented on Figure 238.

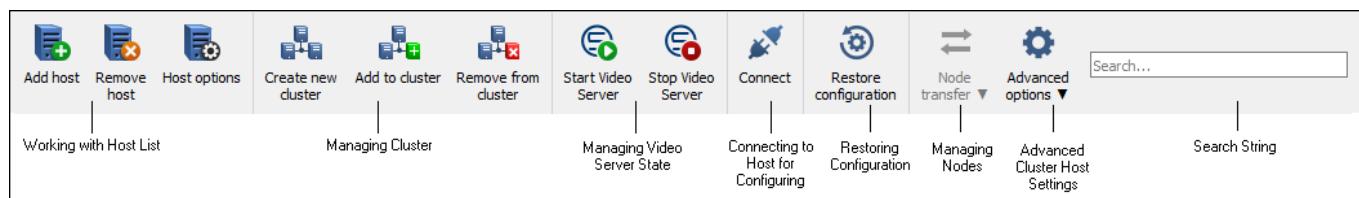


Figure 238. Control toolbar

The control panel provides the following features:

- **Working with Host List;**
- **Managing Cluster;**
- **Managing Video Server State;**
- **Connecting to Host for Configuring;**
- **Restoring SecurOS Configuration;**
- **Managing Nodes;**
- **Advanced Cluster Host Settings;**
- **Search String.**

18.3.1.1.1 Working with Host List

Working with the hosts list includes the following operations:

- **Adding host to the list;**
- **Removing host from the list;**
- **Editing host settings;**

Adding host to the list

Click the **Add host** button or **Insert** key and fill in the fields displayed in the window that appears.

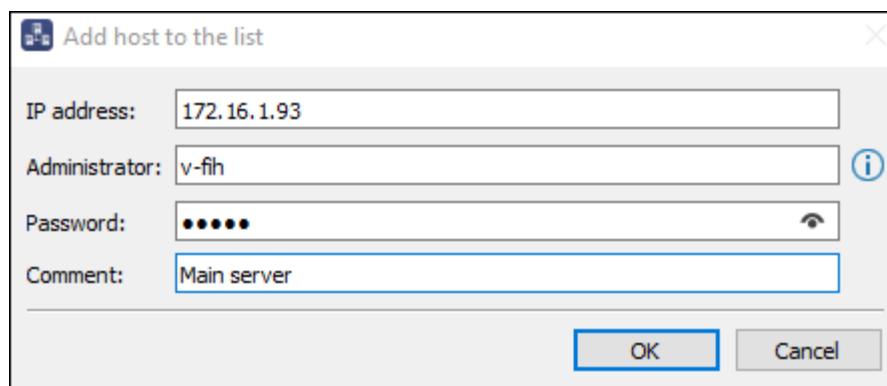


Figure 239. Add host to the cluster window

In the **Administrator** field must be specified user of the operation system, which has an administrator rights on the computer to be added.

Removing host from the list

Select the host and click the **Remove host** button or **Delete** key.

Editing host settings

Select the host and click the **Host options** button or **Enter** key. Authorization parameters and user comment options are available to change.

18.3.1.1.2 Managing Cluster

Cluster control includes the following operations:

- [Creating Cluster](#);
- [Adding host to the cluster](#);
- [Removing host from the cluster](#);

Creating Cluster

Select in the list the host on which the cluster must be created and click the **Create new cluster** button. Fill in the fields of the window that appears.

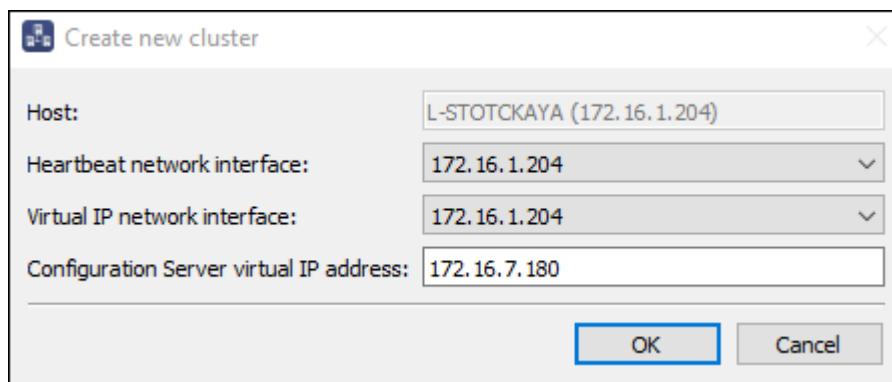


Figure 240. Create new cluster window

Specify available and not used IP address in the **Configuration Server virtual IP address** field.

Note. If the host that already is a member of the cluster is selected, then existing cluster will be recreated.

Adding host to the cluster

Select in the list working host that is not a cluster member and click the **Add to cluster** button. Fill in the fields of the window that appears.

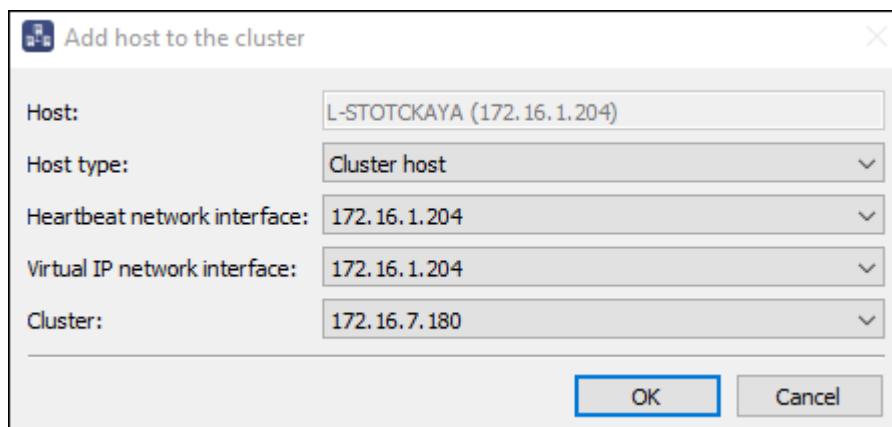


Figure 241. Add host to the cluster window

To connect selected host to the redundant servers cluster (see [Redundant Servers Cluster](#)) select the Non-cluster host in the **Host type** field.

Removing host from the cluster

Select in the list working host that is a cluster member and click the **Remove from cluster** button.

Removing host from the cluster is performed in two steps:

1. Removing host from the list of cluster members.
2. Switching host to the *Video Server* working mode.

Therefore, when removing host from the cluster, three scenario are possible:

1. Host that is being removed is available and there is a quorum within the cluster. In this case both steps will be executed successfully and host will be completely removed from the cluster.
2. Host that is being removed is available and there is no quorum within the cluster. In this case cluster will not be able to remove the host from its members list. Herewith the host itself will switch to the *Video Server* working mode. Further it is necessary to execute the host removing procedure again after quorum is restored.
3. Host that is being removed is unavailable and there is a quorum within the cluster. In this case cluster will remove the host from its members list. Herewith the host will not be able to switch to the *Video Server* working mode. Further it is necessary to execute the host removing procedure again after connection is restored.

18.3.1.1.3 Managing Video Server State

Use the **Start Video Server** and **Stop Video Server** to control SecurOS Video Server state on the selected host.

18.3.1.1.4 Connecting to Host for Configuring

Select host and click the **Connect** button or double-click the host to start the SecurOS client part.

18.3.1.1.5 Restoring SecurOS Configuration

Select host and click the **Restore configuration** button to open window to select configuration file. To restore configuration follow the instruction displayed in the window.

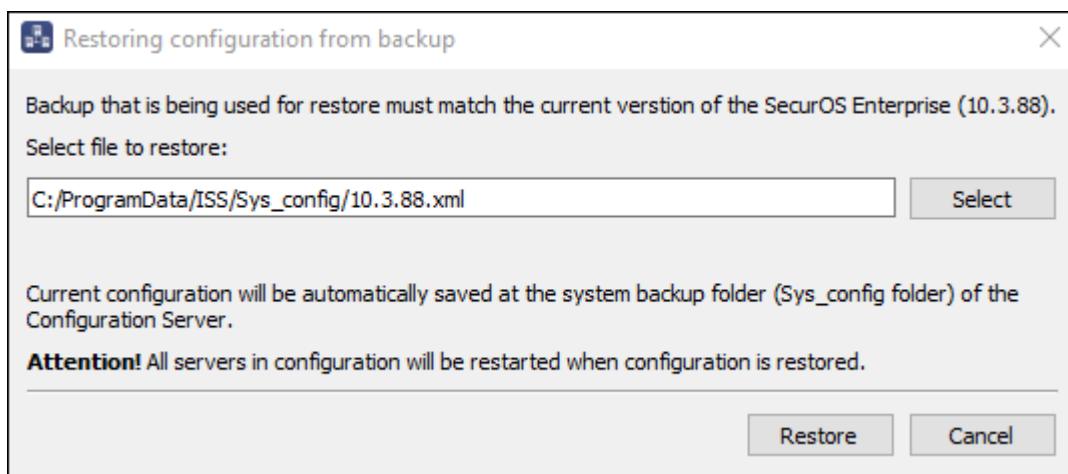


Figure 242. Restoring configuration from backup window

Note. The current password of the superuser (see [SecurOS Users](#)) will not be changed after restoring the configuration.

18.3.1.1.6 Managing Nodes

Node control includes the following operations:

- [Moving Node](#);
- [Choosing / Viewing preferred host](#);

Moving Node

Select from the list the host on which the node that must be moved is working. Click the **Node transfer** button and select the **Move node**. In the window that appears select the cluster host to which the node has to be moved.

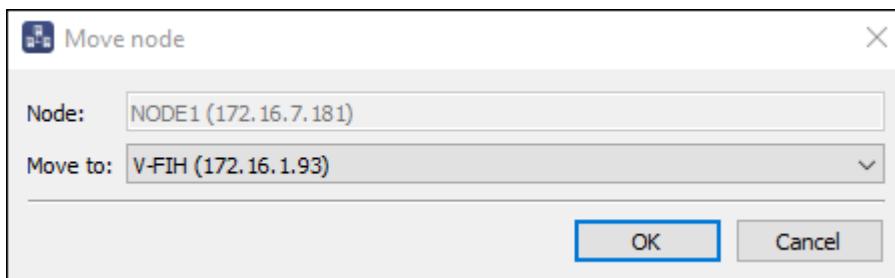


Figure 243. Move node window

Choosing / Viewing preferred host

Select from the list the host on which the node for which the preferred host must be assigned is working. Click the **Node transfer** button and select the **Set preferred host** command. In the window that appears choose cluster host that must be preferred for the node. If **Preferred host** parameter is set this means that selected host already is a preferred for this node.

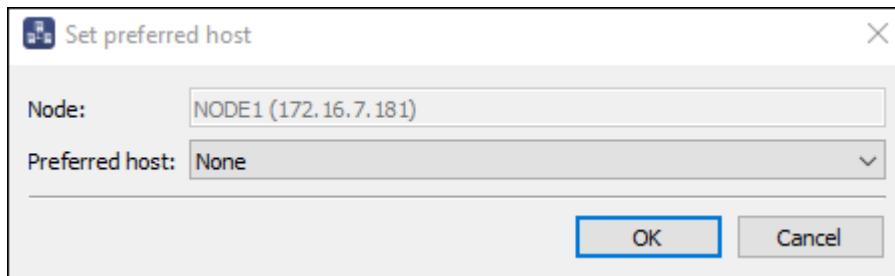


Figure 244. Set preferred host window

For more information about preferred hosts see [Setting Preferred Host for the Node](#).

18.3.1.1.7 Advanced Cluster Host Settings

Advanced cluster host settings includes the following operations:

- [Changing / viewing network interface for virtual IP addresses](#);
- [Turning service mode on/off](#);
- [Moving Configuration Server role](#);

- **Setting up / viewing local drives for storing archive.**

Changing / viewing network interface for virtual IP addresses

Choose cluster host in the list then click the **Advanced options** button and select the **IP settings**. In the **Virtual IP network interface** field will be displayed IP address that corresponds with network adapter used to support virtual IP addresses. Change it if necessary.

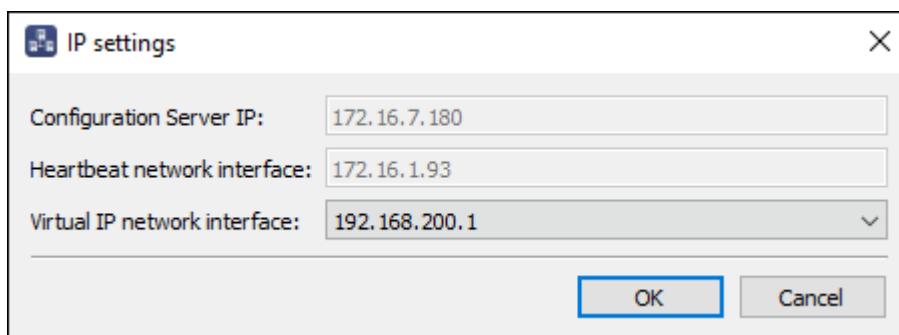


Figure 245. IP settings window

Turning service mode on/off

Choose any cluster host in the list then click the **Advanced options** button and select the **Service mode**. Current value of the **Service mode** parameter corresponds with the type of the current cluster service mode.

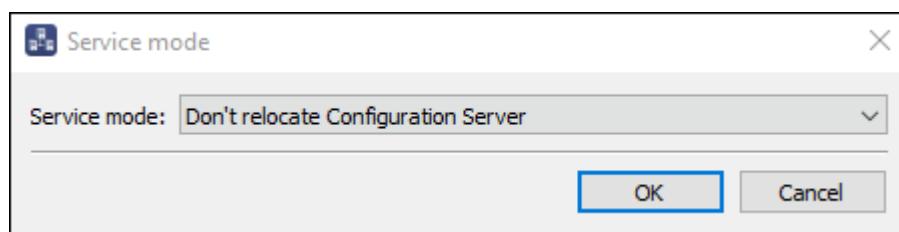


Figure 246. Service mode window

For the details on service mode see [Service mode](#).

Moving Configuration Server role

Choose cluster host in the list than click the **Advanced options** button and select the **Turn into Configuration Server**.

Setting up / viewing local drives for storing archive

Choose cluster host in the list then click the **Advanced options** button and select the **Local drives settings**. Marked drives are currently used for archive storing on the selected host.

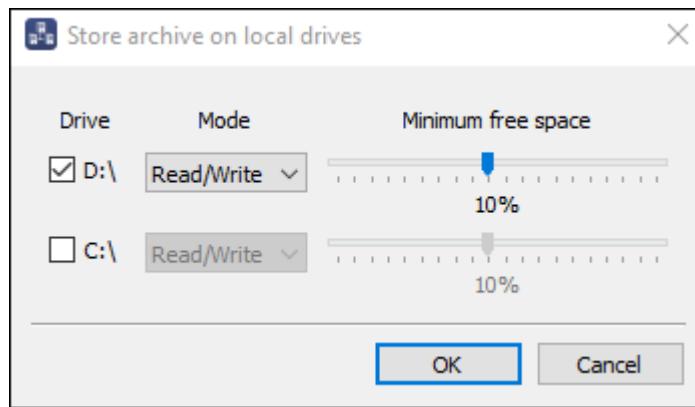


Figure 247. Store archive on local drives window

Note. Writing to the drives selected in this window is performed with higher priority than to the iSCSI drive/network folder specified in the *Computer* object settings.

18.3.1.1.8 Search String

Fill in the search string the part of the host/node name or user comment to find required host within the table.

Warning! Do not leave search string filled for a long time, otherwise one can miss failures in other hosts working.

18.3.1.2 Hosts Table

Hosts table consists all hosts added to the utility and displays them as a tree. It includes the following columns:

- **Host.** Contains host name, its IP address and configuration structure.
- **Video Server status.** If the connection with the server is established then one can control *Video Server* state with the help of the **Start Video Server/Stop Video Server** buttons (see [Managing Video Server State](#)).
- **Node.** Contains node name and its IP address when host is a member of the cluster.
- **CS connection.** Contains state of the connection between host and its *Configuration Server*.
- **Comment.** Contains additional information about host provided by the administrator.

Tree structure is represented on Figure 248.

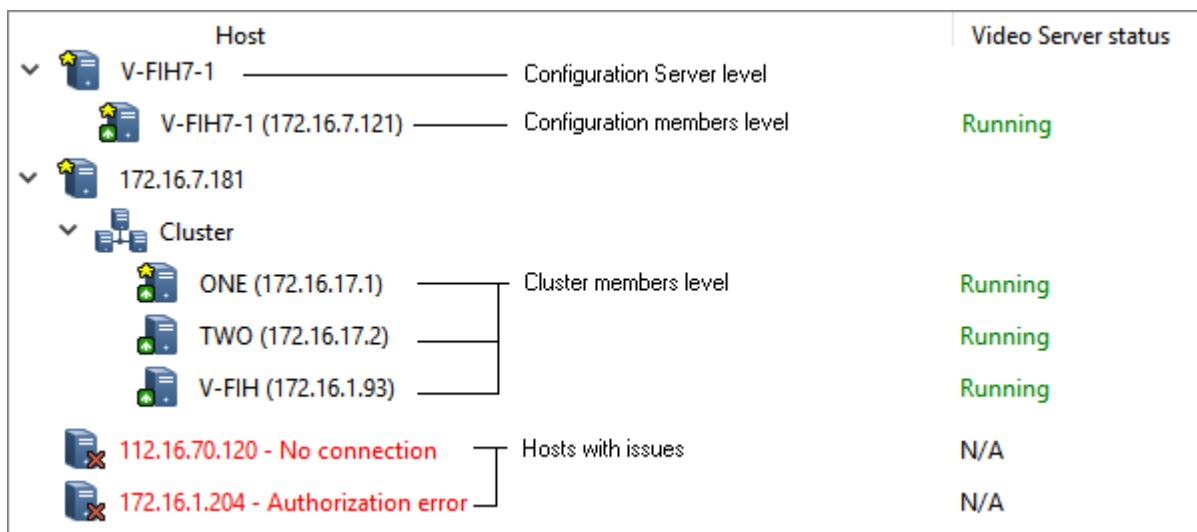


Figure 248. Hosts tree structure

Tree in the **Host** column has the following structure:

1. **Configuration server level.** At this level the *Configuration Servers* are located (names or IP addresses).

Note. This string is a grouping. To execute operations with the *Configuration Server* add it to the utility and select string corresponding to it at the second level of the table.

