



INTELLIGENT SECURITY SYSTEMS



SECUROS

Version 8

Administration Guide

SecurOS Administration Guide (AG - EN, build 84 on 28.01.2016).

© Copyright Intelligent Security Systems, 2016.

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	9
1.1 Scope	9
1.2 Target Audience	9
1.3 Using This Manual	9
1.4 Getting Technical Support	9
1.5 SecurOS Editions Naming Convention	10
1.6 Design Convention	11
1.7 Design Elements	11
2 Purpose, Implementation And Operation Principles	12
2.1 SecurOS Architecture	12
2.1.1 Types Of Servers And Workstations	12
2.1.1.1 Classification by Functionality	12
2.1.1.1.1 Video Server	12
2.1.1.1.2 Operator Workstation	13
2.1.1.1.3 Administrator Workstation	13
2.1.1.2 Classification of Roles in Configuration Management	13
2.1.1.2.1 Configuration Server	13
2.1.1.2.2 Peripheral Server	14
2.1.1.2.3 Managing Network Configuration by Configuration Server	14
2.1.1.2.3.1 How To Configure Servers When Deploying Network	14
2.1.1.2.3.2 Configuration Update Procedure	14
2.1.1.2.3.3 Restoring Configuration from Backup Copy	15
2.1.2 Types Of System Configurations	15
2.1.2.1 Standalone Configuration	15
2.1.2.2 Client-Server Configuration	15
2.1.2.3 Distributed Network Environment	15
2.1.3 Video Surveillance Using Remote SecurOS Security System	15
2.2 Software And Hardware Platform	16
2.2.1 Administrator Workstation System Requirements	17
2.2.2 Operator Workstation System Requirements	17
2.2.3 Video Server System Requirements	18
2.2.4 Audio Subsystem Requirements	18
2.2.5 Notification Subsystem Requirements	19
2.2.6 Access Control/Fire Alarm Subsystem Requirements	19
2.2.7 Environment Requirements	19
2.2.7.1 Computer Name Restrictions	19
2.3 Software Implementation. SecurOS' Subsystems	19
3 SecurOS Installation	21
3.1 Installing And Configuring The Configuration Server	21
3.1.1 Installing and Configuring the SecurOS on Video Server	21
3.1.1.1 Hardware Installation	21
3.1.1.1.1 Guardant Key Installation	21
3.1.1.1.2 TVISS Boards Installation and Cameras Connection	21
3.1.1.2 License Key	22
3.1.1.2.1 The Key is a part of a product	22
3.1.1.2.2 Request the key by e-mail	22
3.1.1.3 Software Installation	23

3.1.1.3.1 Using Current Parameters of the Windows User Account needed for PostgreSQL	24
3.1.1.3.2 Using Current Parameters of the Database and Administrator User Account	24
3.1.1.3.3 Software Installation Procedure.	25
3.1.1.4 Initial Configuration	31
3.1.1.4.1 Initial Configuration Using The System Configuration Wizard	31
3.1.1.4.2 Restoring Configuration.	39
3.1.1.4.3 Start with Empty Database	40
3.1.2 Launching SecurOS On The Configuration Server.	40
3.2 Installing, Launching and Configuring Peripheral Servers and Operator Workstations	41
3.2.1 Adding To The Network And Configuring Peripheral Servers And Operator Workstations.	42
3.2.2 SecurOS Installation On Peripheral Servers.	43
3.2.3 SecurOS Installation On Operator Workstation	46
3.2.4 Installing Additional Multimedia Components	47
3.2.5 Launching And Configuring SecurOS On Peripheral Servers	47
3.2.6 Launching SecurOS On Operator Workstation.	49
4 SecurOS Administration Overview	50
4.1 Working With Control Panel	50
4.1.1 Control Panel Activation.	50
4.1.2 Administration Mode.	51
4.1.2.1 Object Tree	52
4.1.2.2 Administrator Toolbar.	52
4.1.3 User Session Administration	52
4.1.4 Getting Help.	53
4.1.5 Hide Control Panel	53
4.2 Working with Objects	54
4.2.1 Creating Objects	54
4.2.1.1 Creating Objects Limits	54
4.2.2 Editing Object Settings.	55
4.2.3 Deleting Objects	55
4.2.4 Disabling Objects	55
4.2.5 Renaming Objects.	55
4.2.6 Searching Objects.	56
4.3 Working with Object Table Parameters	57
4.4 Managing User Rights Within Security Network.	57
4.4.1 User Registration. Setting up User Rights.	58
4.4.1.1 Default User Accounts.	58
4.4.2 Changing Superuser Password	58
4.5 SecurOS Logging.	59
4.6 Updating License Key on All Servers.	60
4.6.1 License Expiration Reminder	60
4.7 IP-Device Manager.	61
4.7.1 Specification	62
4.7.2 Basic Operations.	66
4.7.2.1 Launching IP-Device Manager.	66
4.7.2.2 Searching Devices in the Network.	67
4.7.2.3 Adding IP Device.	67
4.7.2.4 Editing Parameters and Setting up IP Device Usage.	68
4.7.2.5 Copying IP Device.	70
4.7.2.6 Deleting IP Device.	71
4.8 Health Monitor self-diagnostic Module	72
4.9 Using Camera's Edge Storage	76
4.9.1 Setting up System to Use Local Data Storage.	77
4.9.1.1 Setting up IP Camera Equipped with Edge Storage.	77
4.9.1.2 Setting up SecurOS Objects	78

4.9.2 Synchronization Procedure Features	79
5 Core Subsystem	81
5.1 Working Principles	81
5.2 Object Reference	81
5.2.1 System	82
5.2.2 Security Zone	83
5.2.2.1 Setting Up Event Redirection	84
5.2.3 Database	88
5.2.4 Department	90
5.2.5 User Account	90
5.2.6 Active Directory Storage	91
5.2.7 User Rights	93
5.2.8 Computer	96
5.2.8.1 Servers to connect	99
5.2.8.1.1 Operations with the Servers to connect List	103
5.2.8.2 Auto login	104
5.2.9 Monitoring center agent	105
5.2.10 Remote system	106
5.2.11 Event Filter	107
5.2.12 SNMP agent	111
5.2.12.1 Setting up Windows Management and Monitoring Tools	111
5.3 Configuration Examples	113
5.3.1 Defining Access Levels to Individual Objects	114
5.3.2 Configuration of Network Domain User Rights	114
5.3.2.1 Settings for Windows NT Provider	115
5.3.2.2 Settings for LDAP Provider	115
6 Interface Subsystem	116
6.1 Object Reference	116
6.1.1 Desktop	116
6.1.2 Map	116
6.1.2.1 Maps Working Principles	118
6.1.2.2 Drawing Map Layers	118
6.1.2.3 Working with Map Layers	119
6.1.2.4 Working with Map Objects	121
6.1.3 Map Window	122
6.1.4 Event Viewer	123
6.1.5 External Window	123
6.1.6 HTML Form	124
6.1.7 HTML Dialog	125
7 Video Subsystem	127
7.1 Hardware Decoding	127
7.2 Multi-streaming	130
7.3 Frame Rate Reduction	131
7.4 Working Principles of Motion Detection Zones	131
7.4.1 Managing Motion Detection Zones	132
7.4.1.1 Creating Zones	132
7.4.1.2 Showing Zones	132
7.5 Special Settings for Video Subsystem Components	132
7.5.1 Camera Image Control	133
7.5.2 Video Monitor Settings	133
7.5.3 Record Buffer Settings	133
7.5.4 Archive Recording	134