2. **Configuration members level.** At this level the hosts involved into configuration are located. Including the *Configuration Server*.
3. **Cluster members level.** At this level the members of the cluster created in the given configuration are located. For the cluster hosts the table displays the nodes that currently correspond to these hosts.
4. **Host with issues.** Hosts that failed to connect. They are listed at the end of the list with a problem description.

To mark roles and states the following icons are used in the table:

- – root item of the configuration.
- – root item of the cluster within the configuration.
- – *Configuration Server* in the given configuration.
- – operable host in the given configuration.
- – operable auxiliary host in the given configuration.
- – host is connected, but SecurOS Server part is stopped.
- – host state is unknown. For example, this icon is assigned when SecurOS Server part is being started or stopped.
- – host that is not connected. In this case the reason for the lack of communication is added to the host name.
- – crash host. Place mouse pointer over the **Emergency stop** string to display the crash reason.

18.3.2 ISS Hardware Report Utility

Location:

<SecurOS root folder>\Tools\HardwareReportUtility.exe

Start menu:

Start → Programs → SecurOS → Hardware Report Utility

Utility is used to detect all Guardant keys installed on given computer (see figure 249). The report is used to generate the system license key file key.iss by the Intelligent Security Systems Technical Support Team.

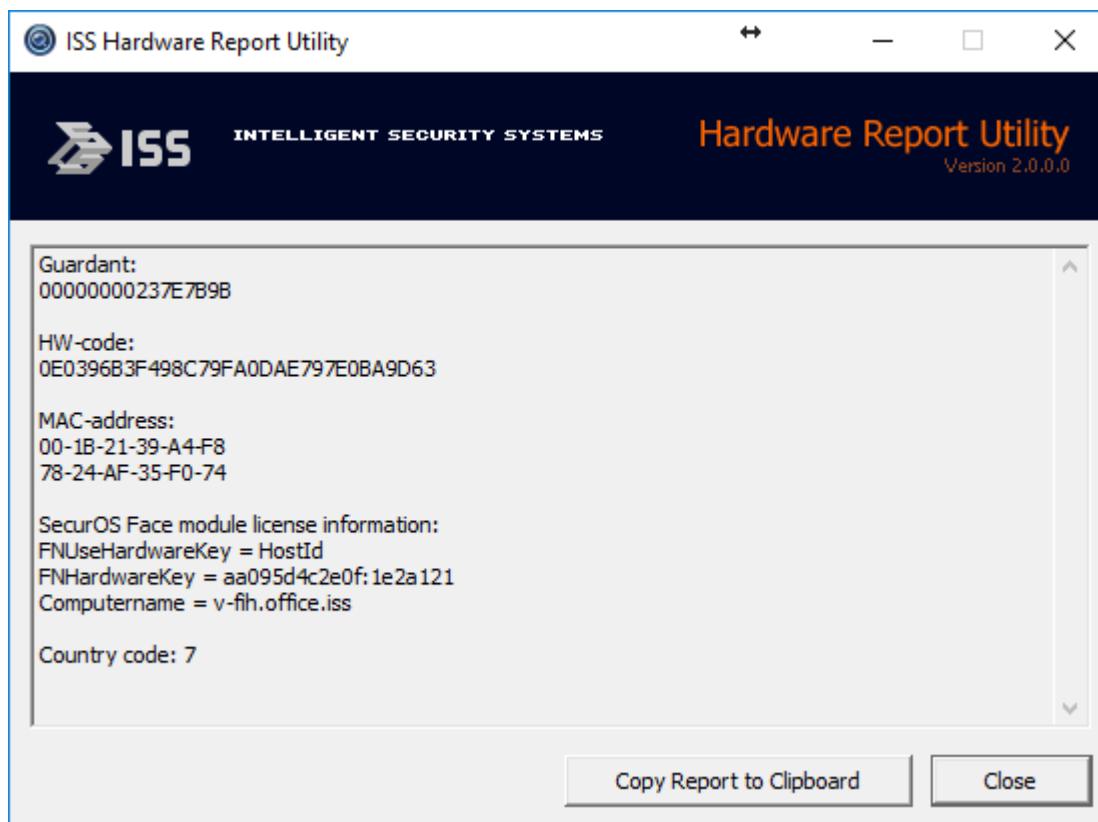


Figure 249. ISS Hardware Report Utility window

To save the utility report into a file:

1. Click **Copy Report to Clipboard** button in the utility window.
2. Create empty text file in any word processing program (Notepad, Microsoft Word etc.).
3. Paste clipboard content and save the report file.

This utility can also be used to check the correct installation of the above hardware devices and associated drivers: if the hardware identifier is missing, this means that device drivers were not installed properly.

18.3.3 ISS System Report Utility (ISSInfo)

Location:

<SecurOS root folder>\Tools\ISSInfo.exe

This utility is intended for collecting technical information about the SecurOS installation, your computer and network (see figure 250). This information is necessary to resolve problems and will always be requested by the Technical Support Team. Collected information will be saved in the ISSInfo report.



Figure 250. ISS System Report Utility window

To create a report

1. Select file name.
2. Specify collection procedure parameters (see [Utility Parameters](#) below).
3. Click the **Go** button.

ISSInfo report (see [Report structure](#)) will be saved as **.7z** file.

Utility Parameters

- **Include full crash dumps** – tick this checkbox if SecurOS *Server* or *Client* crash information must be included in the report. To free up space on your hard drive after you exit the utility, tick the **Remove crash dumps when the information collection is complete** checkbox.

Note. In case of SecurOS *Client application* or its child process crash, the appropriate OS informational message is displayed (for example, see Figure 251). In case of SecurOS *Server part* or its child process crash, [Health Monitor](#) self-diagnostic module's message is displayed. Full dumps are required only to analyze such system crashes and not required for all any problems.

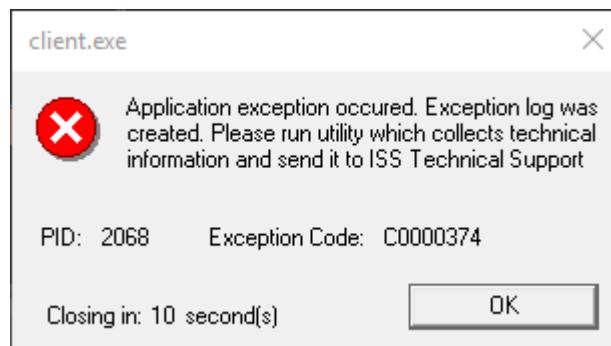


Figure 251. Informational message about system crash

- **Collect additional databases** – select this checkbox to collect additional information about SecurOS and installed intelligent Modules. All additional databases that are being used on this computer will be collected (see [DSAdmin Utility](#)).

Note. Additional information must be collected only by request of the Intelligent Security Systems Technical Support Team. In all other cases it is not required.

Report structure

The report contains the following folders and files:

- crashlogs folder – contains log-files of the crashes of the SecurOS or its components;
- cur folder – contains files with settings of the modules logging, program and scripts, xml-files of the integrated Cameras and Video Servers libraries, and also license key file key.iss;
- cur\securos.sqlite file – contains the copy of the SecurOS configuration, used by client;
- devices folder – contains binary log-file for the found problems of interaction with cameras;
- dumps folder – contains full or minimal dumps of the crashes of the SecurOS and/or its components;
- installer folder – contains SecurOS installer log-files;
- logs folder – contains SecurOS log-files;

Note. SecurOS' Modules log-files are stored in the ISS\Logs folder, path to which is specified in the %ProgramData% Environment Variable.

- logs\tomcat folder – contains Apache TomCat server log-files (WebConnect);
- logs\nginx folder – contains nginx server log-files (WebConnect);
- PostgresLogs folder – contains PostgreSQL log-files;
- System32 folder – contains Windows system libraries used by the SecurOS;
- TomCat folder – contains Apache TomCat server log-files (WebView);
- WindowsEventLogs folder – contains the Application and System Windows Logs (the Application.evtx and System.evtx files, respectively);
- DallasCode.txt file – contains information about codes of the installed hardware devices (Guardant);
- data.sql, videoi.sql and protocol.sql files – contain information from securos, fsindex and protocol databases, accordingly. In case the additional databases are collected (see [DSAdmin Utility](#)) other sql-files with appropriate names are included in the report;
- DxDiagInfo.txt file – contains information about system devices of the computer, where SecurOS is installed and utility was started;
- cluster.json file – contains information about configuration of the cluster, which given computer belongs to;
- integrators.txt file – contains list of the installed integrators and their versions that are stored in the C:\Program Files (x86)\ISS\Integrators folder;
- ISS_Config.reg file – contains information about the HKLM\SOFTWARE\ISS registry key;

- **modules.txt** file – contains list of the **dll**- and **exe**-files with their versions from the SecurOS folder;
- **netstat.txt** file – contains information about active connections of this computer at the moment you run the utility;
- **SystemInfo.nfo** file – contains general system information about computer where SecurOS is installed and given utility was started.

18.3.4 ISS Media Export Utility

Location:

<SecurOS root folder>\Backup.exe

Start menu:

Start → Programs → SecurOS → ISS Media Export Utility

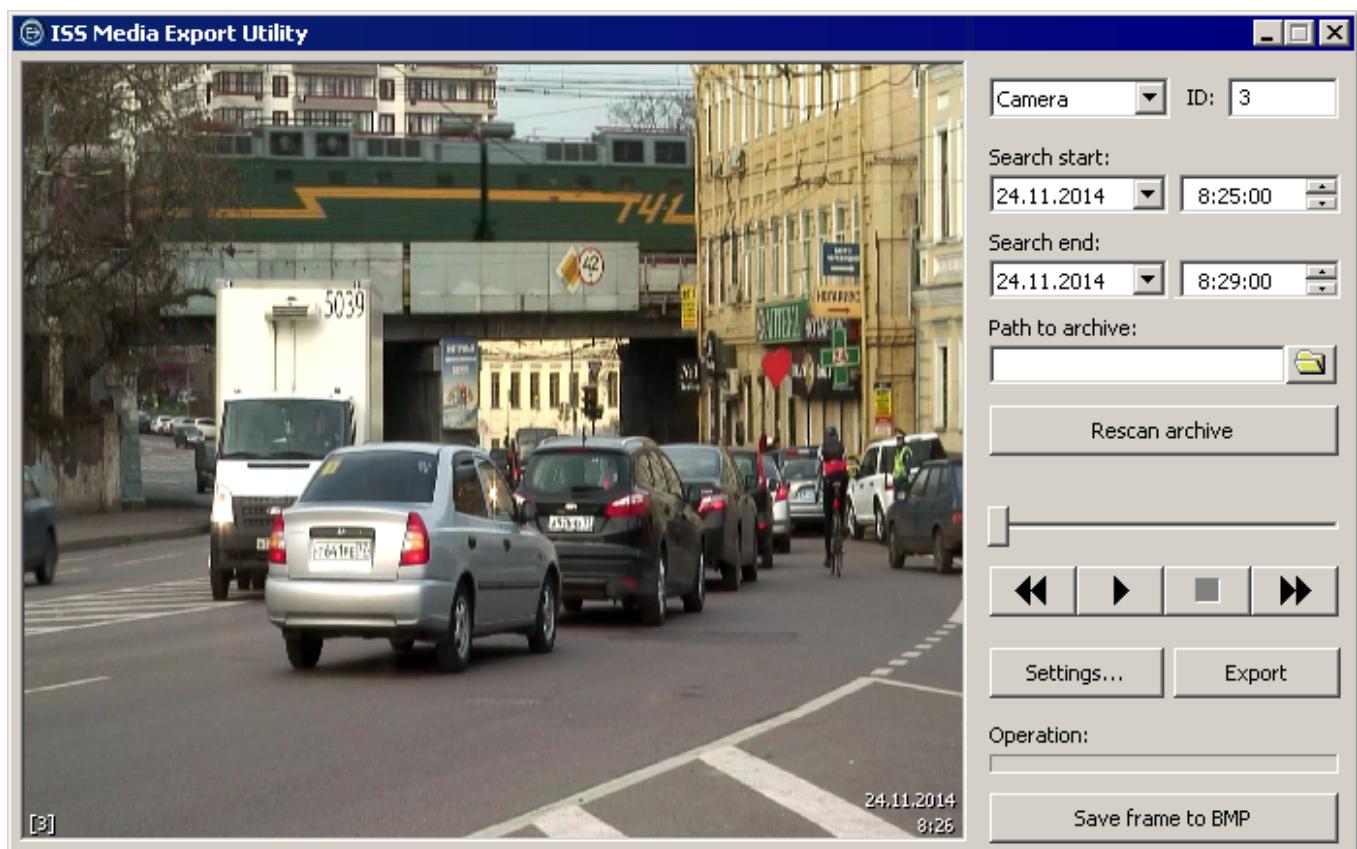


Figure 252. ISS Media Export Utility window

This utility (see figure 252) is used to playback and also export video and audio archives from ISS Native to AVI/ASF format, export a frame to BMP format and also export separate audio files, recorded with the help of a standalone (not associated to a camera) microphone.

Warning! This utility can only be used to export video/audio archives locally from video servers.

To export video:

1. Select the **Camera** in the archive source list and specify the ID of the *Camera* object.
2. Define the **Search start** and **Search end** for the archive search.

3. Click the **Path to archive** button and select the archive for export. To scan all logical drives leave the field blank.
4. Click the **Rescan archive** button to scan for media that fits the specified time range for the specified *Camera*.
5. When it is necessary to view archive, use the **Play/Stop** buttons to start and stop playback. Use the slider or the **Rewind/Forward** buttons to navigate through the selected time range.
6. If needed, change your selection by repeating steps **1 – 5**.
7. Define export settings (audio codec, output directory etc.) in the **Export Settings** dialog.
8. Click the **Export** button to start the procedure. The process may take some time depending on the length of the video and export settings.
9. While exporting is in progress, you can click the **Stop** button to stop the export at this point. The part that has already been exported will be saved as an AVI or ASF file.

Note. While playing or navigating through the archive, click the **Save frame to BMP** button to export a single video frame in BMP format. Files will be saved to the directory specified in the **Export Settings** dialog.

Warning! To playback "quick converted" video It is recommended to use the VLC media player.

To export audio, recorded with the help of standalone microphone:

1. Select the **Microphone** in the archive source list and specify ID of the *Microphone* object.
2. Define the **Search start** and **Search end** for the archive search.
3. Click the **Path to archive** button and select the archive for export. To scan all logical drives leave the field blank.
4. Click the **Rescan archive** button to scan for media that fits the specified time range for the specified *Microphone*.
5. Define export settings (audio codec, output directory etc.) in the **Export Settings** dialog.
6. Click the **Export** button to start the procedure. The process may take some time depending on the length of the audio and export settings.
7. While exporting is in progress, you can click the **Stop** button to stop the export at this point. The part that has already been exported will be saved as a AVI or ASF file.

Note. This utility is not intended to playback audio files.

18.3.4.1 Export Settings dialog

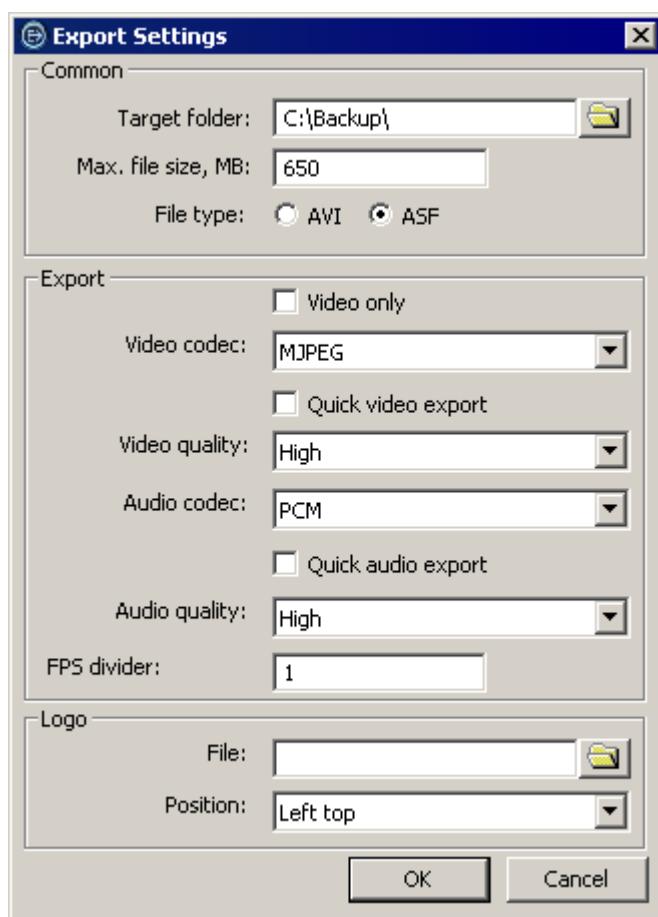


Figure 253. Export settings dialog window

Table 97. Export settings

Parameter	Description
Common	
Target folder	Path to a directory where output files will be saved. Type it manually or use the button on the right to open the Choose folder dialog.
Max. file size, MB	Use this option to split large output files to several smaller ones with the specified size in megabytes. Default value is 650 MB. Warning! Some media players do not support AVI-files greater than 2 GB.
File type	Select option corresponding to output file format (AVI or ASF).
Export	
Video only	Select the checkbox to export video only (without audio).
Video codec	Select video codec.

Parameter	Description
Quick video export	Select the checkbox to perform a quick video export. Quick video export can be performed only for archives created with H.263, H.264, MPEG-4 or MJPEG codecs. Notes: <ol style="list-style-type: none"> 1. Video codec, Video quality, FPS Divider, File and Position parameters will be ignored in the Quick video export mode. 2. If Quick video export is selected, but the conversion is not possible for some reason, then the parameters specified above will be used.
Video quality	Select required quality of the output video file.
Audio codec	Select audio codec.
Quick audio export	Select the checkbox to perform a quick audio export. Quick audio export can be performed only for archives created with GSM, PCM or ADPCM codecs. Notes: <ol style="list-style-type: none"> 1. Audio codec and Audio quality parameters will be ignored in the Quick audio export mode. 2. If Quick audio export is selected, but the conversion is not possible for some reason, then the parameters specified above will be used.
Audio quality	Select required quality of the output audio.
FPS divider	Set FPS divider parameter. Warning! Option works correctly only for video produced with no delta-frame algorithm. For example, MJPEG for IP cameras. In other cases, using this option can cause frame twitching and skipping.
Logo	
File	Select logo file name (PNG file format).
Position	Select logo position on the frame.

18.3.4.2 Command-line parameters

You can use the Media Export Utility (see [ISS Media Export Utility](#)) from the command-line and from batch files to automate the exporting process. When executed from command line, currently defined export settings will be used. To change these settings, open the Media Export Utility in normal (window) mode, setup export parameters, then close utility. Required parameters can also be set when launching utility from command line.

Media Export Utility command-line syntax (example contains only frequently used parameters):

```
backup.exe --out <out_file> --cam <camera_number> --from "<start_date_time>" --to "<end_date_time>" --span <span_size> --silent
```


Table 98. Command-line parameters

Parameter	Type	Description
Search parameters		
--cam	<number>	ID of camera from which video will be converted.
--from	<date>	Start date/time of the archive to export. Example: 19-02-05 00:00:00.
--to	<date>	End date/time of the archive to export. Example: 20-02-05 11:59:59 PM.
--frame		Used to export frame defined with --cam and --from parameters to .BMP image.
Search directory		
Warning! If --archive-folder or --archive-path parameters are not set then only the primary archive will be searched.		
--archive-folder		Long-term archive will be searched.
--archive-path	<absolute path>	Archive will be searched only in the specified directory.
Export parameters		
--out	<full filename>	Output filename include absolute path. For example, C:\export\out.avi.
--video-only		Export video without audio.
--container	<file type>	File type. Possible values: AVI or ASF.
--span	<number>/<string>	Span to fragments up to. Specify a number (value in MB) or reserved variables: DVD (4.7 GB for using DVD disk), or CD (650 MB for using CD disk).
--video-codec	<string>	Codec used to export video. Possible values: MJPEG, MPEG4.
--audio-codec	<string>	Codec used to export audio. Possible values: PCM, WMA, MP3.
--video-quality	<number>	Video quality. Number in range of [0; 100].
--audio-quality	<number>	Audio quality. Number in range of [0; 100].
--raw-video		Quick video export.
--raw-audio		Quick audio export.
--fps-divider	<number>	FPS divider. Number in range of [1; 100].

Set `--silent` parameter to start utility in silent mode.
Set `--help` parameter to display list of parameters.

Example 1:

```
backup --cam 1 --from "27-12-06 18:36:42" --to "28-12-06 22:43:12" --span 2
```

Description: export video archive of camera 1 for the defined period spanning to fragments up to 2 Mb.

Example 2:

```
backup --out "C:\custom path\pwnage.avi"  
--from "27-12-06 18:36:42" --to "28-12-06 22:43:12" --span cd
```

Description: export video archive for the defined period spanning to fragments up to CD disk size (650 MB).

Note. Camera number and other settings are taken from the utility configuration.

18.3.5 DSAdmin Utility

This utility is intended to store/change database connection strings for the following databases:

- **SecurOS settings database.** This database stores system object settings. Database name is specified when installing database. By default the `securos` name is used.
- **SecurOS events database.** This database stores information about events, that occurred within system. This database is created automatically when system installing with the name of `protocol`.
- **SecurOS video archive database.** This database stores information about registered alarms and specified archive bookmarks. This database is created automatically when system installing with the name of `fsindex`.
- Any other additionally installed database.

Location:

<SecurOS root folder>\dsadmin.exe

Appearance of the main window is represented on figure 254.

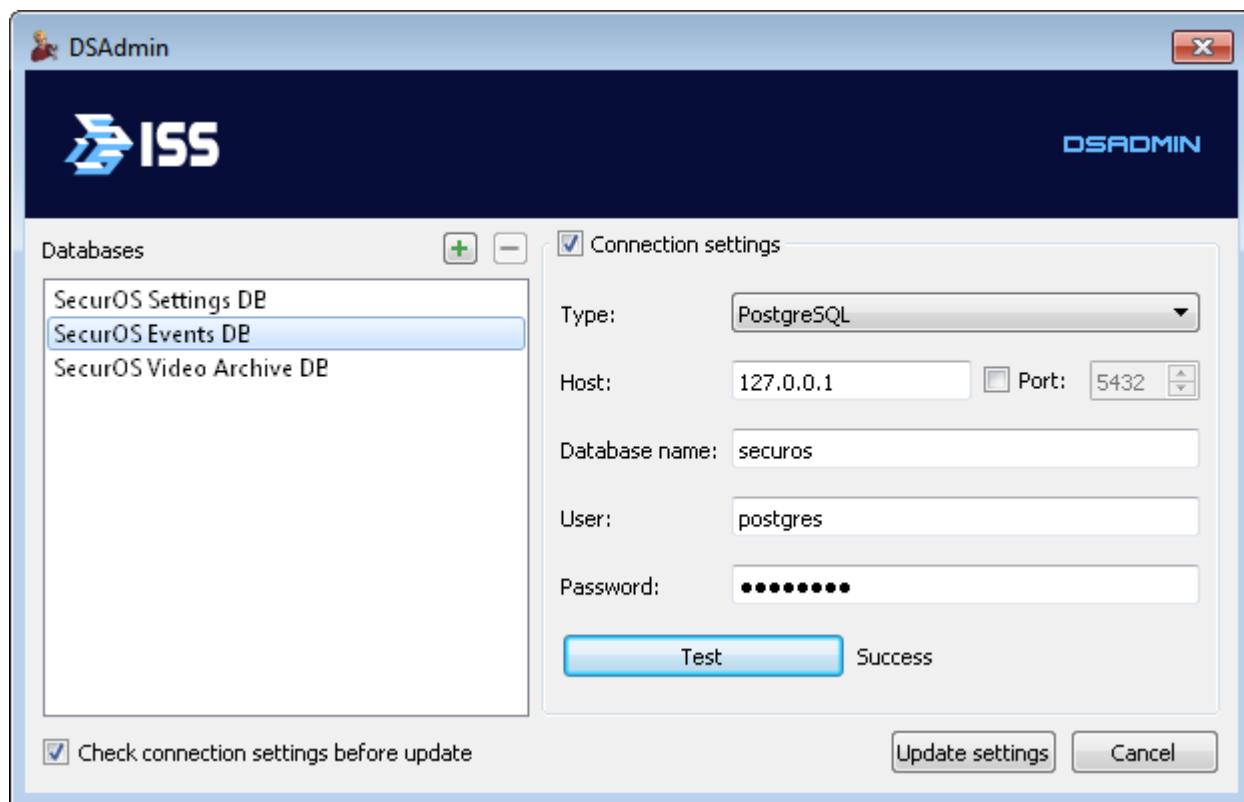


Figure 254. DSAdmin Utility window

Table 99. DSAdmin Utility parameters

Parameter	Description
Databases	This list always contains the following databases: <ul style="list-style-type: none"> • SecurOS settings database — mandatory database, is used always. • SecurOS events database — mandatory database, but can not be used depending on utility settings. By default it is used. • SecurOS video archive database — mandatory database, but can not be used depending on utility settings. By default it is used. Besides mentioned above, this list can contain any number of additionally installed databases.
Databases list	
Connection settings	

Parameter	Description
Connection settings	<p>This flag indicates if database is used. It is displayed only for two main databases: SecurOS events database and SecurOS video archive database. Otherwise is not displayed. If not selected, then connection parameters are disabled, connection between SecurOS and database is broken. If these settings are saved, then all connection parameters are set to null.</p> <hr/> <p>Notes:</p> <ol style="list-style-type: none"> 1. This flag is taken into account when the ISS System Report Utility (ISSInfo) is executed. If Collect additional databases option is selected, data for only databases that are used will be collected. 2. If additional databases are installed, then ISS System Report utility will collect similar data for those ones that are included in the Databases list (see above).
Type	<p>Database type. Required parameter. Possible values:</p> <ul style="list-style-type: none"> • PostgreSQL (is the default value); • SQL Server.
Host	Name or IP address of the server where database is installed. Required parameter.
Port	Port number for database connection. Optional parameter. If selected, this port is used when connecting. If not selected, the 5432 port is used for connection (default value).
Database name	Name of the database specified when installing. Required parameter.
User	Name of the database's administrator account specified when installing database. Required parameter.
Password	Password of the database's administrator account specified when installing database. Required parameter.
Test (button)	Click the button to check database connection with specified connection parameters. If connection established, then the Success result is displayed to the right of the button. Otherwise the Failed result is displayed. In this case check specified connection parameters and repeat test.
Common parameters	
Check connection settings before update	Deselect this option if checking connection with all specified databases before update is not required.
Update settings (button)	Click this button to apply all changes and exit.
Cancel (button)	Click this button to discard all changes and exit.

To add connection to the additional database to the list do the following:

1. Click the button above the **Databases** block.
2. A new entry will appear in the **Databases** list (see Figure 255).

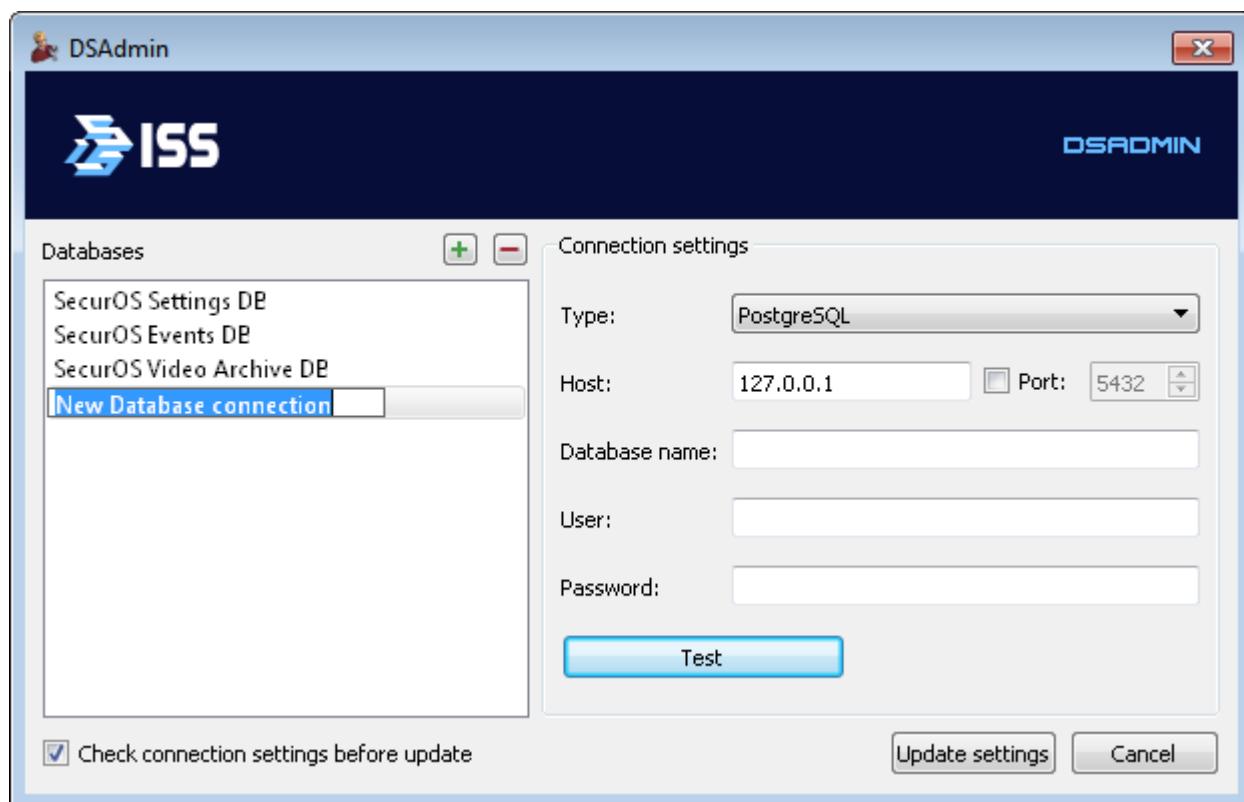


Figure 255. Adding new database

3. Specify name of the new database. Press the **Enter** key.
4. Specify required parameters in the **Connection settings** block, then click the **Test** button to check the connection.
5. If checking result is successful, then click the **Update settings** button to save the changes and exit.

To delete connection to the additional database to the list do the following:

1. In the **Databases** block click the additional database entry that should be deleted from the list.
2. Click the button above the **Databases** block. Connection to the selected database will be deleted from the list. At the same time:
 - physical database is not removed;
 - software product that uses removed database keeps working correctly.

Note. Only user created connection to an additional database can be deleted.

18.3.6 Database Update Utility

This utility is intended for setting up and updating the SecurOS database, where SecurOS object settings are stored (securos database). Modification is performed with the help of the securos.dbi file, where description of the actual database structure is stored.

Location:

<SecurOS root folder>\idb.exe

Appearance of the main window is represented on figure 256.



Figure 256. ISS Database Update Utility window

Table 100. Database Update Utility parameters

Parameter	Description
Connection settings	

Parameter	Description
Type	<p>Database type. Required parameter. Possible values:</p> <ul style="list-style-type: none"> • PostgreSQL (is the default value); • SQL Server; • SQLite. <hr/> <p>Note. SQLite value is used when SecurOS Client application starts on separate Computer in order to provide creation and updating local SecurOS database, that must be implemented on this Computer as .sqlite file.</p>
Host	Name or IP address of the server where database is installed. Required parameter.
Port	Port number for database connection. Optional parameter. If selected, this port is used when connecting. If not selected, the 5432 port is used for connection (default value).
Database name	Name of the database specified when installing. Required parameter.
User	Name of the database's administrator account specified when installing database. Required parameter.
Password	Password of the database's administrator account specified when installing database. Required parameter.
Test (button)	Click the button to check database connection with specified connection parameters. If connection established, then the Success result is displayed to the right of the button. Otherwise the Failed result is displayed. In this case check specified connection parameters and repeat test.
Database descriptor path	Path to the securos.dbi file. Default value is <SecurOS_root_directory>\securos.dbi. It is possible to specify path manually or with the help of the Select button (see below).
Select (button)	Click the button to choose folder, where custom .dbi file is located. Specify path to the file in the standard file manager window.
Compact database	Select this checkbox to perform standard PostgreSQL's VACUUM operation.
Struct update redundant tables (drop)	Select this checkbox to delete obsolete database tables completely.
Update database (button)	Click this button to update database in accordance with the specified parameters and to exit.

Parameter	Description
Cancel	Click this button to discard the changes and exit.

18.3.7 ISS SecurOS Registration Files Editor

This utility is used to describe SecurOS object types – their properties, characteristics and behavior within the system.

Additional Information

Type of the object within SecurOS means unique char identifier of the object class that is used within program code. SecurOS object type can not be changed.

Each property, characteristic or object type behavior rule within SecurOS is specified with the help of appropriate component of the object type description. Components of the object type description are used to represent object within appropriate interfaces, for example, within operator's interface of the *Media Client*, in the *Event Viewer's* log-files, on the *Map*, etc.

By default, descriptions of the object types existing within SecurOS are created in accordance to the rules defined by software developer. When adding a new object types, for example, during SecurOS integration with the third-party systems or equipment, their own object type descriptions can be created for newly added objects with the help of this utility.

Location:

<SecurOS root folder>\ddi.exe

To start working with object type descriptions one should load and open appropriate *securos_xx.ddi* file, located in the SecurOS root folder, where xx – ID of the description language, for example, *fr* (french).

Appearance of the main utility window when description file is opened is represented on figure 257.

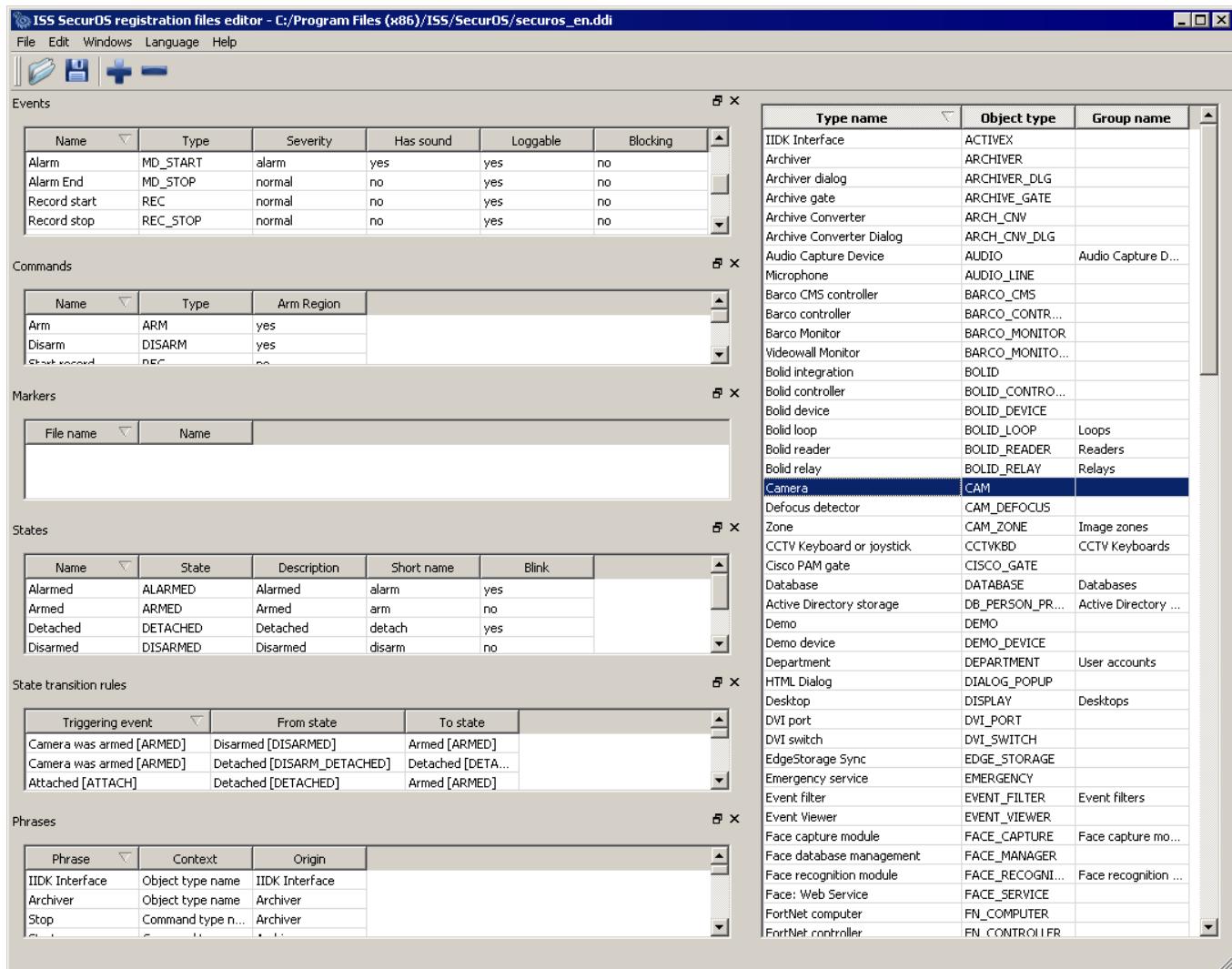


Figure 257. ISS SecurOS Registration Files Editor Main Window

List of registered object types is displayed on the right area of the window as a table:

- **Type name** — name of the object type (char). This name is used to represent object in the *Object Tree*, on the *Map*, in the *Media Client* and *Event Viewer* user interfaces, etc. Variable parameter;
- **Object type** — unique type of the object. Is used to represent object class instance. Variable parameter;

Note. It is necessary to change object type only if it changed inside software source code. Otherwise changes will not be applied to the system, but at the same time will be saved in the description file.