7.5.4.1 Disk Volume Settings.	134
7.5.4.2 Video Recording Settings.	134
7.5.4.3 Long-term Archive Settings And Archive Converter.	135
7.6 Export Video Using Monitor	135
7.7 Object Reference	136
7.7.1 System Objects	137
7.7.1.1 Video Capture Device	137
7.7.1.1.1 AC Recorder.	139
7.7.1.2 Camera	140
7.7.1.3 Defocus detector.	149
7.7.1.3.1 Fine Tuning Recommendations.	151
7.7.1.4 Layout	152
7.7.1.5 View	154
7.7.1.6 Zone	154
7.7.1.7 Light Detector	158
7.7.1.8 PTZ Controller.	159
7.7.1.9 PTZ Device	160
7.7.1.10 Archive Converter	161
7.7.1.11 Archiver	165
7.7.1.12 Image Processor.	167
7.7.1.13 RTSP Server.	167
7.7.1.14 EdgeStorage Sync.	171
7.7.2 User Interface Objects.	171
7.7.2.1 Monitor	171
7.7.2.2 Media Client	177
7.7.2.2.1 Working with Views.	191
7.7.2.3 Archive Converter Dialog.	196
7.7.2.4 Archiver Dialog	197
7.8 Configuration Examples	197
7.8.1 Standalone Configuration.	198
7.8.2 Video Server + Operator Workstation	199
7.8.3 Setting Up Camera.	200
7.8.3.1 Adding Video Capture Device	200
7.8.3.2 Adding Camera to System.	201
7.8.3.3 Adding Camera to Monitor.	202
7.8.3.4 Adding User Rights	203
7.8.3.5 Setting up telemetry.	204
7.8.3.5.1 Setting up telemetry for IP devices	204
7.8.3.5.1.1 Exclusive Telemetry Control.	206
7.8.3.5.2 Setting up telemetry with PTZ Controller Creation.	207
7.8.4 Joystick Configuration	210
8 Audio Subsystem	211
8.1 Operation Modes	211
8.1.1 Synchronized Audio/Video Recording and Playback	211
8.1.2 Separate Audio Recording and Playback	211
8.2 Object Reference	212
8.2.1 System Objects	212
8.2.1.1 Audio Capture Device	212
8.2.1.2 Microphone	215
8.2.2 User Interface Objects.	216
8.2.2.1 Audio Player	217
8.3 Example of System Configuration for Synchronized Audio/Video Recording and Playback.	219
9 I/O Subsystem	220

9.1 Object Reference	220
9.1.1 Sensor	220
9.1.2 Relay	221
9.1.3 CCTV Keyboard or joystick	222
9.1.3.1 Bosch Intuikey	223
9.1.3.2 Panasonic WV-CU950	225
9.1.3.3 Pelco KBD300A	226
9.2 Configuring System to Work with Wiper	227
10 Notification Subsystem	228
10.1 Object Reference	228
10.1.1 E-mail Message Service	228
10.1.2 E-mail Message	229
10.1.3 Short Message Service	230
10.1.4 Short Message	230
10.1.5 Audible Notification Service	231
11 Automation Subsystem	232
11.1 Working Principles	232
11.1.1 Time Zones	232
11.1.2 Macros	232
11.1.3 Scripting	232
11.1.4 Integration with 3rd Party Systems	233
11.2 Object Reference	233
11.2.1 Time Zone	233
11.2.2 Macro	234
11.2.3 Program	236
11.2.4 VB/JScript program	237
11.2.5 IIDK Interface	239
11.2.6 HTTP Event Gate	240
11.3 Setting up Macros and Scripts	245
11.3.1 Macros	245
11.3.2 VB/JScript programs	246
12 Light Integration	247
12.1 General Description	247
12.2 Setting Up Integration	247
12.3 SecurOS Integrations	248
12.3.1 Bolid	248
12.3.2 FortNet	250
12.3.3 Yantar	251
13 Keyboard Shortcuts	252
13.1 Administration Toolbar	252
14 Appendixes	253
14.1 Appendix A. Upgrading/Uninstalling Software	253
14.1.1 Upgrading Software	253
14.1.2 Uninstalling Software	253
14.1.3 Release 6.2 Updating Procedure	254
14.1.3.1 Software Updating On Configuration Server	255
14.1.3.2 Updating Software On Peripheral Servers	255
14.2 Appendix B. Quick Video Subsystem Configuration	256

14.3 Appendix C. System Utilities.	257
14.3.1 ISS Hardware Report Utility	258
14.3.2 ISS System Report Utility	259
14.3.3 ISS Media Export Utility	261
14.3.3.1 Export Settings dialog	263
14.3.3.2 Command-line parameters.	264
14.3.4 gtUSB Configuration Utility	266
14.3.5 ISS Startup Configuration Utility	267
14.3.6 DSAdmin Utility	269
14.3.7 ISS Database Update Utility	270
14.3.8 ISS Object Types Database Editor	271
14.3.8.1 Names Tab	273
14.3.8.2 Events Tab	273
14.3.8.3 Reacts Tab	275
14.3.8.4 Markers Tab.	276
14.3.8.5 States Tab	277
14.3.8.6 State Rules Tab.	278
14.3.9 ISS Server Role Manager Utility	280
14.4 Appendix D. TCP/IP Ports Used by SecurOS.	281
14.5 Appendix E. Additional Windows Settings	283
14.5.1 Installing Multimedia Components and Services under MS Windows Server 2008 R2	283
14.5.2 Installing Media Foundation under MS Windows Server 2012 R2.	283
14.5.3 Installing Microsoft .NET Framework 3.5 under MS Windows Server 2012 R2.	284
14.5.4 SMTP Mail Server Installation and Configuration.	284
14.5.5 Win7/Win8.1/Windows Server Automatic Login Configuration	287
14.5.6 Starting Interactive Services Detection Service under Win8/8.1/Server 2012 R2	288
14.5.7 Complete Disabling UAC under Win8/8.1/Server 2012 R2 with the help of System Registry.	288
14.5.8 Disabling Disk Cleanup Master	288
14.6 Appendix F. Technical Support Information	289

Index**291**

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. The user should have read the **SecurOS Installation Guide** prior to reading this document, because it gives introductory information on how to plan their system.

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 (**SecurOS Installation Guide**, **SecurOS User Guide** etc.). One can find these manuals as separate files on the SecurOS installation CD or download them from our website (www.isscctv.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:

- in USA:
phone: +1 732 855 1111 (Monday to Friday, 8:30am - 6pm EST);
e-mail: support@isscctv.com

- in Russia:
phone: +7 (495) 645 21 21 (Monday to Thursday, 9am - 6pm MST; Friday 9am - 5pm MST);
e-mail: support@iss.ru
- in Brazil:
phone: +55 11 2262 2894 (Monday to Friday, 9am - 6pm BRT);
e-mail: suporte@isscctv.com
- in Mexico:
phone: +52 1 551330 0181 (Monday to Friday, 9am - 6pm CDT);
e-mail: supportlatam@isscctv.com
- in Colombia/Ecuador:
phone: +57 300 442 2808 (Monday to Friday, 9am - 6pm COT/ECT);
e-mail: supportlatam@isscctv.com
- in Chile:
phone: +56 9 6573 2993 (Monday to Friday, 9am - 6pm CLT);
e-mail: supportlatam@isscctv.com
- in Ukraine:
phone: +38 (044) 238 24 83 (Monday to Friday, 9am - 6pm EET);
e-mail: support@isscctv.com.ua
- in Peru/Bolivia:
phone: +51 997 111 678 (Monday to Friday, 9am - 6pm PET/BOT);
e-mail: supportlatam@isscctv.com
- in Argentina:
phone: +54 91152528779 (Monday to Friday, 9am - 6pm ART);
e-mail: supportlatam@isscctv.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 security system" 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.
monospace	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. Additionally, basic system configurations, determined by type and number of SecurOS servers and workstations used are considered.

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 the following main categories that define the SecurOS software installation type:

- **Video Server.**
- **Operator Workstation.**
- **Administrator 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 cameras (IP and/or CCTV analog 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). The *Video Server* installation also includes all the functionalities of the **Administrator Workstation** and **Operator Workstation** installation types.

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.

2.1.1.1.3 Administrator Workstation

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

The *Administrator Workstation* is a client computer similar to the *Operator Workstation* but has an additional administrator interface for configuring the security network. On such a computer one can perform the following administrator operations:

- Create and configure system objects.
- Delete existing objects.
- Change the parameters of the created and operating objects.

2.1.1.2 Classification of Roles in Configuration Management

The role of the server defines its place in the SecurOS network configuration management procedure. Each SecurOS network computer must be assigned one of the following:

- **Configuration Server.**
- **Peripheral Server.**

2.1.1.2.1 Configuration Server

Reliable operation of a 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 present 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.

The *Configuration Server* is assigned during system installation. The *Configuration Server* can be represented by one of the following SecurOS network computers — *Video Server* or *Administrator Workstation*.

Warning! Only one network server can be assigned as the *Configuration Server*.

In the *SecurOS Xpress* and *SecurOS Lite* editions, the *Video Server* is by default the *Configuration Server*.

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**).

2.1.1.2.2 Peripheral Server

Any server that is not the *Configuration Server*, is a *Peripheral Server*. The peripheral server is assigned during the system installation and can be represented by any of the typical network computers — *Video Server* or *Administrator Workstation*.

Warning!

1. The *Peripheral Server* can't apply configuration changes independently.
2. 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 of disconnection, the system will automatically shutdown on the given *Peripheral Server* and all *Operator Workstations* connected to it.

2.1.1.2.3 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.

2.1.1.2.3.1 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).

2.1.1.2.3.2 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 *Peripheral Servers*, the administrator (or operator) makes changes to the Object Tree for that *Computer* (or *Computers*).
2. If a *Peripheral Server* 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 *Peripheral Server*.
-
3. The *Configuration Server* processes the request(s). It applies changes by first renewing it's 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*.

2.1.1.2.3.3 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.

2.1.2 Types Of System Configurations

This section describes basic system configurations determined by type and number of SecurOS servers and workstations used.

2.1.2.1 Standalone Configuration

A standalone configuration assumes that the SecurOS modules and database are installed on a single network server, which is also an *Operator Workstation*. This configuration is typical for small-scale entry-level systems.

2.1.2.2 Client-Server Configuration

In a client-server configuration, server and client components are deployed on different computers of the SecurOS network, providing specific functionalities according to the types of components installed. This configuration is typical for mid-sized systems.

2.1.2.3 Distributed Network Environment

In this configuration each security system cluster is maintained with the individual instance of SecurOS, which is implemented in a Client-Server architecture. This configuration is intended to be used for security systems within branched networks with large amounts of data streams and makes it possible to reduce load on the server components.

2.1.3 Video Surveillance Using Remote SecurOS Security System

This functionality is available in the *SecurOS Monitoring & Control Center* only.

In certain cases it may be required to create several independent security systems with a single top level control center. This case is possible, for example, for banking, where all branches are monitored with the help of a single Monitoring Center.

Two types of Monitoring Centers, differing in functionality, can be created and configured within SecurOS:

1. Monitoring Center working with remote video archives;
2. Monitoring Center working with local video archives.

The remote security system is controlled and monitored via a set of objects, which are created on the Monitoring Center server when it is configured (see **Remote system**). To work with the video streams from the remote system, copies of the cameras from the remote system are created on the Monitoring Center's server. The operator can perform different actions with the video depending on the Monitoring Center type: in the first case, the video streams are only available for viewing (access to the video archive created by the remote system cameras is allowed), and in the second case, the video streams can be recorded locally on the Monitoring Center server (access to the video archive created by the remote system camera is forbidden).

Monitoring Center working with remote video archives

Monitoring Center working with remote video archives allows operator to perform the following operations:

1. Viewing video provided by the remote system's *Cameras* in real-time;
2. Working with *Alarms* and *Bookmarks*;
3. Converting video archive stored on the remote server to AVI / ASF format;
4. Controlling *Cameras* on the remote servers using PTZ.

Monitoring Center working with local video archives

Monitoring Center working with local video archives allows operator to perform the following operations:

1. Viewing video provided by the remote system's *Cameras* in real-time;
2. Recording video streams provided by the remote system's *Cameras*. Recording is executed locally on the Monitoring Center's server;
3. Controlling *Cameras* on the remote servers using PTZ;
4. Other operations using camera cell control elements.

In other words, a Monitoring Center working with local video archives 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.

When planning the system architecture it should be considered that a Monitoring Center working with local video archives requires a much greater TCP/IP bandwidth than a Monitoring Center working with remote video archives. A Monitoring Center working with remote video archives is capable of controlling up to 5000 *Cameras* of the remote security system(s) simultaneously. The number of cameras controlled by the "local" Monitoring Center depends on the system characteristics of the *Video Server*, where the Monitoring Center is deployed (see **Video Server System Requirements**).

To provide Monitoring Center functionality within a SecurOS security system the **Monitoring center agent** and **Remote system** objects of the Core subsystem were designed.

2.2 Software And Hardware Platform

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

2.2.1 Administrator Workstation System Requirements

Table 1. Administrator Workstation System Requirements

Parameter	Requirements
OS	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.
CPU	Intel Core i3-4130/ AMD FX-4350 or above Warning! Hardware decompression of H.264 stream is not supported by AMD CPUs.
RAM	Not less than 4 GB
HDD	Not less than 40 GB
HDD free space for software installation	Not less than 500 MB
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	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.
CPU	Intel Core i3-4130/ AMD FX-4350 or above (for example, Intel Core i5-4xxx). Warning! Hardware decompression of H.264 stream is not supported by AMD CPUs.
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	Not less than 500 MB
HDD free space for operation	Not less than 200 MB

Parameter	Description
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
TCP/IP network speed	Not less than 100 Mbps. 1000 Mbps is recommended to view uncompressed video from several cameras simultaneously

2.2.3 Video Server System Requirements

Table 3. Video Server System Requirements

Parameter	Description
OS	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.
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 stream is not supported by AMD CPUs.
RAM	Not less than 4 GB. 12 GB is recommended
HDD	Not less than 150 GB
HDD free space for software installation	Not less than 500 MB
HDD free space for PostgreSQL installation	Not less than 500 MB
TCP/IP network speed	Not less than 100 Mbps. 1000 Mbps is recommended

2.2.4 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. Alternatively, TVISS-MX/RT/HC video capture card(s) can be used to capture audio, because they have additional audio input on-board.

Notes:

1. If there is no integrated sound card and only a TVISS video capture card is installed, it is necessary to install an additional sound card to playback audio records on this server.
 2. Integrated or additional sound card provides audio capture only from one microphone. If its necessary to capture audio streams from a large number of microphones, TVISS video capture cards should be used.
-

2.2.5 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.

2.2.6 Access Control/Fire Alarm Subsystem Requirements

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

2.2.7 Environment Requirements

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

2.2.7.1 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 16 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 Software Implementation. 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 programming system scripts and macros, and time zone automation controls (see [Automation Subsystem](#)).

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

3 SecurOS Installation

This section describes system installation on different SecurOS servers and workstations.

3.1 Installing And Configuring The Configuration Server

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

3.1.1 Installing and Configuring the SecurOS on Video Server

This section describes installation and configuration of the SecurOS managing server on computer which assigned functionality is *Video Server*.

3.1.1.1 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 and TVISS video capture boards.

The Guardant keys are used for licensing restrictions only. The TVISS boards ensure functioning of the Video server with analog video surveillance cameras, and also are responsible for license restrictions.

3.1.1.1.1 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 section](#)) is selected.

Note. The Guardant key driver can be installed later in a manual mode. For the detailed description of the procedure see the [SecurOS SecurOS Installation Guide](#).

3.1.1.1.2 TVISS Boards Installation and Cameras Connection

For installation of the TVISS video capture boards, they must placed in a available PCI/PCIe slot on the motherboard of the video server. A special cable (dongle) will be provided to connect the board to the video surveillance cameras. These steps must be done before the beginning of the SecurOS software installation.

Detailed description of the procedures of installing TVISS boards and connecting cameras is available in the [SecurOS Installation Guide](#).

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

3.1.1.2 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 TVISS boards) 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. TVISS board key;
3. 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.

3.1.1.2.1 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).

3.1.1.2.2 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 **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).

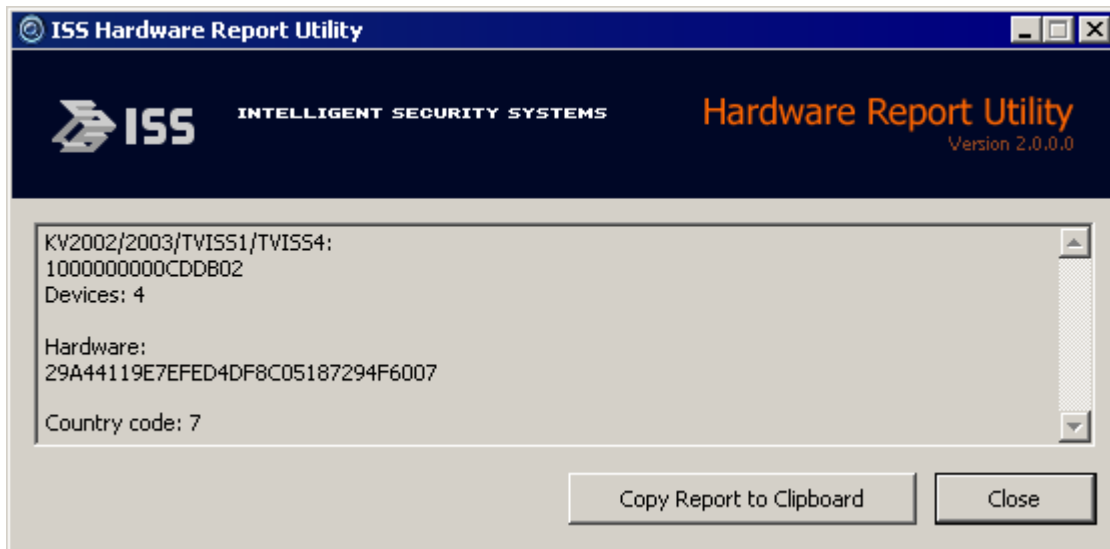


Figure 1. Hardware Report Utility window

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.