- **Group name** — name of the grouping object in the SecurOS *Object Tree*. Variable parameter.

To view description click required object in the list.

In the left area of the main window the following information concerning selected object type will be displayed (by default all available information is displayed):

- **Events** window — contains a table of system events that can be generated by selected object type;
- **Commands** window — contains a table of commands that can be used to control selected object type;

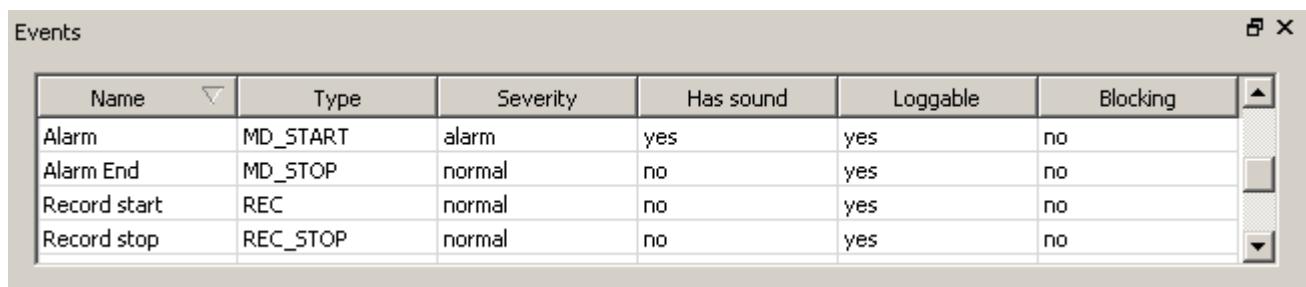
- **Markers** window – contains a table that is intended for object icon file name definition. Object icons displayed in the *Map Window* are specified in the object source code. Appropriate .png graphic files are located in the skins_common folder of the SecurOS root directory;
- **States** window – contains a table of all possible states for selected object type.;
- **State transition rules** – contains a table of transmission rules from one state of the object to another. Transmission rules control initial and final states that selected object has upon certain event coming. Initial event, initial state and final state are in the table;
- **Phrases** – contains names that are used as object captions displayed in all interfaces (in the *Object Tree*, in the *Map Window*, in the *Media Client* and *Event Viewer* interfaces, etc. Also contains phrases used in information messages displayed in the own interface windows of the objects (for example, in the *Archiver* window).

Mentioned above windows can be displayed or hidden with the help of **Windows** menu in the main utility window.

To change field value within any window double-click this field, then select required value or type it manually.

Other components of the **Menu bar** and **Toolbar** in the main utility window are intuitively understandable and not considered within this manual.

Events Window



The screenshot shows a Windows-style dialog box titled "Events". Inside, there is a table with columns: Name, Type, Severity, Has sound, Loggable, and Blocking. The table contains four rows of data:

Name	Type	Severity	Has sound	Loggable	Blocking
Alarm	MD_START	alarm	yes	yes	no
Alarm End	MD_STOP	normal	no	yes	no
Record start	REC	normal	no	yes	no
Record stop	REC_STOP	normal	no	yes	no

Figure 258. Events window

In this window the following parameters of the object type *Events* are specified:

- **Name** – name of the event that will be displayed in the *Event Viewer* interface;
- **Type** – unique event ID.

Note. It is necessary to change object type only if it changed inside software source code. Otherwise changes will not be applied to the system, but at the same time will be saved in the description file.

- **Severity** – severity of the event. Defines how this event will affect the system and need of operator intervention when it occurs. Possible values:
 - normal – event that does not require operator attention. Such event is highlighted in *Event Viewer* in blue;
 - informational – event that requires additional operator attention. Such event is highlighted in *Event Viewer* in white;
 - alarm – event that requires intervention of operator or technical support expert. Such event is highlighted in *Event Viewer* in red.

- **Has sound** – event attribute that indicates necessity to play sound when events occurs. It makes sense only if sound is defined in the source code of the object;
- **Loggable** – indicates necessity to save record relevant to occurred event into the protocol database (system events protocol). Possible values:
 - yes – message about local events will be saved into the database;
 - no – message about local events will not be saved into the database.
- **Blocking** – indicates necessity to transfer message about local event to all computers within network. Possible values:
 - yes – message about local events will be transferred into the network;
 - no – message about local events will not be transferred into the network.

Commands Window

Name	Type	Arm Region
Arm	ARM	yes
Disarm	DISARM	yes
Start record	REC	no

Figure 259. Commands window

In this window the following parameters of the object type *Commands* are specified:

- **Name** – command name;
- **Type** – unique command ID that is defined inside object source code;
- **Arm Region** – this parameter is not used in current version of the utility.

Markers Window

File name	Name
rele_light	Light
rele_lock	Lock
rele_woofer	Woofer

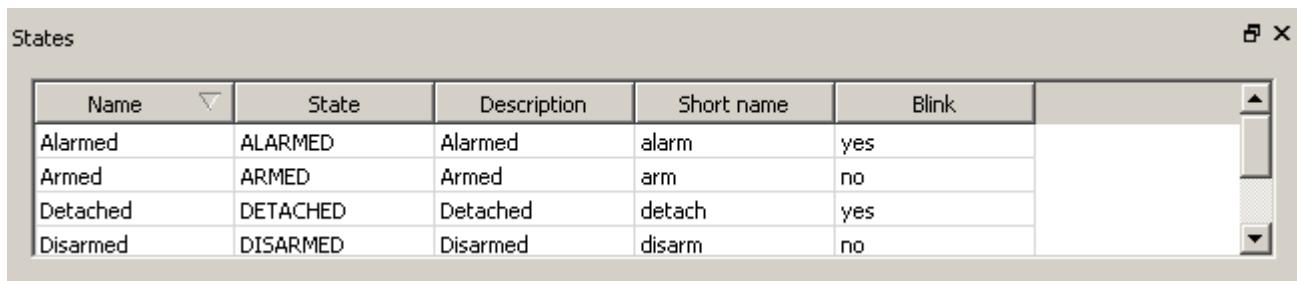
Figure 260. Markers window

In this window the following parameters of the object *Icons* that are displayed in the *Map Window* are specified:

Warning! Parameters of the icons make sense only for *Sensor* and *Relay* objects.

- **File name** – value that is used within script to create the final name of the image file;
- **Name** – possible value from the list of values of appropriate parameter in the *Sensor* or *Relay* object settings window.

States Window



The States window displays a table of four rows representing different object states:

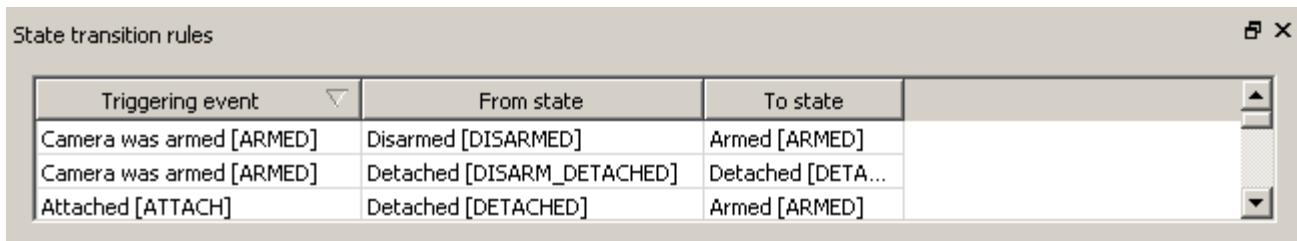
Name	State	Description	Short name	Blink
Alarmed	ALARMED	Alarmed	alarm	yes
Armed	ARMED	Armed	arm	no
Detached	DETACHED	Detached	detach	yes
Disarmed	DISARMED	Disarmed	disarm	no

Figure 261. States window

In this window the following parameters of the object type *States* are specified:

- **Name** – name of the state. This name is displayed, for example, in the *Map Window*;
- **State** – unique state ID;
- **Description** – state text description;
- **Short name** – value that is used within script to create the final name of the image file. This image will be used in the *Map Window* to indicate appropriate object state;
- **Blink** – additional mark of the state. Controls object icon blinking in the *Map Window* when object gets a given state. Possible values:
 - yes – icon is blinking;
 - no – icon is not blinking.

State transition rules Window



The State transition rules window displays a table of three rows defining transitions between states:

Triggering event	From state	To state
Camera was armed [ARMED]	Disarmed [DISARMED]	Armed [ARMED]
Camera was armed [ARMED]	Detached [DISARM_DETACHED]	Detached [DETA...]
Attached [ATTACH]	Detached [DETACHED]	Armed [ARMED]

Figure 262. State transition rules window

The following parameters of the rules are specified in this window:

- **Triggering event** – ID of the event that initiates transition;
- **From state** – ID of initial state for transition upon **Triggering event**;

Warning! If leave blank then transition will be done from any state.

- **To state** – ID of the final object state.

Phrases Window

Phrase	Context	Origin
IIDK Interface	Object type name	IIDK Interface
Archiver	Object type name	Archiver
Stop	Command type n...	Archiver

Figure 263. Phrases window

In this window are specified the *Phrases* that are used as an object captions and used in information messages displayed in the own object interface windows. Contains the following fields:

- **Phrase** – a phrase that will be used to describe an object within main SecurOS interface elements (*Object Tree*, *Map Window*, *Event Viewer* etc.) or phrase for information message used in the own object interface window;
- **Context** – phrase usage context;
- **Origin** – source of the phrase (i.e. **Object type**).

Note. Changing the **Phrase** will cause automatic changing of the **Origin** field and the **Object type** field in the right window.

Warning! Once file was changed one should save the changes and restart SecurOS, otherwise changes will not be applied.

18.3.8 ISS Server Role Manager Utility

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*, *SecurOS Professional*.

The utility is intended to reassign one of the SecurOS *Peripheral Servers* as *Configuration Server* when current *Configuration Server* can not be used anymore.

Location:

<SecurOS root folder>\ServerRoleManager.exe

To reassign current *Configuration Server* do the following:

Warning! The *Guardant* hardware key must be moved from current *Configuration Server* to that *Peripheral Server*, which will serve as a new *Configuration Server* (see [Guardant Key Installation](#)). Otherwise, system can't be started on the new *Configuration Server*.

1. Launch utility on that *Peripheral Server*, which will serve as *Configuration Server*.
2. In the utility window select the **Configure the computer as a Configuration Server** (see Figure 264).

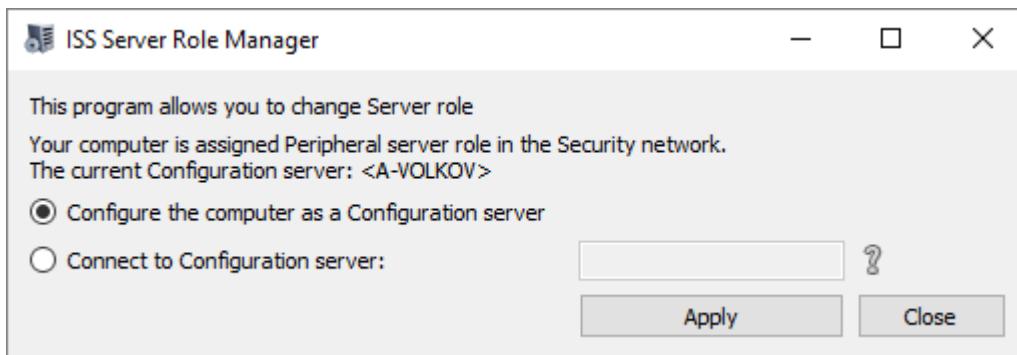


Figure 264. Specifying new Configuration Server

Note. The **current Configuration server** string displays name of the computer, which is being reassigned.

3. Click the **Apply** button.
4. Restart SecurOS.
5. Sequentially launch utility on each of the *Peripheral Servers* and do the following:
 - In the utility window select the **Connect to Configuration Server** (see Figure 265).

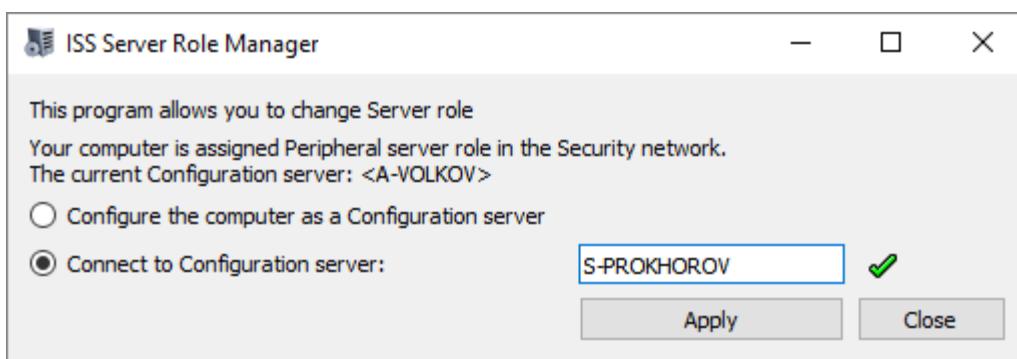


Figure 265. Connect to Configuration Server option

Note. The **current configuration** string displays name of the computer, which is being reassigned.

- In the text box fill in the name of the computer, which is assigned a new *Configuration Server*.

Note. If the name of new *Configuration Server* is specified correctly and computer is available within SecurOS network, the mark will be displayed on the right of the text box. Otherwise the mark will be displayed.

- Click the **Apply** button.
- Restart SecurOS.

18.3.9 Server Control Agent Utility

Using this utility, one can perform the following operations:

- Start/Stop SecurOS *Server part*;
- Obtain additional information about SecurOS *Server part* launching error;

- Start/Stop SecurOS *Client part*;
- Manage SecurOS Control Service.
- Launching **ISS System Report (ISSInfo)** utility.

Location:

<SecurOS root folder>\ServerControlAgent.exe

Utility is launched automatically when OS is started. After utility is started its icon is displayed in the system tray (see Figure 266).

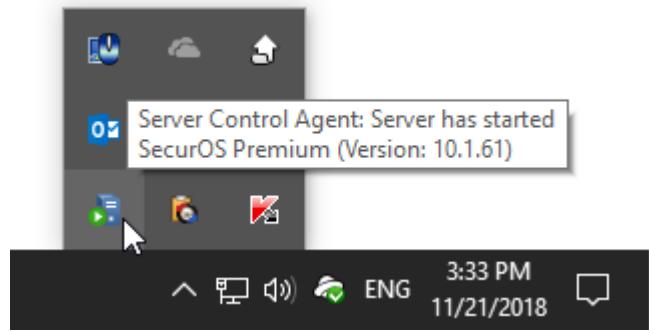


Figure 266. Server Control Agent icon in system tray

Note. If utility has been shut down one can launch it from **Start** menu (**Programs** → **SecurOS** → **Server Control Agent**).

Application icon displays current server state:



— server is started;



— server is stopped;



— server is crashed.

When mouse pointer is placed over the icon, then the hint that shows server current state, SecurOS edition and version number is displayed.

Control is performed with the help of utility context menu (see Figure 267), that contains the following commands:

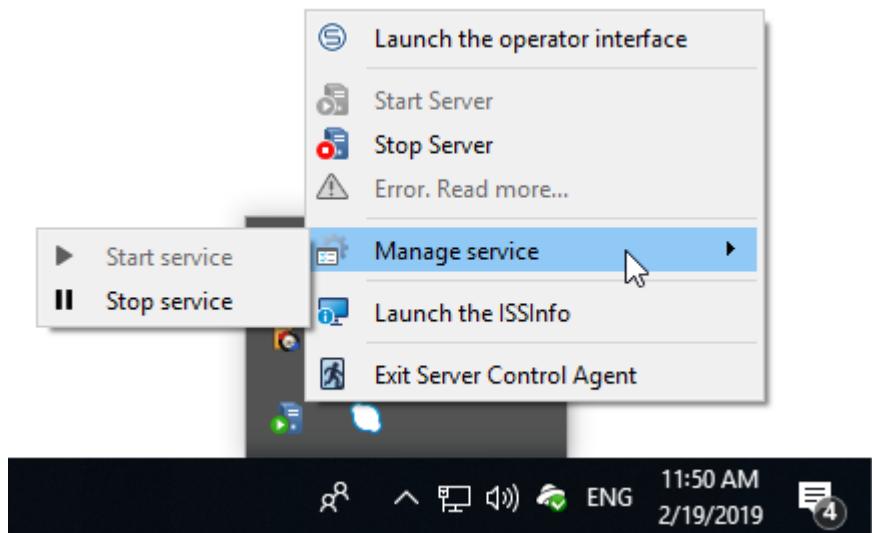


Figure 267. Utility context menu

- **Launch the operator interface** – launch SecurOS *Client part* on given computer;
- **Start Server** – start SecurOS *Server part*;
- **Stop Server** – stop SecurOS *Server part*;
- **Error. Read more...** – display detailed information about *Server part* launching error;
- **Manage service** – change the state of the SecurOS Control Service:
 - **Start service**;
 - **Stop service**.
- **Launch the ISSInfo** – launch the [ISS System Report \(ISSInfo\)](#) utility;
- **Exit Server Control Agent** – shut down utility.

18.3.10 Video Archive Index Repair Utility

This utility is designed to recover damaged or create missing index files of the SecurOS video archive including the archive from cameras with an associated microphone.

Location:

<SecurOS root folder>\MediaIndexRepairer.exe

Utility is implemented as console application, to call which the following syntax of command prompt is used:

```
MediaIndexRepairer.exe    [--path <arg>]    [--camId <arg>]    [--type <arg>]
[--user <arg>] [--pass <arg>] or
MediaIndexRepairer.exe [--help], where:
```

- **--path <arg>** – recreate index files located in the specified folder. Required parameter. Possible arguments:

<Full_path_to_the_archive_root_folder> – recreate index files for the whole archive, or

<"Full_path_to_the_archive_folder_for_an_hour"> – recreate index file for the archive created for an one hour;

Warning!

1. Folder name in the command prompt is case sensitive.
2. When specifying path to the folder that contains archive for an one hour, it is necessary to use the "" characters to screen space included in the file name (see example below).
3. A network folder can be specified. To provide an access to the network folder it is necessary to specify the user name and password (see below).

- `--camID <arg>` – recreate all index files for the archive that was created by camera with specified ID. Optional parameter. If not specified, then index files for archives created by cameras with any ID will be recreated.

This parameter is not used without `--path <arg>`;

- `--type <arg>` – type of the files for index repair. Possible values:
`all` – re-indexing video- and audio archives. Default value;
`video` – re-indexing video archive only;
`audio` – re-indexing audio archive only;
- `--user <arg>` – user and domain name (if exists) to provide an access to the network folder. Optional parameter;
- `--pass <arg>` – user password to provide access to the network folder. Optional parameter;
- `--help` – display help information for the command.

Examples:

- `MediaIndexRepairer.exe --path D:\VIDEO` – recreate all index files of the video and audio archive that was created by all cameras and saved in the `D:\VIDEO` folder;
- `MediaIndexRepairer.exe --path "D:\VIDEO\24-08-15 08" --camId 15` – recreate index file of the archive that was created on August 24 2015 in 08:00 a.m. till 09:00 a.m. time interval by camera with ID 15 and saved in the `D:\VIDEO\24-08-15 08` folder;
- `MediaIndexRepairer.exe --path \\server\VIDEO --user OFFICE\admin --pass password` – recreate all index file of the archive created by all cameras and saved in the `\server\VIDEO` network folder.

To simultaneously process archive with different parameters use several instances of the application. In this case archives specified in the parameters of each instance will not intersect by date/time and/or camera ID.

Warning!

1. Re-indexing of the large volume archives can take considerable time (hours).
2. To work with appropriate archives it is necessary to restart SecurOS once index files are recreated.

18.3.11 Outdated Audio Archive Updater Utility

This utility is designed to do the following:

- To convert SecurOS audio archive of an old format to the new one for cameras with an associated microphone;
- To automatically delete old SecurOS audio archive and create the index file when the conversion

process is finished.

Warning!

1. Conversion of the large volume archives may take considerable time (hours).
2. It is required to restart SecurOS to work with the new audio archive.

Location:

<SecurOS root folder>\AudioArchiveConverter.exe

Utility is implemented as console application, to call which the following syntax of command prompt is used:

AudioArchiveConverter.exe [--path <arg>] [--user <arg>] [--pass <arg>] or
AudioArchiveConverter.exe [--help], where:

- --path <arg> – convert the audio archive located in the specified folder. Required parameter.
Possible arguments:
 - <Full_path_to_the_archive_root_folder> – convert audio files for the whole archive, or
 - <Full_path_to_the_archive_folder_for_an_hour> – convert audio files for the archive created for one hour, or
 - <Full_path_to_the_archive_file> – convert only the specified file.

Warning!

1. Folder name in the command prompt is case sensitive.
2. When specifying path to the folder that contains archive for an one hour, it is necessary to use the "" characters to screen space included in the file name (see example below).
3. A network folder can be specified. To provide an access to the network folder it is necessary to specify the user name and password (see below).

- --user <arg> – user and domain name (if exists) to provide an access to the network folder.
Optional parameter;
- --pass <arg> – user password to provide access to the network folder. Optional parameter;
- --help – display help information for the command.

Examples:

- AudioArchiveConverter.exe --path D:\VIDEO – convert all audio files of archive that was created by all cameras and saved in the D:\VIDEO folder;
- AudioArchiveConverter.exe --path \\server\VIDEO --user OFFICE\admin --pass password – convert all audio files of the archive created by all cameras and saved in the \\server\VIDEO network folder.
- AudioArchiveConverter.exe --path "D:\VIDEO\12-04-19 12" – convert all audio files of the archive that was created on August 12 2019 in 12:00 PM a.m. till 1:00 PM a.m. time interval by camera with ID 15 and saved in the D:\VIDEO\12-04-19 12 folder;
- AudioArchiveConverter.exe --path "D:\VIDEO\12-04-19 12\4009641.w05" – convert the audio file of the archive that was created on August 12 2019 at 12:40:09.641 PM by camera with ID 5 and saved in the D:\VIDEO\12-04-19 12 folder;

To simultaneously process audio archive with different parameters use several instances of the application. In this case audio files specified in the parameters of each instance will not intersect by date/time and/or camera ID.

Conversion results:

- When converting a folder, all the old audio files are removed. They will replaced with audio files of a new format, and the index file will be created.
- When converting a single file, the audio file of a new format will be created. The original file will not be removed. The index file for the new audio archive will not be created.

18.3.12 Certificate Generator Utility

The utility is intended for creation trial self-signed SSL certificates. Such certificates can be used to check and demonstrate capabilities of the digital signature (see [Digital Signature](#)) and to work via secured HTTPS protocol for such modules as *Mobile Application Server* (see [SecurOS Mobile Quick Start Guide](#)), *AutoMobile Server* (see [SecurOS AutoMobile User Guide](#)), *Rest API*, etc.

Warning! Certificates created with the help of the utility are intended solely for demonstration and commissioning purposes.

Location:

<SecurOS root folder>\CertificateGenerator.exe

Appearance of the main window is represented on Figure 268.

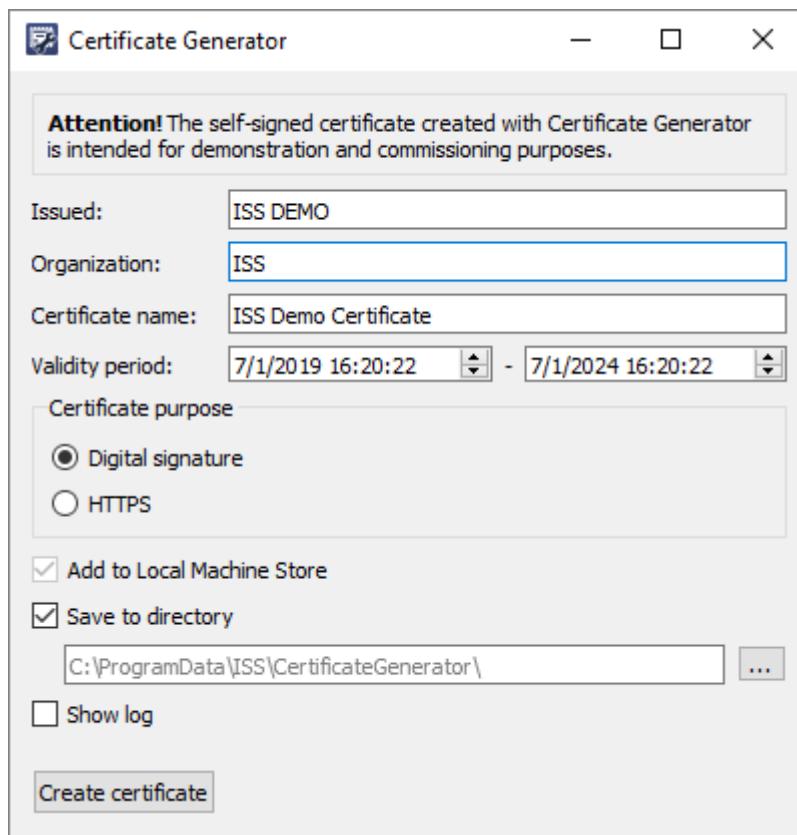


Figure 268. Certificate Generator Utility window

To create certificate do the following:

1. Fill in the window fields:

- **Issued:** this value will be displayed in the **Issued by** and **Issued to** properties of the certificate;
 - **Organization:** this value will be displayed in the **Organization** property of the certificate;
 - **Certificate name:** this value will be displayed as the name of the certificate;
 - **Validity period:** certificate validity period.
2. Choose certificate purpose:
- **Digital signature:** certificate will be used for digital signature.
 - **HTTPS:** certificate will be used to provide secured connection. This option is enabled only when utility is run as administrator.
3. Choose where to install or save the certificate:
- To make the certificate trusted on the given computer select the **Add to Local Machine Store** checkbox (default value).
 - To save the certificate to the specified directory select the **Save to directory** checkbox. To specify the path enter it manually or use file manager. When saving the created certificate it also will be installed to the local machine storage. Saving the certificate to a separate directory allows further to install and use it on different computers within the SecurOS network. For example, it is necessary to install such certificate on each computer of the cluster to provide working of the pointed above modules when using SecurOS in the cluster configuration.

Warning! The options for choosing a place to install or save a certificate are available only when running the utility as administrator.

4. Select the **Show log** checkbox to view detailed information about certificate creation process.
5. Click **Create certificate** button to create certificate with specified parameters.

18.3.13 AuditClient Utility

This functionality is available in the following editions: *SecurOS Monitoring & Control Center*, *SecurOS Enterprise*, *SecurOS Premium*.

The utility is intended to obtain the SecurOS user actions audit data. This data is stored in special audit databases located on each SecurOS *Video Server* and complement each other. Queries are addressed only to the database of the currently connected *Video Server*. Audit data from several *Video Servers* can be obtained when connecting to each of them sequentially. If the system is configured with the help of the **dsAdmin** utility (see [DSAdmin Utility](#)) so the audit data from all *Video Servers* of the network is saved into the single database, then aggregated audit data can be obtained in one utility session.

Audit data is retrieved accordingly to the query parameters specified by the user in the utility settings. Query can be executed both with the standard and custom parameters. In the latter case the query can be saved as a search template.

Location:
<SecurOS root folder>\audit_client.exe

To connect to the audit server when starting the utility, one must log in to SecurOS (see Figure [269](#)).

Warning! Only SecurOS *User* with the **Allow to audit system** checkbox selected in the *User Rights* object settings can authorize and connect to the audit server (see [User Rights](#)). Otherwise, connection to the audit server is not possible.

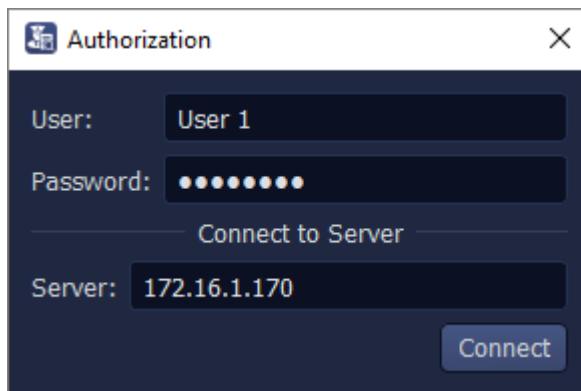


Figure 269. AuditClient Utility. Authorization Window

The window contains the following fields:

- **User/Password** – name and password of the SecurOS *User* or OS user (see [Active Directory / LDAP](#)) who is allowed to audit the system.
- **Server** – IP address or DNS name of the SecurOS *Video Server* where the audit database is located. When connecting locally one can use 127.0.0.1 or localhost values.

In case of successful authorization and connection to the audit server, the main utility window will be available (see Figure 270).

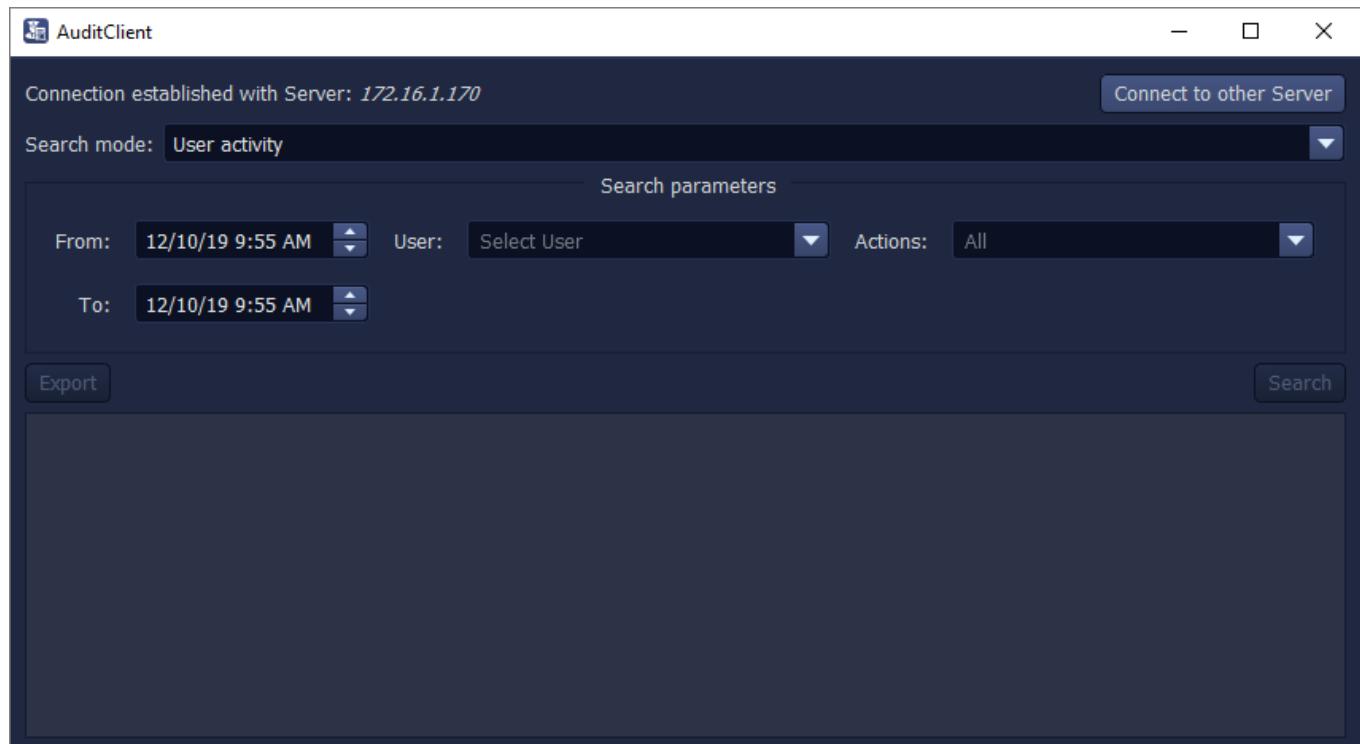


Figure 270. AuditClient Utility Main Window

At the top of the window the **Search parameter setting form** is located. It contains the following controls:

- **Connection established with Server** – information field where IP address or DNS name of the

connected audit server is displayed;

- **Connect to other Server** (button) – click this button to connect to other audit server;
- **Search mode** – select search mode:
 - User activity – is used to request all user actions, for which an audit is provided;
 - Configuration & object's mode changes – is used to request user actions related to changing object settings, changing the object's operating mode and archive recording mode;
 - Access to video – is used to request user actions related to viewing live or archive video;
 - PTZ Control – is used to request user actions related to PTZ control;
 - Video export – is used to request user actions related to video export;
 - Work with Auto Module – is used to request user actions performed when working with SecurOS Auto;
 - Advanced search – is used to create complex queries if none of the above query modes is suitable for obtaining the required data;
 - Search mode template – this mode is available if at least one search template is saved in the system. In this case, the name of the saved search template is displayed in the list of search modes. For the details see [Working with Search Templates](#).
- **Search parameters** (block of parameters depending on selected search mode):
 - From – date and time of the beginning of the search period, in date and time format of the OS;
 - To – date and time of the end of the search period, in date and time format of the OS;
 - User – select SecurOS *User* to analyze his actions in the system. This list contains only those users whose actions are saved in the audit database at the moment of connection to the audit server;
 - Actions – select user actions that must be analyzed;
 - Object Type – select type of the object under which an actions have been performed;
 - ID – identifier of the object of selected type;
 - Camera ID – *Camera*'s identifier;
 - LP number – license plate number with which any operations have been performed when working with SecurOS Auto Module;
 - Users – select users whose actions must be analyzed;
 - Object Type – select type of the object under which an actions have been performed;
 - Advanced – select this checkbox to set search parameters manually. For more information about creating custom queries, see the [Advanced search](#) section;
- **Export** (button) – click this button to export search results. For the details see the [Exporting Results](#) section below;
- **Search** (button) – click this button to start searching with specified parameters;
- **Buttons** (available only in Advanced search mode or when working with the previously created search templates. For the details see the [Working with Search Templates](#) section):
 - **Remove Template** – remove current template from the search modes list;
 - **Save as Template** – save specified set of parameters as search template for further use.

At the bottom of the window the search results table is located (see Figure 271). Structure of this table also depends on the selected search mode.

Warning! Data in the search results table is not dynamically updated. That means only audit data that matches the specified query time interval is displayed, even if new user actions are being registered in the system. To update displayed data one must execute a new request taking into account the changed time interval.

The screenshot shows the AuditClient application window. At the top, it displays 'AuditClient' and the connection status 'Connection established with Server: 172.16.1.170'. There is a 'Connect to other Server' button. Below this is a search bar with 'Search mode: User activity'. Underneath the search bar are 'Search parameters' fields for 'From' (11/10/19 9:55 AM), 'User' (User1), 'Actions' (All), and 'To' (12/10/19 9:55 AM). On the left, there are 'Export' and 'Search' buttons. The main area is a table with the following columns: Time, User, Computer, Action, Object, Interval, and Comment. The table contains five rows of data, all from Wednesday, November 27, 2019, at 9:55 AM, performed by User1 on S-PROKHO... computer. The actions listed are Watch live video, Setup, Watch live video, Watch live video, and Login.