3.1.1.3 Software Installation

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

Warning!

1. 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.
2. It's strongly recommended to disable the User Account Control option before installing SecurOS software under Windows 7 and Windows Server 2008 R2.

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

3.1.1.3.1 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.

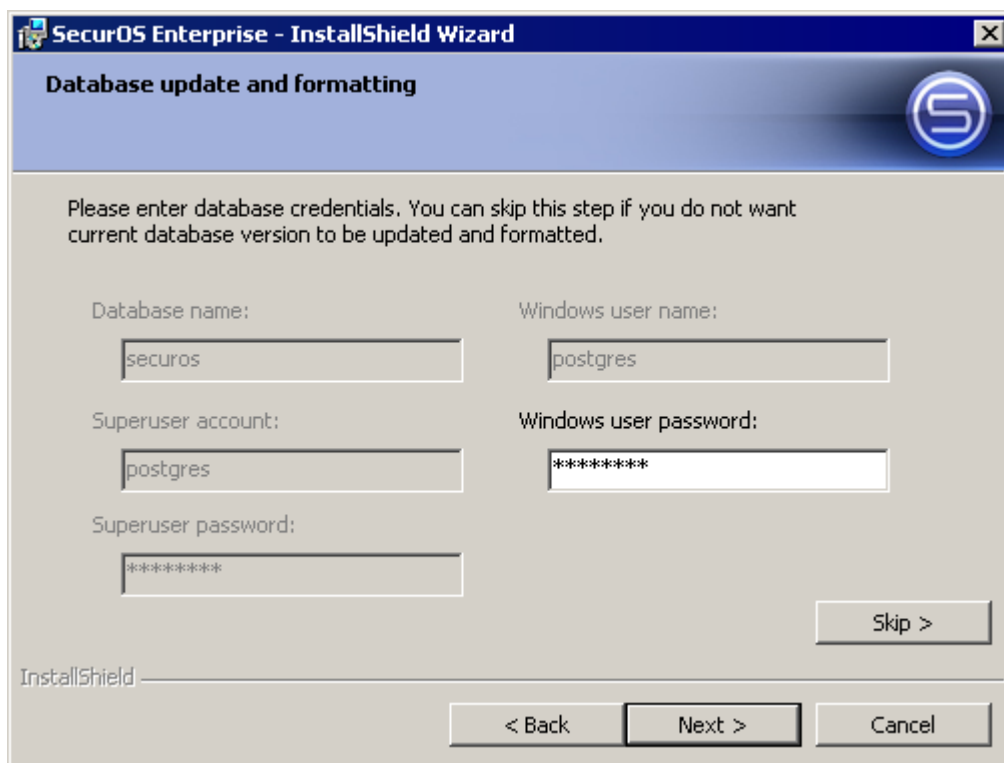


Figure 2. Database update and formatting Window

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.

3.1.1.3.2 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.

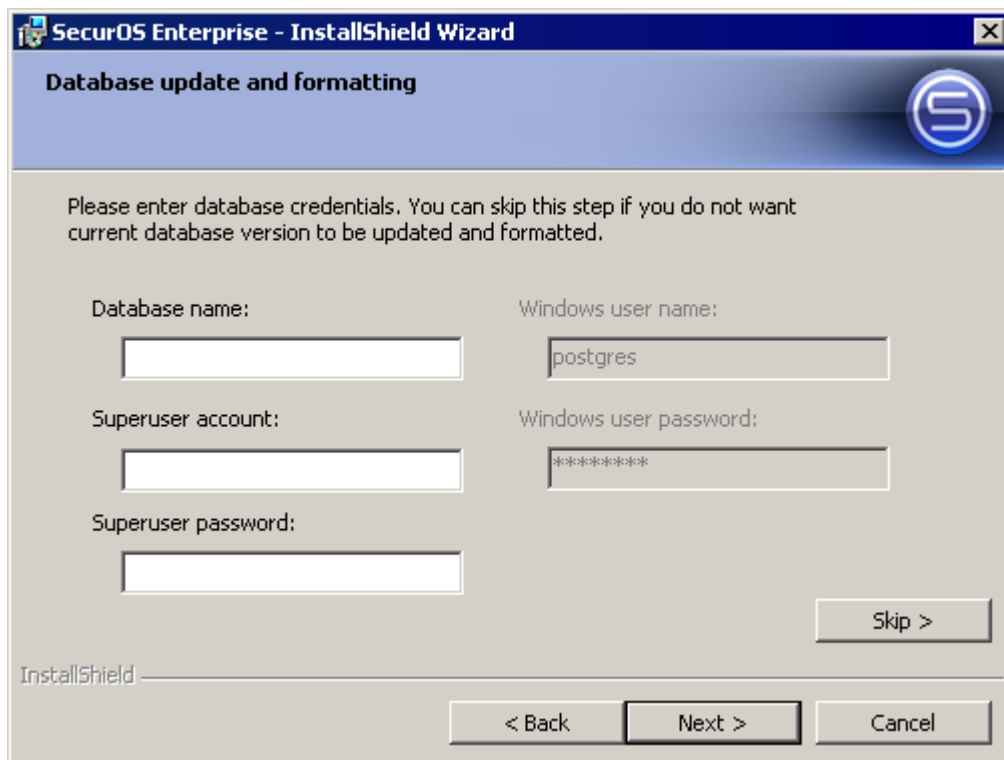


Figure 3. Database update and formatting Window

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.

3.1.1.3.3 Software Installation Procedure

Warning!

1. 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](#));
2. SecurOS software installation is possible only on those computers which names correspond to the requirements stated in [Computer Name Restrictions](#) section.

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).

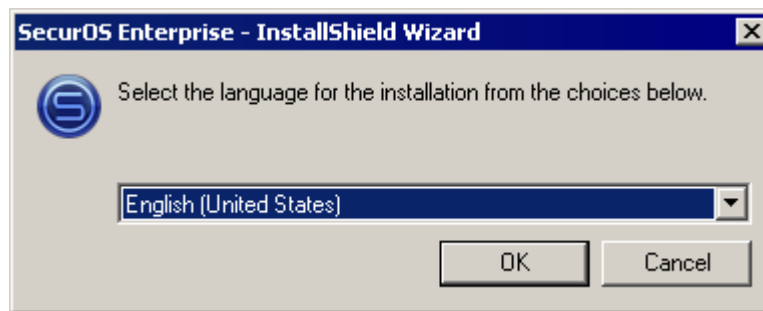


Figure 4. Choose Setup Language window

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).

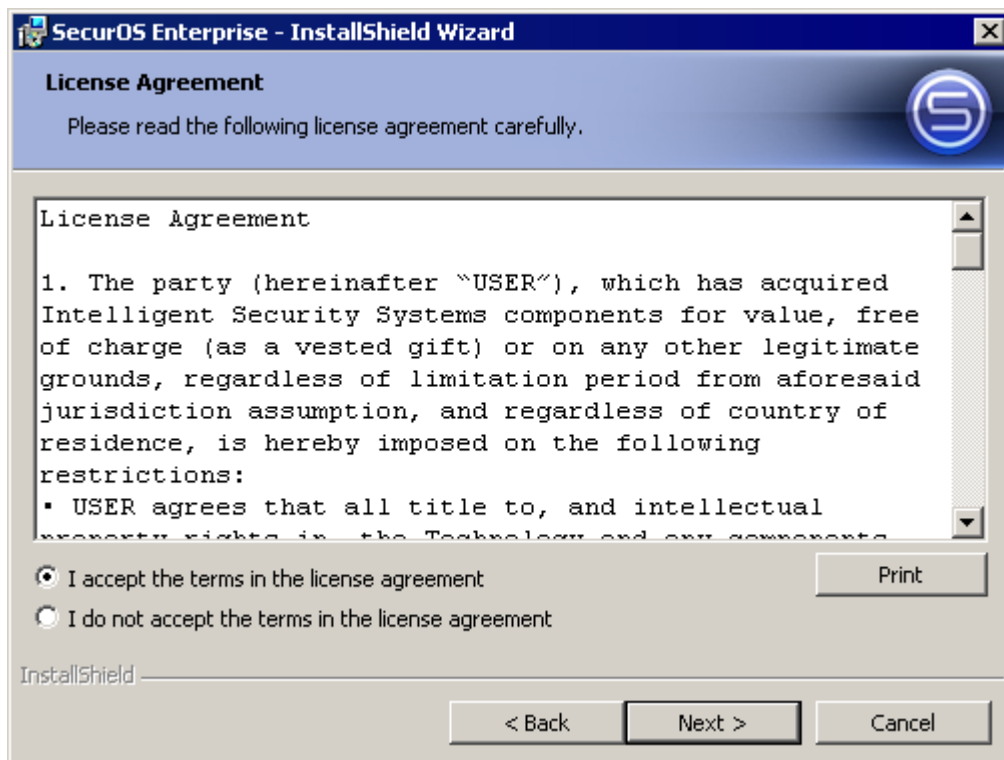


Figure 6. License Agreement window

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

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

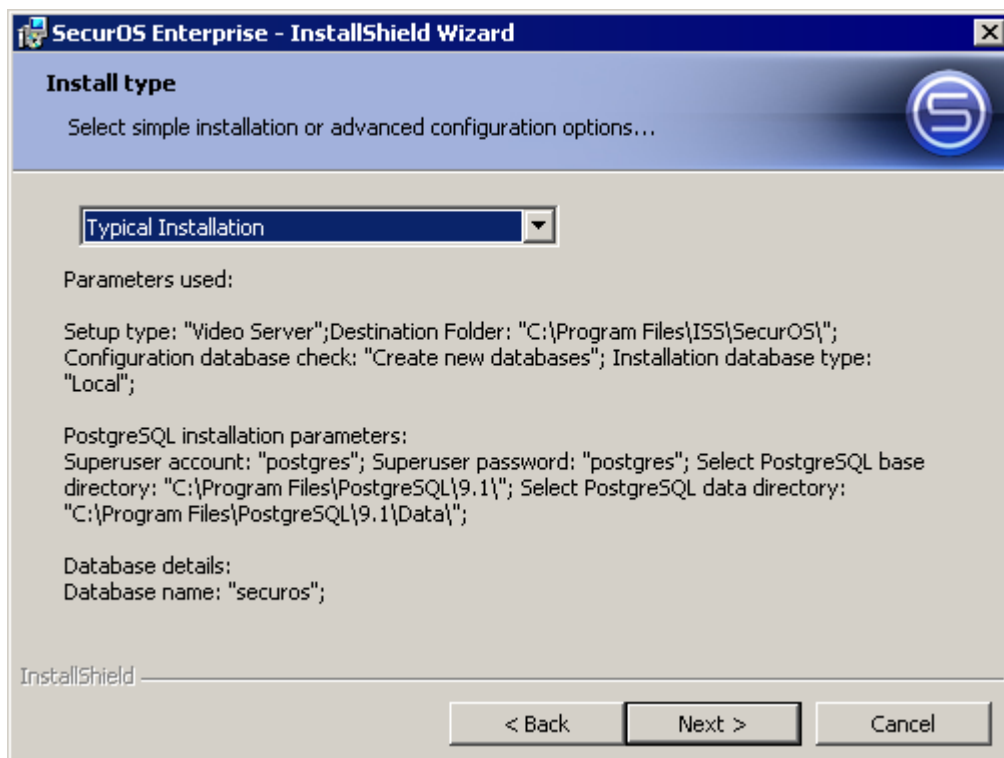


Figure 7. Install Type window

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

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.

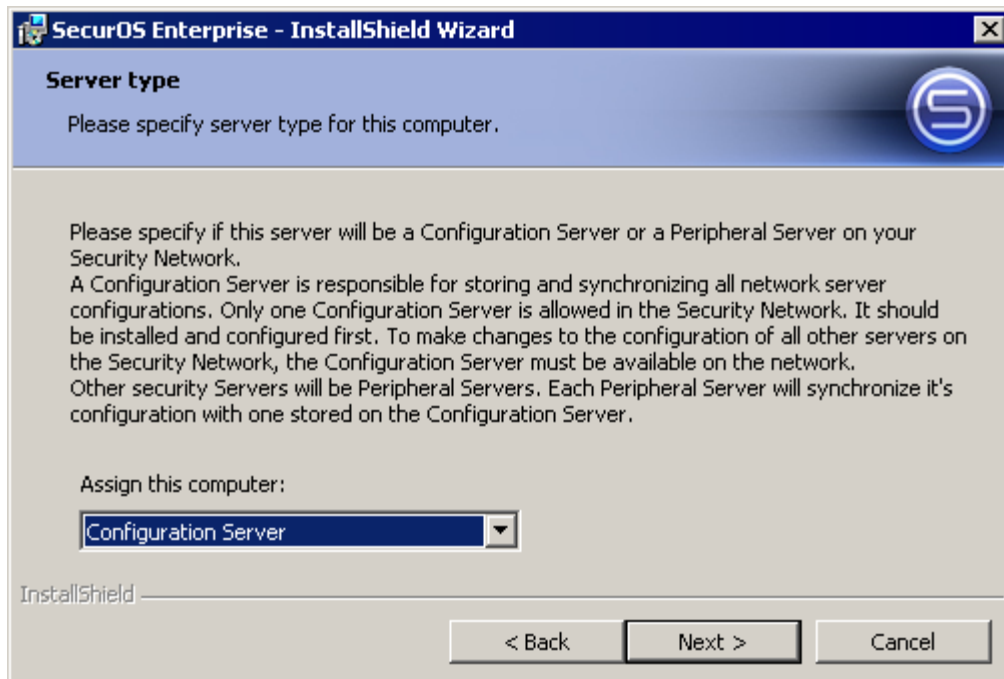


Figure 8. Server Type window

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

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.

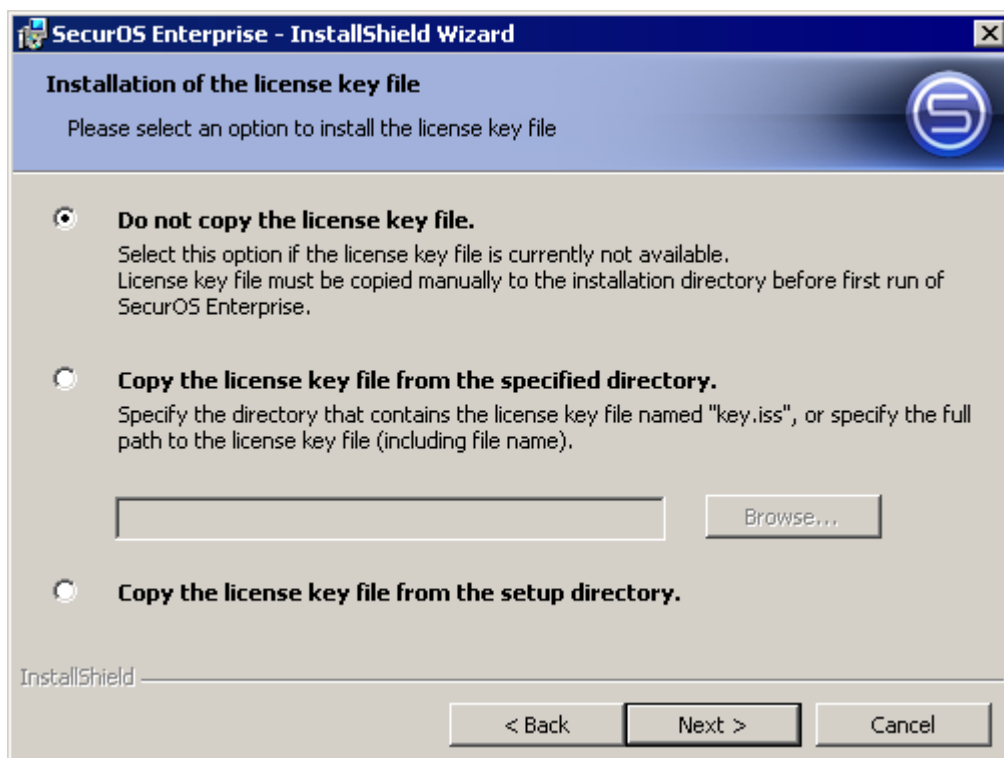


Figure 9. Installation of the license key file window

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 **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 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 to continue.