Time	User	Computer	Action	Object	Interval	Comment
Wednesday, November 27, 2019 09:55:00	User1	S-PROKHO...	Watch live video	Camera 8 [8]	Wednesday, November 27, 2019 09:55:00 - Wednesday, November 27, 2019 09:55:00	
Wednesday, November 27, 2019 09:55:00	User1	S-PROKHO...	Setup	Camera 7 [7]	Wednesday, November 27, 2019 09:55:00 - Wednesday, November 27, 2019 09:55:00	
Wednesday, November 27, 2019 09:55:00	User1	S-PROKHO...	Watch live video	Camera 8 [8]	Wednesday, November 27, 2019 09:55:00 - Wednesday, November 27, 2019 09:55:00	
Wednesday, November 27, 2019 09:55:00	User1	S-PROKHO...	Watch live video	Camera 8 [8]	Wednesday, November 27, 2019 09:55:00 - Wednesday, November 27, 2019 09:55:00	
Wednesday, November 27, 2019 09:55:00	User1	S-PROKHO...	Login			

Figure 271. Search results table

Depending on the selected **Search mode** the result table may contain the following columns:

- **Time** — action time, in OS date and time format, including milliseconds;
- **User** — name of the SecurOS user who performed an action;
- **Computer** — name of the *Computer* within SecurOS network where an action has been performed;
- **Action** — performed action;
- **Object** — object under which an action has been performed, in <Object_name> <Object_ID> format;
- **Interval** — interval that matches specified **Audit interval** (see [System](#)), in OS date and time format, including milliseconds. Is used to register the prolonged actions (viewing live/archive video, PTZ control). For the details of intervals see the [User Actions Analysis Example](#) section;
- **Name** — name and identifier of the *Tour*, *Preset* or name of the *Watchlist* that have been changed by the user;
- **LP number** — license plate number with which any operations have been performed when working with SecurOS Auto Module or search string value;
- **old LP number** — previous license plate number with which any operations have been performed when working with SecurOS Auto Module;
- **Comment** — comment created automatically by the system for some events.

Advanced search

If the **Advanced** checkbox is selected user can create his own search template (filter) of any complexity, not provided by one of the specified standard search modes. This query can also be saved for future use (see below). The following entities can be used as the query parameters:

1. events.id – event ID in the audit database;
2. events.server_host – name of the *Computer* on which the audit server works;
3. events.server_node – name of the *Node* on which the audit server works (when working in cluster). When working not in cluster configuration coincides with the events.server_host value;
4. events.event_time – event time, in YYYY-MM-DD HH:MM:SS.FFF format;
5. events.event_action – performed action ID;
6. events.user_domain – domain where the *User* which actions must be analyzed is registered;
7. events.user_host – name of the *Computer* on which the actions have been performed;
8. events.user_name – name of the *User* which actions must be analyzed;
9. events.comment – system comment to the event;
10. intervals.event_id – event ID;
11. intervals.time_from – the beginning of the interval (for prolonged actions), in YYYY-MM-DD HH:MM:SS.FFF format;
12. intervals.time_to – the end of the interval (for prolonged actions), in YYYY-MM-DD HH:MM:SS.FFF format;
13. objects.event_id – event ID;
14. objects.obj_type – type of the object under which an actions have been performed;
15. objects.obj_id – ID of the object under which an actions have been performed;
16. objects.obj_name – name of the object under which an actions have been performed;
17. params.param_type – type of the parameter under which an actions have been performed (when configuring PTZ or working with SecurOS Auto);
18. params.param_value – parameter value (when configuring PTZ or working with SecurOS Auto).

The following keywords and operators can be used in the query:

Table 101. Keywords and Operators

Keyword/Operator	Description
(,)	Parentheses. Maximum nesting is 10.
""	Double quotes. Strings and regular expressions must be enclosed in double quotes.
and, &	Logical AND
or,	Logical OR
match	Matching specified regular expression
nomatch	Not matching specified regular expression
==	Equal to

<code>!=</code>	Not equal to
<code>>, <, >=, <=</code>	Comparison operators

Below are the examples of custom queries.

- `events.comment != NULL and objects.obj_type MATCH "CAM"` — requesting all actions with all *Camera* objects for which the **Comment** column is not empty.
- `events.comment MATCH "prima." AND objects.obj_type MATCH "CAM" AND objects.obj_id MATCH "^(8)$"` — requesting all access actions to the *Primary archive* of the *Camera 8*.
- `events.user_name MATCH "^(User 2)$" AND objects.obj_type MATCH "CAM" AND objects.obj_id MATCH "^(1|4|7|.7)$"` — requesting actions of the *User 2* that have been performed under *Camera* objects, which identifiers are 1, 4 and 7 or ends with 7.
- `events.comment MATCH "prima." AND intervals.time_from >= "2019-12-03 09:00" AND intervals.time_to < "2019-12-03 09:30" AND events.event_time > "2019-12-07 14:00" AND events.event_time <= "2019-12-07 14:45"` — requesting actions with the 2019-12-03 09:00 – 2019-12-03 09:30 archive interval, that have been performed by user from 2019-12-07 14:00 to 2019-12-07 14:45.

Working with Search Templates

Any set of parameters specified in the form's fields in the **Advanced search** mode can be saved as search template for further use. Query defined in the **Advanced** field also can be saved as a search template.

To save search template set required values in the form's fields and click the **Save as Template** button. In the **Creating template** window (see Figure 272) specify template name and click the **OK** button.

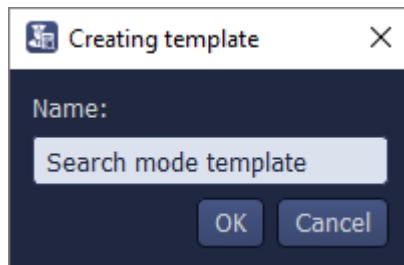


Figure 272. Creating template Window

Search template will be saved in the **Search mode** list. To apply saved search template select it in the list and click the **Search** button.

Exporting Results

Audit data can be exported to the .CSV format file into the user specified directory. To export data click the **Export** button, then in the **Create report** window (see Figure 273) set the directory and the file name. Click the **Create report** button.

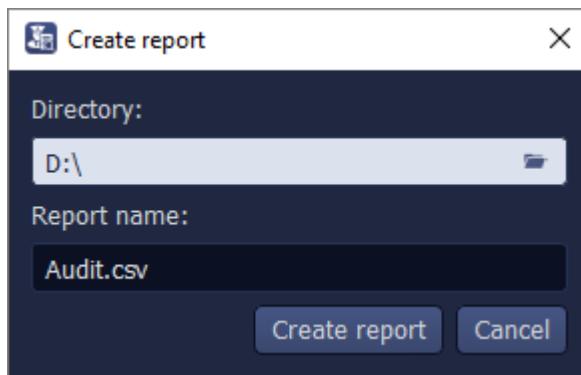


Figure 273. Create report Window

Warning! The ";" character (semicolon) is used as a data fields separator in the created .csv file.

18.3.13.1 Configuring Result Table

Each operator can customize the *Result table* appearance. The following components can be adjusted in the window:

- Number of the displayed table columns;
- Order of the table columns;
- Width of the table columns.

To change the number of the displayed columns right click table header, then in the list of columns deselect those columns that must not be displayed in the table (see Figure 274). To display hidden columns click the ones that are not selected.

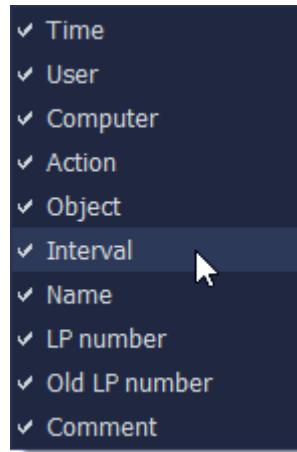


Figure 274. Display/Hide table columns

To change the columns order click the required column and holding mouse button down move it to the required position.

To change the columns width place mouse pointer over the columns separator. Mouse pointer will be as presented in Figure 275.

Time	User	Computer	Action	Object	Interval	Comment	Name	LP number	Old LP number
Wednesday, ...	User1	S-PROKHO...	Watch live ...	Camera 8 [8]	Wednesday,...				
Wednesday, ...	User1	S-PROKHO...	Setup	Camera 7 [7]					

Figure 275. Changing table column width

Press the mouse button, and while holding it down, move the cursor in the required direction.

18.3.13.2 User Actions Analysis Example

User action analysis example is based on the archive viewing operations data. Analysis of live video viewing and PTZ control actions is carried out in the same way.

The data of the request for user actions when working with archived video is shown in Figure 276. **Audit interval** (see [System](#)) is set to 5 minutes.

Time	User	Computer	Action	Object	Interval	Comment
Tuesday, December 3, 2019 14:06:44.904	User2	S-PROKHOROV	Watch live video	Camera 5 [5]	Tuesday, December 3, 2019 14:05:00.000 - Tuesday, December 3, 2019 14:09:59.999	
Tuesday, December 3, 2019 14:08:08.144	User2	S-PROKHOROV	Archive playback	1 Camera 5 [5]	Tuesday, December 3, 2019 11:15:00.000 - Tuesday, December 3, 2019 11:19:59.999	primary archive
Tuesday, December 3, 2019 14:26:53.042	User2	S-PROKHOROV	Archive playback	2 Camera 5 [5]	Tuesday, December 3, 2019 09:10:00.000 - Tuesday, December 3, 2019 09:14:59.999	primary archive
Tuesday, December 3, 2019 14:30:35.057	User2	S-PROKHOROV	Archive playback	3 Camera 5 [5]	Tuesday, December 3, 2019 09:15:00.000 - Tuesday, December 3, 2019 09:19:59.999	primary archive
Tuesday, December 3, 2019 14:35:34.860	User2	S-PROKHOROV	Archive playback	4 Camera 5 [5]	Tuesday, December 3, 2019 09:20:00.000 - Tuesday, December 3, 2019 09:24:59.999	primary archive
Tuesday, December 3, 2019 14:40:34.983	User2	S-PROKHOROV	Archive playback	5 Camera 5 [5]	Tuesday, December 3, 2019 09:25:00.000 - Tuesday, December 3, 2019 09:29:59.999	primary archive

Figure 276. Audit of the user actions when viewing archive video

In this example *User 2* performed the following actions in SecurOS:

- At 14:08:08 switched *Camera 5* to archive mode.
- From 14:08:08 to 14:41:12 performed some operations with the archive.
- At 14:41:12 switched to the live video mode.

In the audit *Result table* the following entries correspond to these actions (in order of listing):

1. At 14:08:08.144 user switched camera to view the *Primary archive* (type of operated archive is displayed in the **Comment** column). When switching to the archive mode archive pointer has been set to the last frame of the archive. In archive used for example the time stamp of the last archive frame is 11:18:32. For the given **Audit interval** (5 minutes) this position of the archive pointer corresponds to the 11:15:00.000 – 11:19:59.999 **Interval** that is displayed in the table. After that during 18 minutes, from 14:08:08.144 to 14:26:53.042, user did not access another fragment of the archive. User actions are not analyzed in more detail (for example, he could view fragments continuously or frame by frame within the current **Interval** that matches **Audit interval**).
2. At 14:26:53.042 user set the archive pointer to the 09:11:17 time stamp that is beyond the

boundaries of the previous **Audit interval** and corresponds to the 09:10:00.000 – 09:14:59.999 **Interval** (by archive time) and began viewing the archive.

3. At 14:30:35 user accessed archive fragment in the 09:15:00.000 – 09:19:59.999 **Interval** (by archive time).
4. At 14:35:34 user accessed archive fragment in the 09:20:00.000 – 09:24:59.999 **Interval** (by archive time).
5. At 14:40:34 user accessed archive fragment in the 09:25:00.000 – 09:29:59.999 **Interval** (by archive time). By the condition of the example, the user finished viewing the archive at 14:41:12 and switched to live video mode. At this moment the archive pointer has been set at the 09:25:34 time stamp that does not cross the boundaries of the current 09:25:00.000 – 09:29:59.999 **Interval**.

18.4 Appendix D. TCP/IP Ports Used by SecurOS

SecurOS and its modules use a list of TCP/IP ports for interaction.

Warning! Third-party applications should not use the ports that are used in the SecurOS software.

You should check your firewall settings and open the following ports in both directions for SecurOS executable files *.exe located in SecurOS program directory.

Table 102. TCP/IP Ports

Service	Port numbers
Core	
SecurOS Base components	20950, 21111, 21112
Databases	5432
Health Monitor	23322, 22432
Remote system	20950
Cluster	2379, 2380
SecurOS Server Manager	20941
Video and Audio Subsystems	
Video stream	20900
Archive Converter	22131
Archiver	20901
EdgeStorage Gate	20903
Video Wall Control Panel	21434
Barco Monitor	22413
Audio stream	20910

Service	Port numbers
ONVIF protocol operation	50000
Base Interface Subsystem	
Operator's Interface (all components)	38880
Media Client	22428
Event Viewer	21055
Map Window	22437
Auxiliary components	
CCTV Keyboard or Joystick	22411
External Window	21053
Alarm Viewer	23518
HTML Dialog/Form	30300
HTML5 FrontEnd	22821
Space Keeper	22429
3D Map	26889
Integrations	
VB/JScript program	21827
IIDK	21030
ActiveMedia Kit	23100
Integration Point	23000
Intelligent Modules	
Computer Vision	20930
SecurOS ACS	21515
SecurOS Auto	21756
SecurOS Cargo	22291
SecurOS FaceX	22817
SecurOS Mobile	7779
SecurOS NMD	22338
SecurOS POS	22126
SecurOS Transit	20666

Service	Port numbers
SecurOS UVSS	22523

18.5 Appendix E. Additional Windows Settings

Additional Windows settings provide correct SecurOS operation and are needed in order to use some of the system functionalities, as well as to allow optimized system operation.

18.5.1 Installing Multimedia Components and Services under MS Windows Server 2008 R2

Windows Server 2008 is completely a server operating system. There are no multimedia components and services installed when you perform initial OS install. However, these system components are necessary for proper SecurOS operation including audio subsystem, archive converter and must be installed manually. To install required components and services do the following:

1. Download Windows Media Services 2008 for Windows Server 2008 R2 Update Package from Microsoft Download Center:
<http://www.microsoft.com/en-us/download/details.aspx?id=20424>
2. Install downloaded package files.
3. Enter **Server Manager** menu and do the following:
 - Select **Roles** tab;
 - Click **Add Roles** button;
 - Install **Streaming Media Services** with the Wizard and restart server if required.
4. Enter **Server Manager** menu and do the following:
 - Select **Features** tab;
 - Click **Add Features** button;
 - Install **Desktop Experience** with the Wizard and restart server.
5. Reboot Windows Server 2008.

18.5.2 Installing Media Foundation under MS Windows Server 2012 R2

Windows Server 2012 is completely a server operating system. There are no multimedia components and services installed when you perform initial OS install. However, these system components are necessary for proper SecurOS operation including, particularly, *Video Capture Device* with **Player AVI** type, and must be installed manually. To install the **Media Foundation** component do the following:

1. Open the **Server manager** console application.
2. In the **Manage** menu select **Add roles and features** option.
3. On the **Select installation** page select **Role-based or feature-based installation** option.
4. Click **Next** to select features. Select the **Media Foundation** feature.
5. On the **Confirm installation selections** page review your role, feature, and server selections. If you are ready to install, click **Install**.
6. Restart server if needed.

18.5.3 SMTP Mail Server Installation and Configuration

Note. All actions must be performed under local or domain administrator account.

On the computer with *Mail service* installed open **Control Panel** and choose **Add or Remove Programs**, then **Add/Remove Windows Components**.

Choose **Internet Information Services (IIS)** from the list and click the **Details** button (see figure 277).

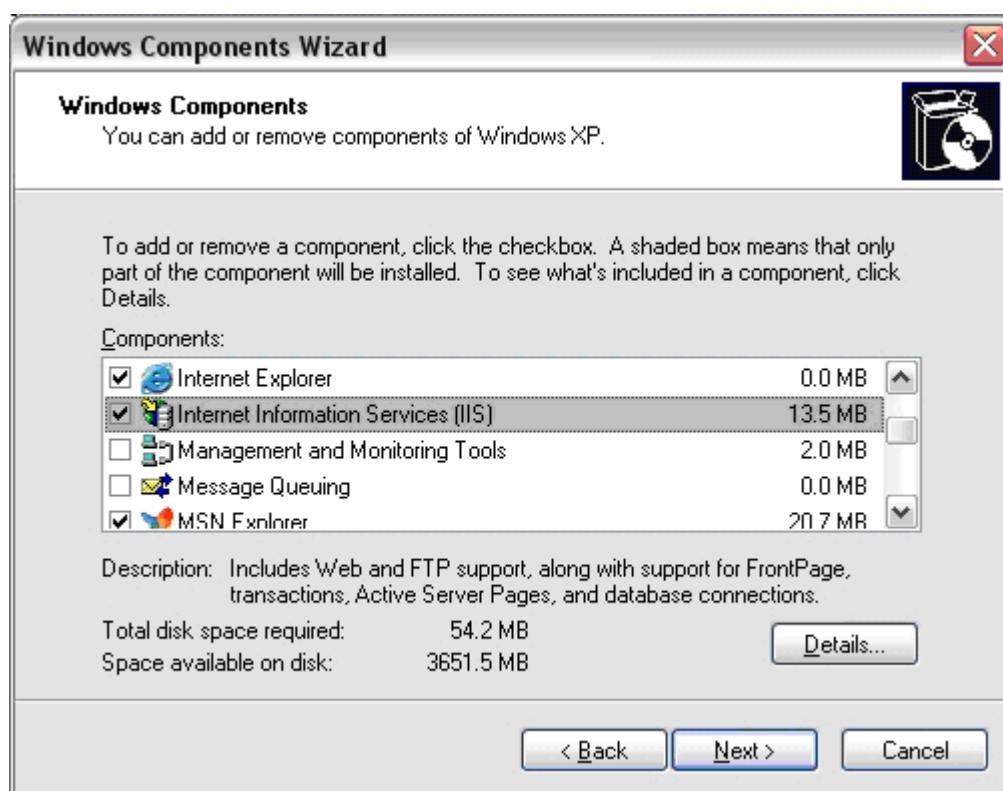


Figure 277. Windows Components Wizard

Enable **SMTP Service** in the list (see figure 278). Click **OK** and **Next** buttons.