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

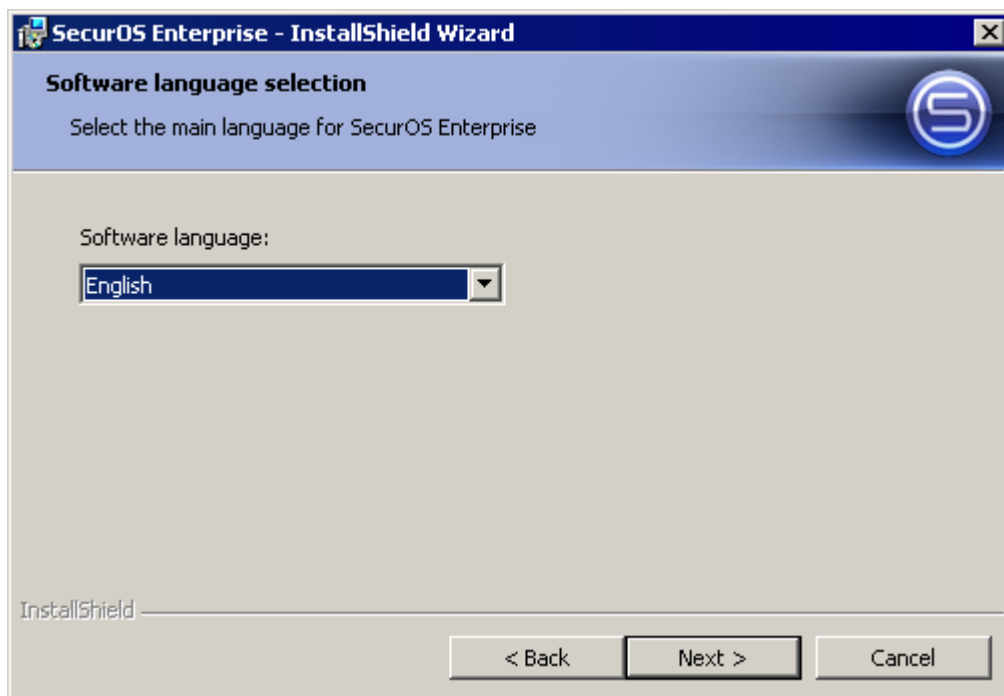


Figure 10. Software language selection window

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 to continue.

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

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

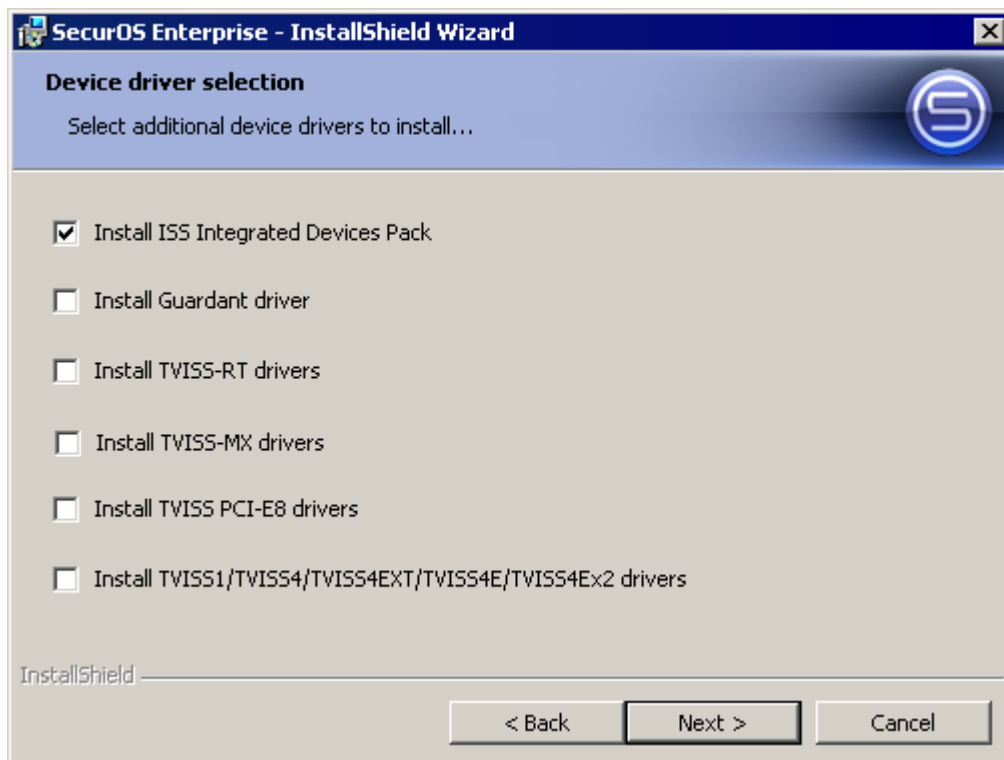


Figure 11. Device driver selection window

Uncheck the default checked **Install ISS Integrated Devices Pack** if it is not proposed to integrate additional devices. Choose the check box of the Guardant or video capture board that was in the delivery set and has already been installed on the computer. Click the **Next** button to continue.

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

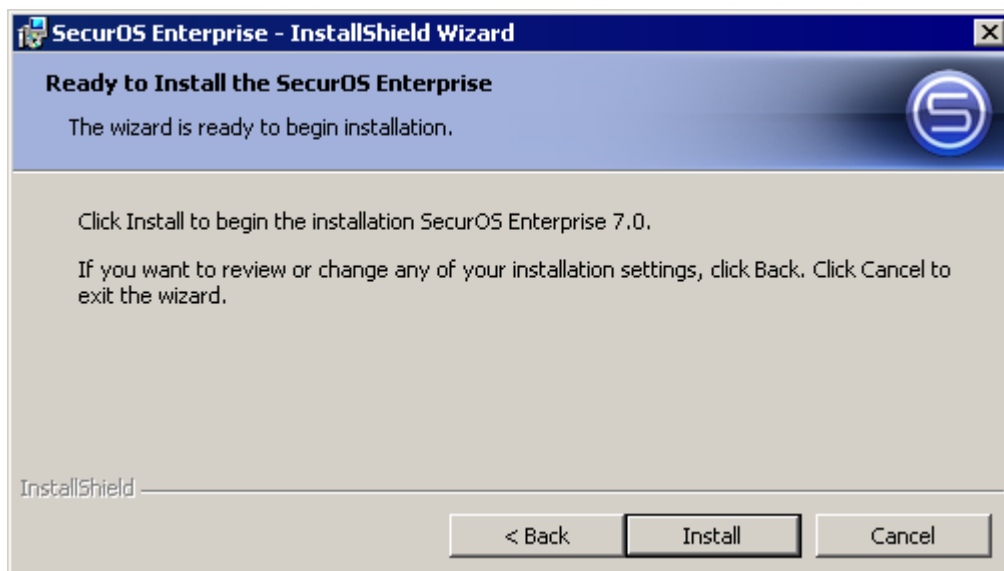


Figure 12. Ready to Install SecurOS window

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.

3.1.1.4 Initial Configuration

Initial SecurOS configuration is carried out on the *Configuration Server* with the help of the *System Configuration Wizard*, which is automatically started at the first start of the software and 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.

3.1.1.4.1 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 by going to the Windows **Start** menu and selecting the following menu options **All Programs** → **SecurOS** → **SecurOS** (see figure 14).

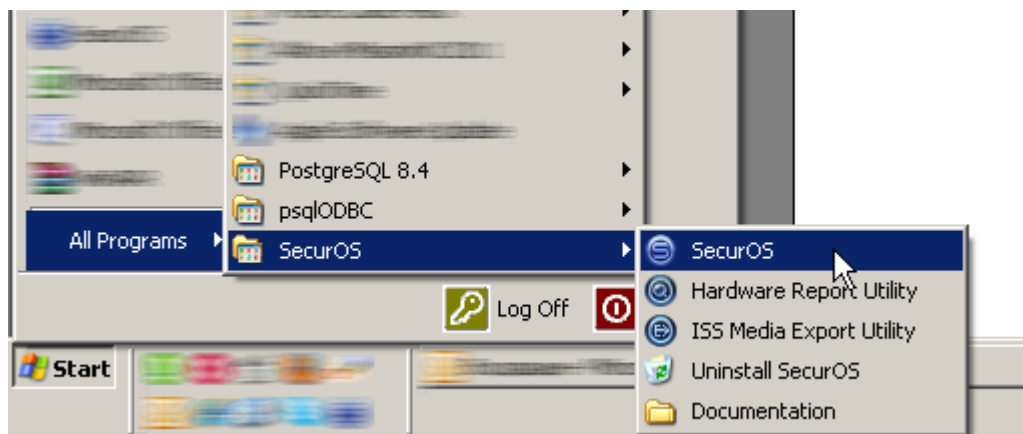


Figure 14. Start menu (All programs)

The system will display an initialization window, in which steps of the procedure of system preparation for initial start (see figure 15) will be displayed.

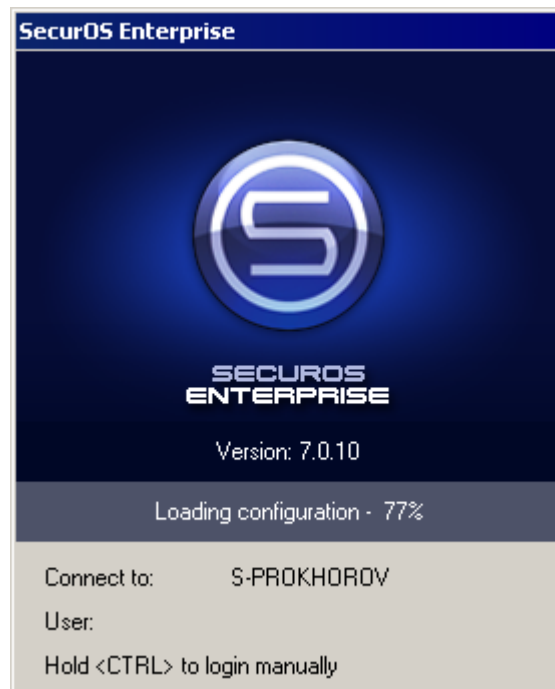


Figure 15. SecurOS initialization window

After the preparation procedure has completed the system will open the *System Configuration Wizard* window which will provide options for system configuration (see figure 16).

2. For basic configuration select the `Configure using Wizard` option that is active by default.

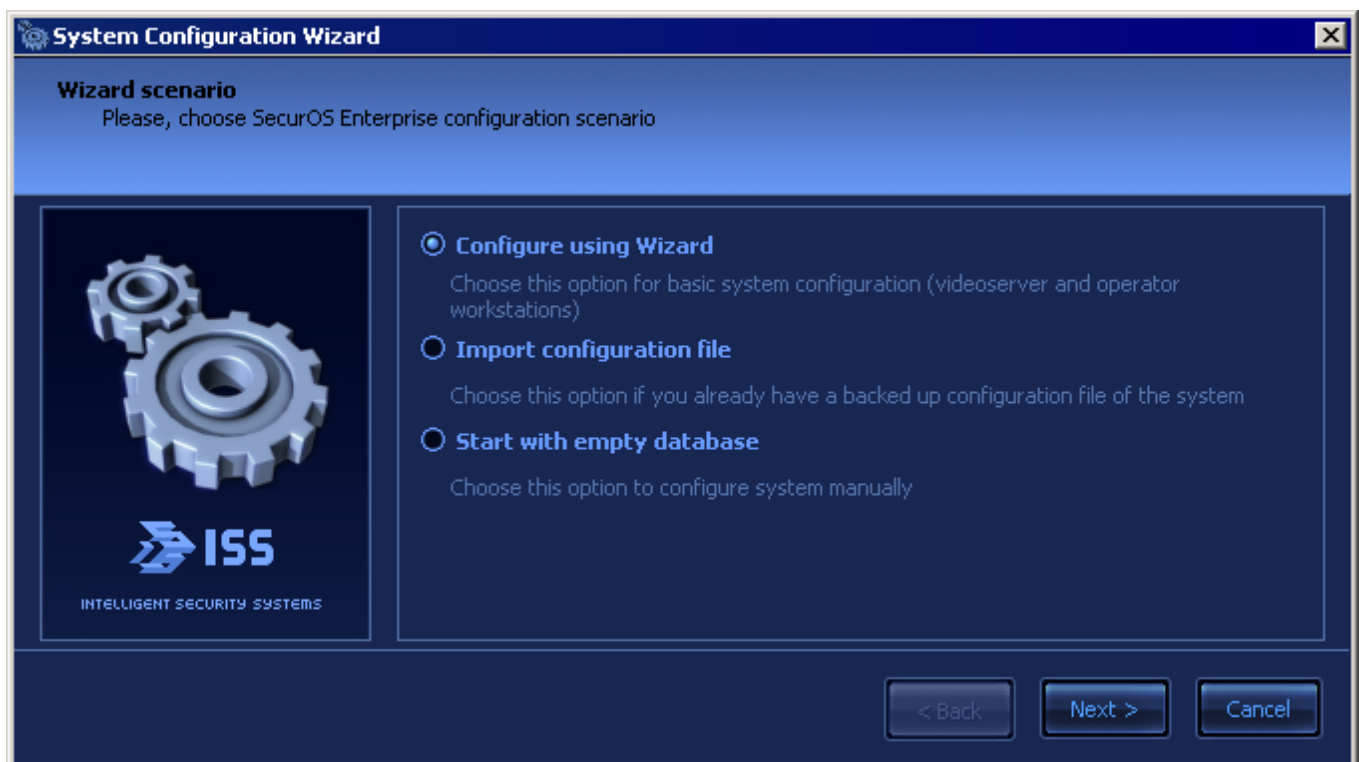


Figure 16. Wizard scenario window

Click **Next** button to continue.

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

3. The **License view** window will appear (see figure 17).

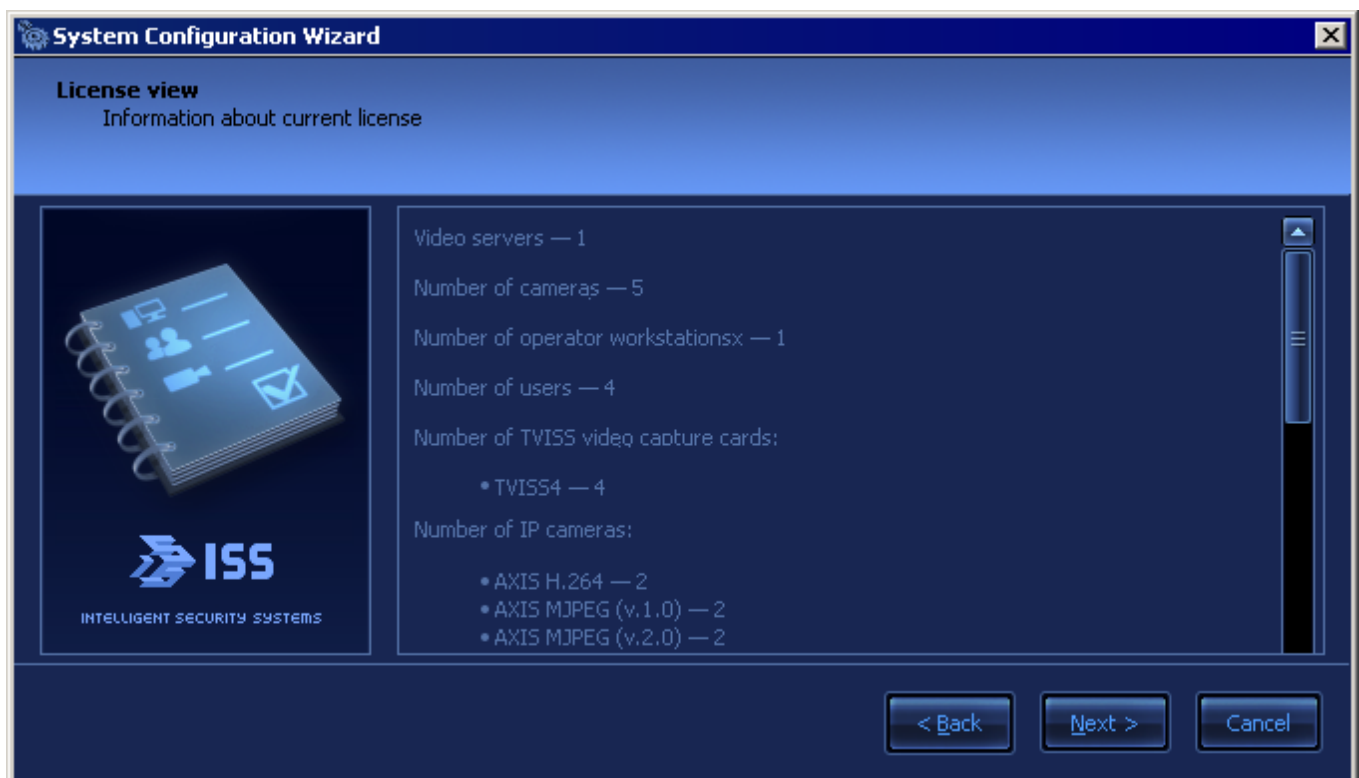


Figure 17. License view window

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

4. The **Superuser password setup** window will appear (see figure 18).



Figure 18. Superuser password setup window

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

The system will display window to enter new parameter values (see figure 19).