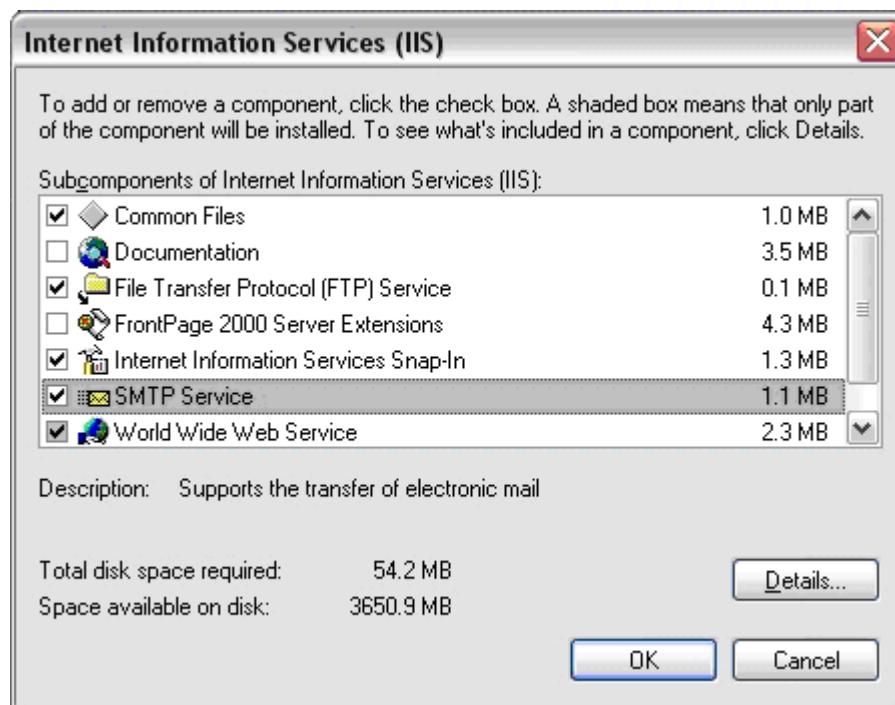


Figure 278. Internet Information Services Components

To configure SMTP server for message delivery, after SMTP service installation:

1. Open Control Panel → Administrative Tools → Internet Information Services.
2. On the left side of the new window (see figure 279) right-click Default SMTP Virtual server (or another name, given by default) and choose Properties.

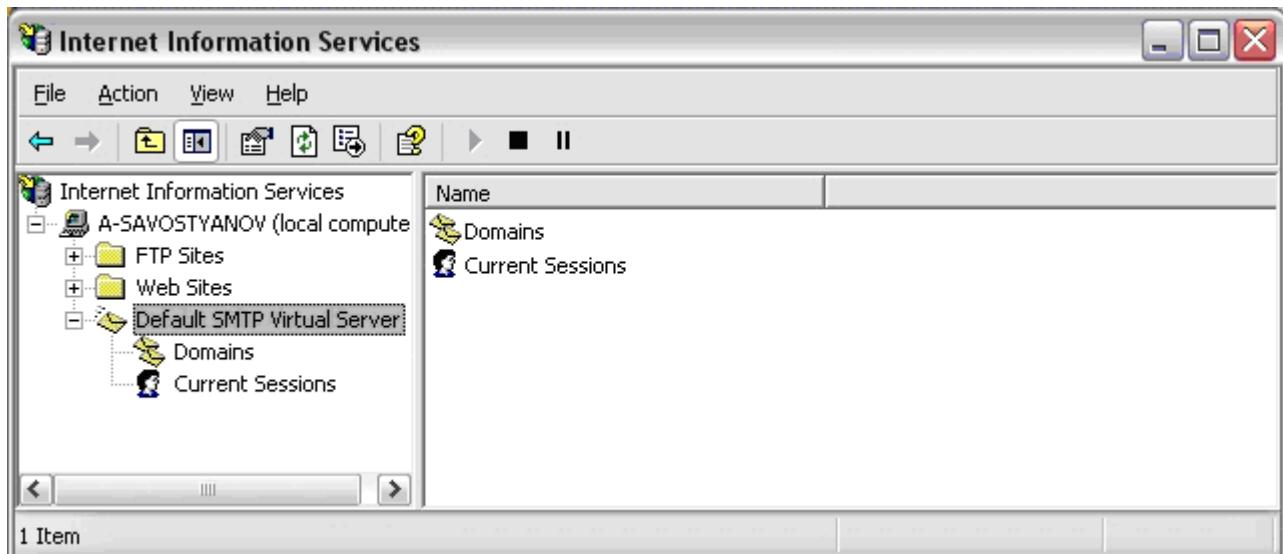


Figure 279. IIS Services tree

3. Choose Access tab and click the Relay button.
4. Choose All in new Relay Restrictions window to allow delivery from all computers sending mail through this server, and click OK (see figure 280).

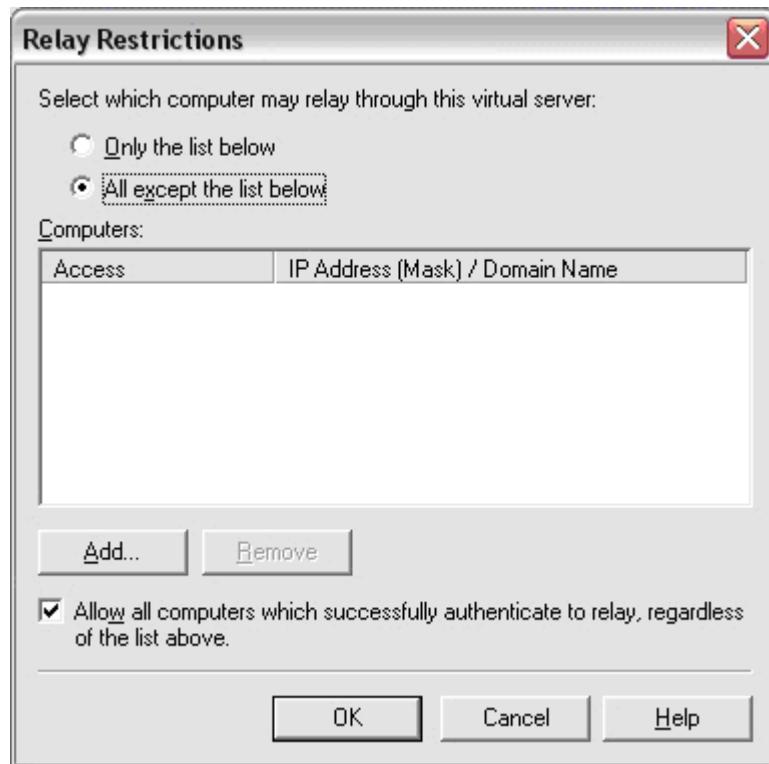


Figure 280. SMTP server relay restrictions settings

5. Choose **Delivery** tab and click the **Advanced** button.
6. In new **Advanced Delivery** window (see figure 281) specify remote server to route all sending mail in **Smart Host** field and click **OK**.

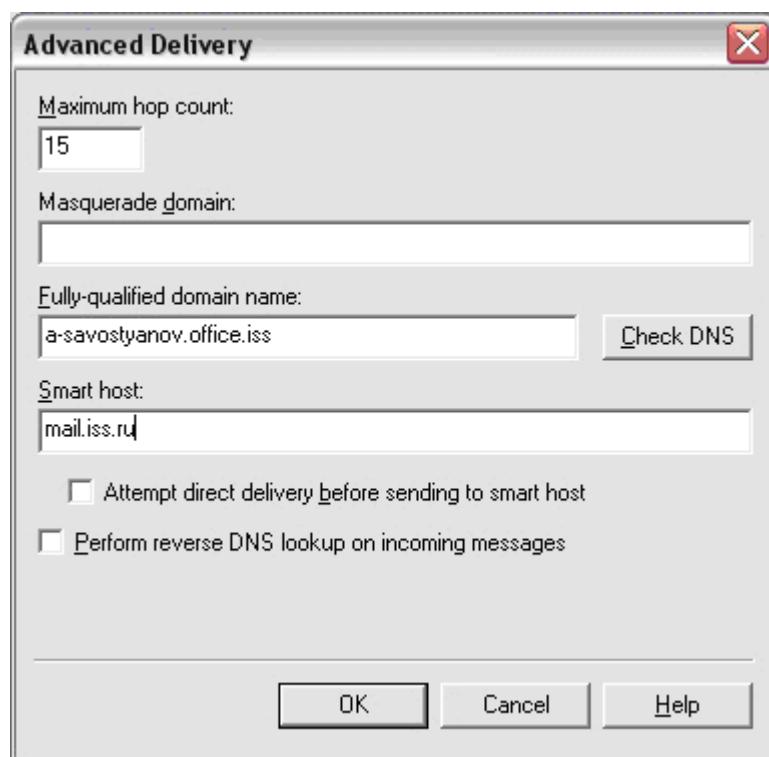


Figure 281. Mail routing remote server settings

7. Click **OK** to close SMTP server properties window and save all changes.
8. Choose **Action → Run** to run SMTP server service.

18.5.4 Disabling Disk Cleanup Master

It is recommended to disable system warnings on full disk for operator workstations / video servers.

To disable the disk cleanup master:

1. Open registry editor (**Start → Run → regedit**).

2. Choose

`\HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer` section and create DWORD parameter with name `NoLowDiskSpaceChecks`.

3. Assign 0 value to created parameter to disable full disks check (1 – to enable this check again).

4. Close registry editor and reboot the computer.

18.6 Appendix F. Error Messages When Launching System

When launching, SecurOS system can report some problems. List of such problems and their descriptions is represented in Table 103

Table 103. Possible error messages on system startup

Message	Recommendations
"Key file not found"	Check that there is a file called <code>key.iss</code> in the SecurOS program folder. If there is no such file, you should copy it manually to the SecurOS root folder on the <i>Configuration Server</i> (file is located on installation CD or, you also can received it by e-mail).
"Starting failed"	Unexpected program error has occurred during system startup. Generate system report using the ISS System Report Utility (see ISS System Report Utility (ISSInfo) for more information) and contact the local ISS Technical Support Team providing this report to analyze it and solve the problem (see Getting Technical Support).
"Key file expired"	Your <code>key.iss</code> file has expired. Contact Technical Support Team for a new key (see Getting Technical Support).
"DB Connection Error"	<p>Perform the following steps:</p> <ul style="list-style-type: none"> • Check the database connection parameters using the DSAdmin Utility. • Check the database connection using the PgAdmin III utility included in the PostgreSQL Kit. • Make sure the Windows service PostgreSQL Database Server 9.x exists and is running. • Make sure that the user who launches the system has rights for reading the <code>HKLM\Software\ISS\SecurOS\NISS400\DB</code> key.

Message	Recommendations
	<ul style="list-style-type: none">• Reinstall SecurOS. Pay special attention to PostgreSQL installation procedure steps.• If these recommendations did not solve the problem, please contact the local ISS Technical Support Team. Attach the system information obtained from the ISS System Report Utility.
"Language is not supported"	During the SecurOS installation you specified interface language that is not allowed in your license key. You should either re-install SecurOS software on this machine and choose valid interface language in Setup Wizard, or provide new key.iss file that permits using this language.
"Country is not supported"	Country settings (Start → Control Panel → Regional and Language Options) differ from those allowed in your license key. Check these settings to see if country is specified properly or provide a new key.iss file that permits using current country settings.

18.7 Appendix G. Technical Support Information

Current section contains service information that is necessary on addressing to Intelligent Security Systems Technical Support.

Note. Collected data have to be send to the Intelligent Security Systems Technical Support Team (see [Getting Technical Support](#)).

To ensure quick technical support, prepare the following technical information:

Warning! Data in items marked by "*" are necessary to report.

1. (*) User (customer) name to address to.
 2. (*) Organization name.
 3. (*) User (or organization) contacts: phone, e-mail.
 4. Name of a personal Intelligent Security Systems manager (on Intelligent Security Systems authorized partner case). Otherwise, give the following data:
 - Company where the hardware and software components were purchased.
 - Actions proposed to solve the problems announced by a partner from whom the product was purchased.
 5. (*) Problem description.
 6. (*) Actions results in the problem.
 7. List of changes which result to the problem in case of applying after some changes in system settings/configuration.
 8. System and diagnostic information on computer and SecurOS system configuration obtained from the **ISS System Report Utility** (see [ISS System Report Utility](#) for detailed information about utility).
- If it is impossible to run the utility provide the following information:

- (*) Guardant keys identifier and Dallas code;

Note. Equipment Dallas code can be found by the **ISS Hardware Report** utility (see [ISS Hardware Report Utility](#) for detailed information about utility).

- (*) name and version of the installed Intelligent Security Systems company software.
- total number of video servers and monitoring (operator) workstations in the system;
- operating system (name and service pack version).

9. Another useful information, if possible. For example:

- computer equipment configuration.
- central processors load.
- main and virtual memory used volumes.
- network load.
- network and network neighborhood configuration.

Index

A

- access level,
 - Configure, 122
 - Control, 122
 - Full access, 122
 - Inherited rights, 122
 - No access, 121
 - View, 121
- Access to Long-term archive, parameter,
 - Media Client, 233
- account,
 - postgres, 55
- ACS and Fire Alarm System Database, parameter,
 - Computer, 125
- Action, parameter, 297
- Activate Desktop, property, 124
- Active Directory / LDAP object description, 117
- Add directory, button,
 - Archiver, 220
- Add footer, parameter,
 - Media Client, 232
- Add SecurOS Evidence Manager, parameter,
 - Archive Converter, 212
- Additional information, property, 116
- Address (IPv4) for Multicast group, parameter,
 - Camera, 182
- Address mapping, parameter,
 - Remote System, 348
- Address, parameter,
 - iSCSI drive, 370
- Administration mode, 57
- Administrator Toolbar, 63
- Advanced, property,
 - HTML5 FrontEnd, 159
- Alarm condition, parameter,
 - Sensor, 270
- Alarming, property, 206
- Algorithm, parameter,
 - Wrong direction detector, 337
- Aling on display center, paramter,
 - HTML Dialog, 281
- Allow auto logon for User(s), property,
 - Computer, 124
- Allow connections from the following IP addresses only, parameter,
 - Monitoring center agent, 356
- Allow to audit system, parameter, 120
- Allow to configure system, property, 120
- Allow to edit FaceX watchlists, parameter, 120
- Allow to hold PTZ control, parameter, 120
- Allow to request PTZ control, parameter, 120
- Allowed direction deviation, parameter,
 - Wrong direction detector, 337
- Allowed IP addresses, table,
 - Monitoring center agent, 356
- Always on top, paramter,
 - HTML Dialog, 281
- Analyze reduced FPS stream, max FPS parameter, 207
- Application window (optional), parameter,
 - External Window, 156
- Application, parameter,
 - External application, 136
- Application, property,
 - External Window, 155
- Archive Converter object description, 209
- Archive export profile object description, 218
- Archive recording, 170
 - archive recording to the files of specified length, 126
 - frames number, 170
 - frames queue, 171
 - free disk space, 170
 - threshold, 170
- Archive, tab,
 - Computer, 124
- Archiver object description, 218
- Archiving mode, parameter,
 - Archiver, 220
- Arguments, parameter,
 - External application, 136
- Armed always, property, 206
- Attachments, parameter,
 - E-mail Message, 285
- Audible Notification Service object description, 286
- Audio Capture Device object description, 264
- Audit interval, parameter,
 - System, 108
- AuditClient Utility,
 - configuring GUI, 440
- AuditClient, utility, 434
- Auto white balance, parameter,
 - Camera, 196
- Autogain, parameter, 196
- Automatic backup, parameter,

- Automatic backup, parameter,
System, 107
- Automatic center align by X, parameter, 196
- Automatic center align by Y, parameter, 196
- ## B
- Backlight Compensation level, parameter,
ONVIF type, 192
- Backlight Compensation, parameter,
ONVIF type, 192
- Base, parameter,
Camera, 180
- Media Client, 235
- Bgain, parameter,
ONVIF type, 192
- Blinding detection property,
Camera, 187
- Bolid, integration, 388
- Bound, parameter, 267
- Brightness, parameter,
ONVIF type, 192
- ## C
- Camera,
Image settings, 170
- Camera alarm mode control, parameter,
Media Client, 232
- Camera elevation, parameter,
Object counter, 332
- Camera ID in the edge device, parameter,
Camera, 181
- Camera is defocused when camera sharpness reduces
by, parameter,
Defocus detector, 200
- Camera is focused, button,
Defocus detector, 200
- Camera object description, 176
- Camera serial number parameter,
Camera, 195
- Camera, setting up, 252
- Cameras and Microphones list, parameter,
Media Client, 231
- Cameras, parameter,
RTSP Server, 226
- Capacity, parameter,
Archiver, 220
- CC, parameter, 284
- CCTV keyboard or joystick object description, 272
- Cells, parameter,
Layout, 203
- Channel, parameter,
- Microphone, 267
- Relay, 271
- Sensor, 270
- Channel, property,
Camera, 177
- Check syntax, button,
VB/JScript program, 299
- Checking period, parameter,
Defocus detector, 200
- Classification Tab,
Tracking Kit III plugin, 314
- Clear all, property (Zone), 207
- Codec for recording, parameter,
Camera, 196
- Codec of camera video stream, parameter,
Camera, 196
- Codec property,
Archive Converter (Audio), 216
- Codec, property,
Archive Converter (Video), 215
- Command "Play the last N s/min of record", parameter,
Media Client, 233
- Computer object description, 122
- Computer's role, property, 124
- Computers that are allowed to connect to the network,
parameter,
IIDK Interface, 300
- configuration,
quick steps, 397
- configuration examples, 250
domain for LDAP provider, 85
domain for Windows NT provider, 85
standalone configuration, 250
Video Server and Operator Workstation, 251
- Configuration Server address, parameter,
Remote System, 348
- Confirm new password, parameter,
System, 107
- Connect, radio-button,
Database, 113
- Contrast property,
Camera, 188
- Contrast, property,
Zone, Motion detection, 206
- Coordinates property,
Camera, 177
- Create DB and User, button,
Database, 115
- Create new level, button,
Map, 147
- Create new, radio-button,

Create new, radio-button,
Database, 113
Crowd detector object description, 329

D

Database name/User/Password, parameters,
Database, 114

Database object description, 113

Database Update Utility (idb.exe), 420

Databases, parameter,

 Databases Replicator, 137

Day/Night shift level, parameter,

 Camera, 193

Defocus detector, 201

Delete with primary archive, parameter, 125

Department object description, 115

Desktop object description, 138

Detect people only, parameter,

 Loitering detector, 327

Detection area, parameter,

 Defocus detector, 200

Device control IP address, parameter,

 Camera, 193

Device tree,

 Map, 146

Device, parameter, 285

Digital zoom, parameter,

 Media Client, 232

Directory, parameter,

 Archiver, 220

Disable if Event Viewer exists, parameter, 287

Disable saving data into local Protocol DB, property,
125

Disable shared PTZ control property,

 Camera, 190

Display area,

 Map, 146

Display, parameter,

 Map Window, 152

 Media Client, 231

Display, property,

 Event Viewer, 154

 External Window, 155

 HTML form, 157

 HTML5 FrontEnd, 158

Do not adjust frame timestamp for fast forward
playback, parameter,

 Camera, 185

Do not recover last, min, parameter,

 Camera, 185

Do not show the notification window when there are
new problems, parameter,

 Health Monitor, 89

Download speed relative to FPS, parameter,
 Camera, 186

DSAdmin utility (dsadmin.exe), 416

Duration of post-recording property,
 Camera, 184

Duration of pre-recording property,
 Camera, 184

Duration, parameter,

 Crowd detector, 330

 Loitering detector, 327

Dwell time detector object description, 334

E

Edge device response timeout, parameter,

 EdgeStorage Gate, 227

Edge Storage,

 Hardware requirements, 167

 Requirements to the camera local storage, 167

 Time synchronization, 167

EdgeStorage Sync object description, 227

Edit, button,

 Archiver, 220

 VB/JScript program, 299

E-mail Message object description, 283

E-mail Message Service object description, 282

E-mail, property, 116

Emergency service object description, 287

Enable Cameras and Microphones grouping, parameter,

 Media Client, 231

Enable failover of the Video server and add to the
cluster, parameter,

 Computer, 124

Enable multicast mode, parameter,

 Camera, 182

Enable shared Views setup, parameter,

 Media Client, 238

Enable stream synchronization parameter,

 Virtual Video Capture Device, 195

Encryption algorithm, parameter, 215

Encryption, parameter,

 E-mail Message Service, 283

Erase records older than, parameter,

 Database, 114

Event name (Object left behind detector detector),
parameter,

 Left behind and Removed object detector, 325

Event name (Removed object detector), parameter,

 Left behind and Removed object detector, 325

Event name, parameter,
 Crowd detector, 330
 Dwell time detector, 335
 Intrusion detector, 329
 Line crossing detector, 333, 334
 Loitering detector, 327
 Object counter, 331
 Running detector, 323, 340
 Wrong direction detector, 337
Event Viewer object description, 153
Event, parameter,
 Macro, 297

Export,
 Audio, 411
 Video, 410
Export to property, 212
Export video with audio, parameter, 215
Exposure Time, parameter,
 ONVIF type, 191
Exposure time, μ s, parameter,
 Camera, 196
External Window object description, 155

F

File type property, 212
Fill all, property, 207
For IP-device, parameter, 265
For motion detection, parameter,
 Camera, 179
For Sound card, 266
For video recording, parameter,
 Camera, 179
Forbid to hide interface, property, 119
Force camera night mode shift, parameter,
 Camera, 193
Format, property,
 Video Capture Device, 173
FortNet, integration, 389
FPS divider property, 215
FPS reduction performed on server property, 215
Frame Export, parameter,
 Media Client, 232
Frame height, px, parameter,
 Camera, 196
Frame Print, parameter,
 Media Client, 232
Frame width, px, parameter,
 Camera, 196
From, parameter, 284
From, To, parameters,
 Schedule, 295

Full FPS on alarm property,
 Camera, 184

G

Gain, parameter, 196, 267
 ONVIF type, 191
Get IQN list, button,
 iSCSI drive, 370
Grid, parameter,
 Layout, 203
Guardant key, 407
 installation, 23

H

Hardware acceleration, parameter,
 Media Client, 232
Hardware property, 271
Hardware, parameter,
 Sensor, 270
Health Monitor object description, 88
Hidden, parameter, 297
High resolution, parameter,
 Camera, 180
 Media Client, 235
Holidays, parameter,
 Schedule, 295
Holidays, property,
 Security Zone, 110
Host property,
 Bolid integration, 388
 FortNet integration, 390
Host, parameter,
 Database, 114
 Remote system, 354
Host/Port, parameters,
 Emergency service (RTSP server), 289
 Emergency service (WebView), 289
HTML Dialog object description, 280
HTML Form object description, 156
HTML5 FrontEnd object description, 157
HTTP address of Emergency Service, parameter, 288
HTTP Event Gate object description, 301
HTTP port, parameter,
 RTSP Server, 225

I

ID, 65
ID, parameter,
 Macro (Actions), 297
 Macro (Event), 297

Identifier (Presets) property,
 Camera, 190
Identifier (Tours), parameter,
 Camera, 190
Ignore qop (Quality of protection) parameter with auth value when using digest authentication parameter,
 Camera, 195
IIDK Interface object description, 300
Illumination mode, parameter,
 Camera, 193
Image Processor object description, 224
Import Cameras with IDs, parameter,
 Remote system, 354
Import, button,
 Map, 147
Incident Types List parameter,
 Emergency service, 289
Information about configured window block,
 Desktop, 140
Inner zone property, 209
Integration point object description, 387
Integration with 3rd Party Systems, 299
Intersection of object and zone, parameter,
 Dwell time detector, 335
 Intrusion detector, 329
 Loitering detector, 327
Intrusion detector object description, 328
IP address, property, 174
IP-Device Manager object description, 68
IQN, parameter,
 iSCSI drive, 370
IR filter mode, parameter,
 ONVIF type, 192
Iris, parameter,
 ONVIF type, 192
ISS Hardware Report Utility, 407
ISS Media Export Utility, 410
ISS SecurOS Registration Files Editor (ddi.exe), 422
ISS System Report Utility, 407

J

joystick,
 configuring, 261

K

keyboard shortcuts, 391

L

Language, parameter,
 VB/JScript program, 298

Layout object description, 202

Layouts panel, parameter,
 Media Client, 238

Left Behind and Removed Object Detector object description, 324

Level, parameter,
 Microphone, 267

License key, 23
 expiration date remainder, 87
 expiration date remainder setup, 87
 request, 24
 updating, 86

Light Detector object description, 208

Light, property,
 Camera, 178

Limit live video FPS, parameter,
 Media Client, 240

Line crossing detector object description, 333

Linked to Camera, parameter,
 Microphone, 267

List of the addresses, parameter,
 IIDK Interface, 300

Load from file, button,
 Emergency service, 289

Local, parameter, 296

Login property,
 Bolid integration, 389

Logo Overlay, parameter,
 Archive Converter, 216

Loitering detector object description, 326

Long Dwell Duration, parameter,
 Dwell time detector, 335

Low resolution, parameter,
 Camera, 180
 Media Client, 235

M

Macro object description, 296

Manual exposure control, parameter,
 ONVIF type, 191

Map,
 Adding level, 148
 Base image, change, 149
 Child level, create, 149
 Display collapsed object caption, 151
 layers image, 147
 Level link, 149
 Level, change text color, 149
 Level, Delete, 150
 Level, rename, 149
 Objects, deleting, 152

M

Map,
 Objects, moving, 150
 Objects, moving object name, 151
 Objects, positioning, 150
 Objects, rotating, 151
 Objects, searching by name, 150
 working principles, 147

Map object description, 145

Map Window object description, 152

Map, parameter,
 Map Window, 152

Max. FPS, parameter,
 Archiver, 221

Maximum backup number, parameter,
 System, 108

Maximum Protocol DB size, property, 125

Memory frames, property, 207

Message field, parameter,
 E-mail Message, 284

Message, parameter,
 Short Message, 286

Microphone object description, 266

Microphone tree, parameter,
 Media Client, 245

Microphone, property,
 Camera, 186

Minimum count, parameter,
 Crowd detector, 330

Minimum object detection time, parameter,
 Left behind and Removed object detector, 326

Minimum/Maximum, parameters,
 Media Client, 235

Mode, parameter,
 Archiver, 220
 Intrusion detector, 329
 Left behind and Removed object detector, 326

Model, parameter,

 Audio Capture Device, 265

Model, property,

 Video Capture Device, 173

Monitoring center agent object description, 355

Multi-cell zoom without stream switching, parameter,
 Media Client, 232

N

Name, 65

 Map, 146

Name pattern, property, 213

Name, parameter,

 Archiver, 221

 Macro (Actions), 297

Macro (Event), 297

Network latency, ms, parameter,
 Camera, 182
New password, parameter,
 System, 106

O

Object class, parameter,
 Intrusion detector, 329
 Object counter, 332
 Wrong direction detector, 338
Object counter object description, 331
Object left behind detector, parameter,
 Left behind and Removed object detector, 325

Object Tree, 63

 Child object, 63
 Desktop, 140
 Parent object, 63

Object tree parameter,
 Sensor, 271

Object tree, parameter,
 Media Client, 240

OK/Cancel, property (buttons), 207

On following week days, parameter,
 Schedule, 295

ONVIF port, parameter,
 ONVIF Server, 227

ONVIF Server object description, 226

Operator reaction on alarm event, property, 154

Outer zone (secondary) property, 209

Outer zone property, 209

P

Pack, parameter,

 E-mail Message, 285

Page dwell time when auto scrolling, parameter,

 Media Client, 233

Pan/Tilt/Zoom, property,
 Camera, 177

Params, parameter, 297

Password property,

 Bolid integration, 389

Password, parameter,

 User account, 116

Password, property,

 Video Capture Device, 175

Path parameter,

 Camera, 181

PCI channel, property, 173

Phone, parameter,

Phone, parameter,
 Short Message, 286

Phone, property,
 User Account, 116

Pixel format parameter,
 Camera, 195

Playback archive from the edge device, parameter,
 Camera, 185

Port for Multicast group, parameter,
 Camera, 182

Port property,
 Bolid integration, 389
 FortNet integration, 390

Port, parameter,
 Database, 114
 E-mail Message Service, 283
 iSCSI drive, 370
 Monitoring center agent, 355
 Movable PostgreSQL, 371
 Remote system, 354
 REST API, 302

Port, property,
 Active Directory / LDAP, 118

Position, parameter,
 Archive Converter, 216

Profile, parameter,
 Camera, 181

Protocol database length, property, 109

Protocol property,
 Relay, 271

Protocol, parameter,
 Audio Capture Device, 265
 Camera, 181

Protocol, property,
 Video Capture Device, 173

Provider, property, 117

Providers, property, 120

PTZ channel property,
 Camera, 189

PTZ control priority, parameter, 120

PTZ control via mouse, parameter,
 Media Client, 232

PTZ Control, parameter,
 Media Client, 231

PTZ protocol property,
 Camera, 189

Q

Quality property,
 Archive Converter (Audio), 216

Quality, property,

 Archive Converter (Video), 215

Quick audio export property, 215

Quick video export property, 215

R

Record system audit data, parameter,
 System, 108

Recording control, parameter,
 Media Client, 231

Recording mode, property,
 Camera, 183

Recover archive from the local storage of Camera (Edge Storage), parameter,
 Camera, 185

Reduce frame rate, parameter, 215

Reduce max FPS to property,
 Camera, 184

Relay number, parameter, 271

Relay, object, description, 271

Remote system object description, 347, 354

Remove after property,
 Archiver, 221
 Camera, 184

Remove, button,
 Archiver, 221

Removed object detector, parameter,
 Left behind and Removed object detector, 325

Replicate to database, parameter,
 Databases Replicator, 137

Requires authentication, parameter, 283

REST API object description, 301

Restore button,
 System, 107

Rgain, parameter,
 ONVIF type, 192

Rights, property, 119

RTP over RTSP (TCP), parameter,
 Camera, 182

RTSP port, parameter,
 RTSP Server, 225

RTSP Server object description, 224

RTSP server, parameter,
 Emergency service, 289
 ONVIF Server, 227

RTSP Specification, parameter,
 RTSP Server, 226

Run Macro at start, parameter, 110

Running detector object description, 322

S

Samplerate, parameter, 265

Saturation, parameter,
 ONVIF type, 192

Save button,
 System, 107

Save movement coordinates (enables Smart Search),
property, 206

Save to file, button,
 Emergency service, 289

Scale, parameter,
 Map, 146

Scene Tab,
 Tracking Kit III plugin, 308

Schedule property,
 Archiver, 220

Schedule, object, description, 293

Schedule, parameter,
 VB/JScript program, 299

Search, box,
 Map, 146

Security Zone object description, 108

SecurOS Logging, 86

SecurOS Server Manager utility, 398

Select zone, parameter,
 Wrong direction detector, 338

Select, button,
 Archive Converter, 216
 External Window, 155

Send Ticket to Emergency Service, parameter,
 Event Viewer, 154
 Media Client, 233

Sensitivity property,
 Light Detector, 209

Sensitivity, parameter,
 Smoke detector, 340
 Wrong direction detector, 338

Sensor, object, description, 269

Serial port number parameter,
 Camera, 190

Server IP address, property,
 Computer, 124

Server, property,
 Active Directory / LDAP, 118

Set typical size of the object, button,
 Object counter, 332

Sharpness, parameter,
 ONVIF type, 192

Short Dwell Duration, parameter,
 Dwell time detector, 335

Short Message object description, 285

Short Message Service object description, 285

Short/Middle/Long range illumination, parameter,

 Camera, 193

Show alarmed levels, parameter,
 Map Window, 153

Show all zones, property, 207

Show Camera ID, parameter,
 Media Client, 232

Show level tree, parameter,
 Map Window, 153

Single-cell zoom with stream switching, parameter,
 Media Client, 232

Size property,
 Camera, 188

Size, property,
 Zone, 207

Smoke detector object description, 339

SMTP Server, parameter, 283

SNMP agent object description, 133

Sound card, parameter,
 Audible Notification Service, 287

Speaker property,
 Camera, 187

Specific date, parameter,
 Schedule, 295

Speed (person width per second), parameter,
 Running detector, 323

Split into files up to property, 212

Standard layouts, parameter,
 Media Client, 235

Store at least property,
 Camera, 184

Store, parameter, 125

Stream 1, parameter,
 Camera, 179

Stream 2, parameter,
 Camera, 179

Stream 3, parameter,
 Camera, 179

Subject, parameter, 284

superuser, 79

System object description, 106

T

technical support,
 gathering system information utility, 398
 how to get, 11
 how to prepare service information, 449

Test connection, button,
 Database, 114
 Microphone, 267, 371

Text color,
 Map, 146

- Time of acknowledgment of alarm event by the operator, property, 155
- Time to display Camera after alarm ends, parameter, Media Client, 231
- Title (Presets) property, Camera, 190
- Title (Tours), parameter, Camera, 190
- To, parameter, 284
- Tour type, parameter, Camera, 190
- Tracker Tab, Tracking Kit III plugin, 313
- Tracking Kit III object description, 305
- Treat a large object as a group of objects, parameter, Object counter, 332
- Type, parameter, Audio Capture Device, 265
Database, 114
Macro (Actions), 297
Macro (Event), 297
- Type, property, Video Capture Device, 173
- ## U
- Update configuration, button, Integration point, 387
Remote system, 355
- URL, property, HTML5 FrontEnd, 158
- Use Archive export profiles, parameter, Media Client, 243
- Use as Operator Workstation Profile, parameter, Computer, 124
- Use authentication, parameter, iSCSI drive, 370
- Use camera settings, parameter, Camera, 180
- Use credentials provided at system login, property, 118
- Use custom script file, parameter, HTML Form, 157
- Use digest authentication only, parameter, Camera, 178
- Use Event filter, parameter, Remote System, 348
REST API, 302
- Use Event Filter, property, 125, 154
- Use HTTPS, parameter, REST API, 302
- Use interframe delays from file parameter, Virtual Video Capture Device, 195
- Use only selected Cameras, parameter, Media Client, 240
- Use only selected microphones, parameter, Media Client, 245
- Use only selected shared Views, parameter, Media Client, 238
- Use primary domain controller, property, 117
- Use remote Camera IDs, parameter, Remote system, 355
- Use secure authentication, parameter, 118
- Use secure connection (HTTPS), parameter, Audio Capture Device, 265
Video Capture Device, 175
- Use SecurOS Motus built-in controller, parameter, Camera, 193
- Use standard script file, parameter, HTML Dialog, 281, 282
HTML Form, 157
- Use stream on request, parameter, Camera, 182
- Use video gate for live video, parameter, Remote System, 349
- User Account object description, 116
- User and Password, parameter, iSCSI drive, 370
- User Name, Password, parameter, 118, 283
- User Rights object, settings for LDAP provider, 86
- User rights object, settings for Windows NT provider, 85
- User Rights object description, 118
- User, property, Video Capture Device, 175
- User/Password, parameters, Emergency service, 289
- Users and Groups, parameter, 121
- User's Layouts, parameter, Media Client, 235
- ## V
- VB/JScript program object description, 297
- Video Capture Device object description, 172
- Video, property, Zone, 207
- View object, Create, 248
Delete, 249
Edit, 248
Rename, 249
- View object description, 204
- View, parameter,

View, parameter,
 Video Capture Device, 175
Viewing, property,
 Camera, 178
Views list, parameter,
 Media Client, 238
Visual settings area,
 Desktop, 140
Volume, parameter,
 Audible Notification Service, 287

W

W, H, parameters,
 Media Client, 231
Washing Kit, property,
 Camera, 178
WDR level, parameter,
 ONVIF type, 192
WDR mode, parameter,
 ONVIF type, 192
WebSocket port, parameter,
 REST API, 302
WebView Monitor, parameter,
 Emergency service, 289
WebView, parameter,
 Emergency service, 289
White Balance, parameter,
 ONVIF type, 192

Wide layouts, parameter,
 Media Client, 235

Wiper property,
 Camera, 177

Work in accordance with selected Schedule, parameter,
201
 Camera, 188
Work with audio, parameter,
 Media Client, 245

Work with Map Window, parameter,
 HTML5 FrontEnd, 159

Work with Media Client, parameter,
 Event Viewer, 154
 HTML5 FrontEnd, 158
 Map Window, 153

Work with Views, parameter,
 Media Client, 238

Working directory, parameter,
 External application, 136

Working mode, parameter,
 Media Client, 230

Write secondary event parameters into Protocol DB,
property, 125

Wrong direction detector object description, 336

X

X, Y, parameters,
 Media Client, 231
X, Y, property,
 HTML Dialog, 281
X, Y, W, H, property,
 Event Viewer, 154
 External Window, 155
 HTML Form, 156
 HTML5 FrontEnd, 158
 Map, 152
X-offset, px, parameter,
 Camera, 196

Y

Y-offset, px, parameter,
 Camera, 196

Z

Zone,
 working principles, 165
Zone object description, 204
Zone types, property, 206