Figure 19. Change superuser password window

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

5. System will display **Users setup** window (see figure 20).



Figure 20. 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;
- Shutdown the current SecurOS user session;
- Shutdown SecurOS system.

Simple user can do the following:

- View objects using the user interface;
- Shutdown the current SecurOS user session.

Click **Next** button to continue.

6. System will display the **Computer name and video archive setup** window (see figure 21).

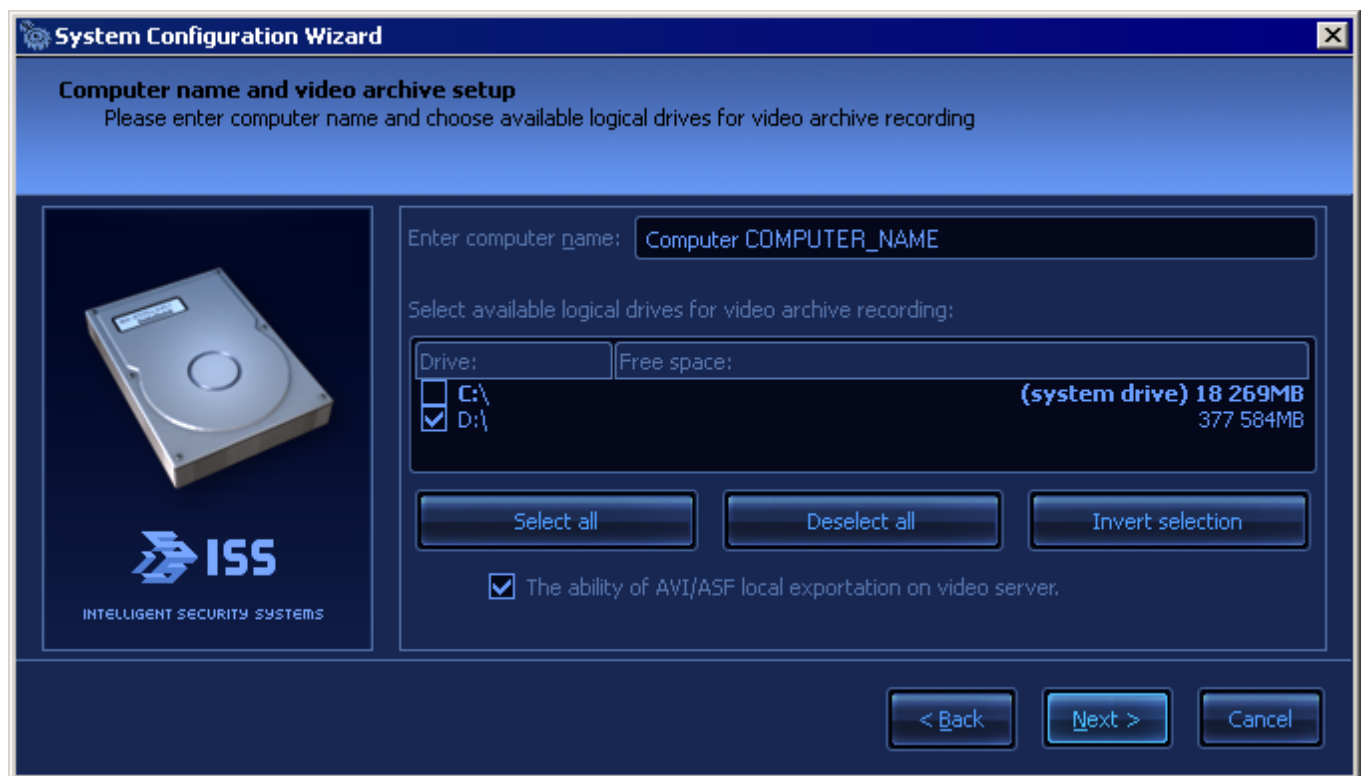


Figure 21. Computer name and video archive setup window

Do the following:

- If necessary edit the *Computer* object name in the **Enter computer 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 in the AVI/ASF format isn't required, clear the **The ability of**

AVI/ASF local exportation on 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.

Click **Next** button to continue.

7. System will display the **Add and configure IP devices** window (see figure 22).

If it is necessary to operate with network IP-devices (for example, IP cameras), click **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.

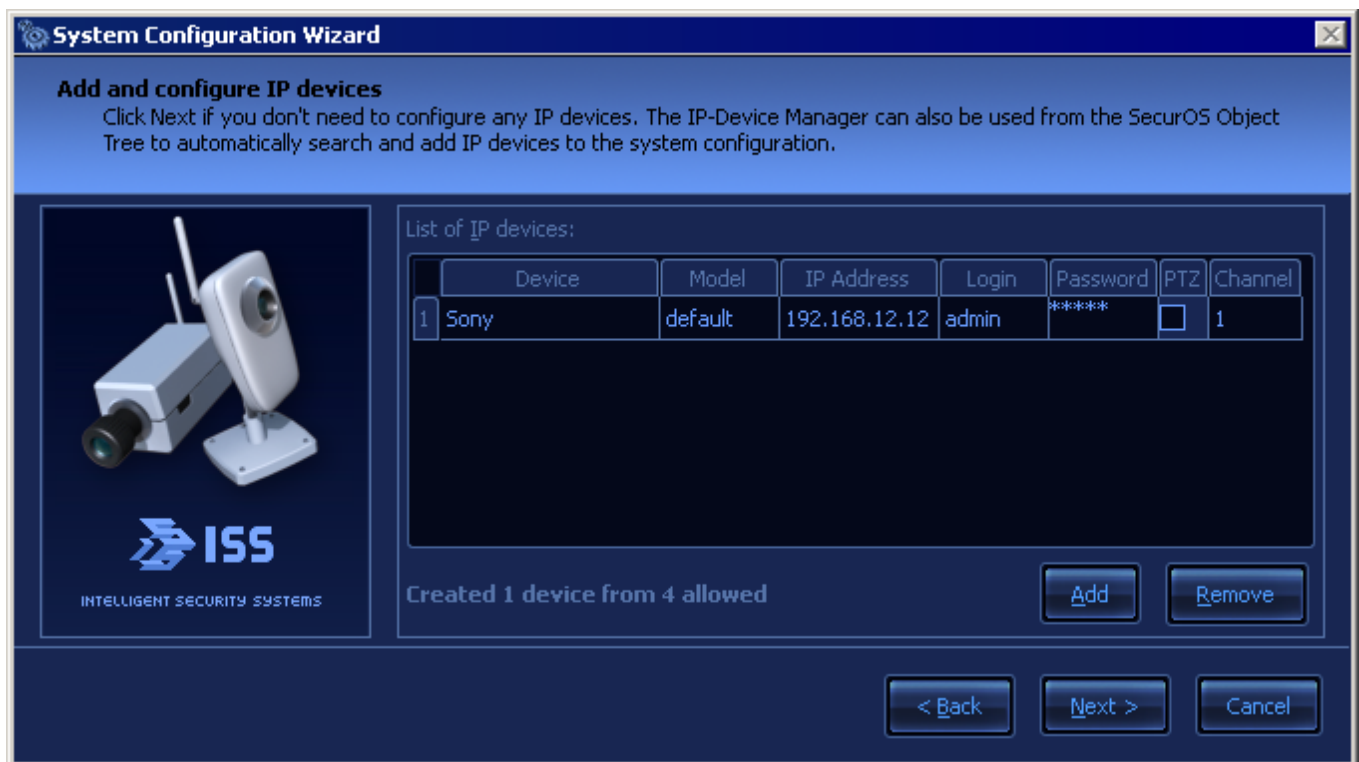


Figure 22. Add and configure IP devices window

Click **Next** button to continue.

Note. IP devices can be added later.

8. If video capture boards are installed on the computer the **Information about installed TVISS cards** window will appear (see figure 23).

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

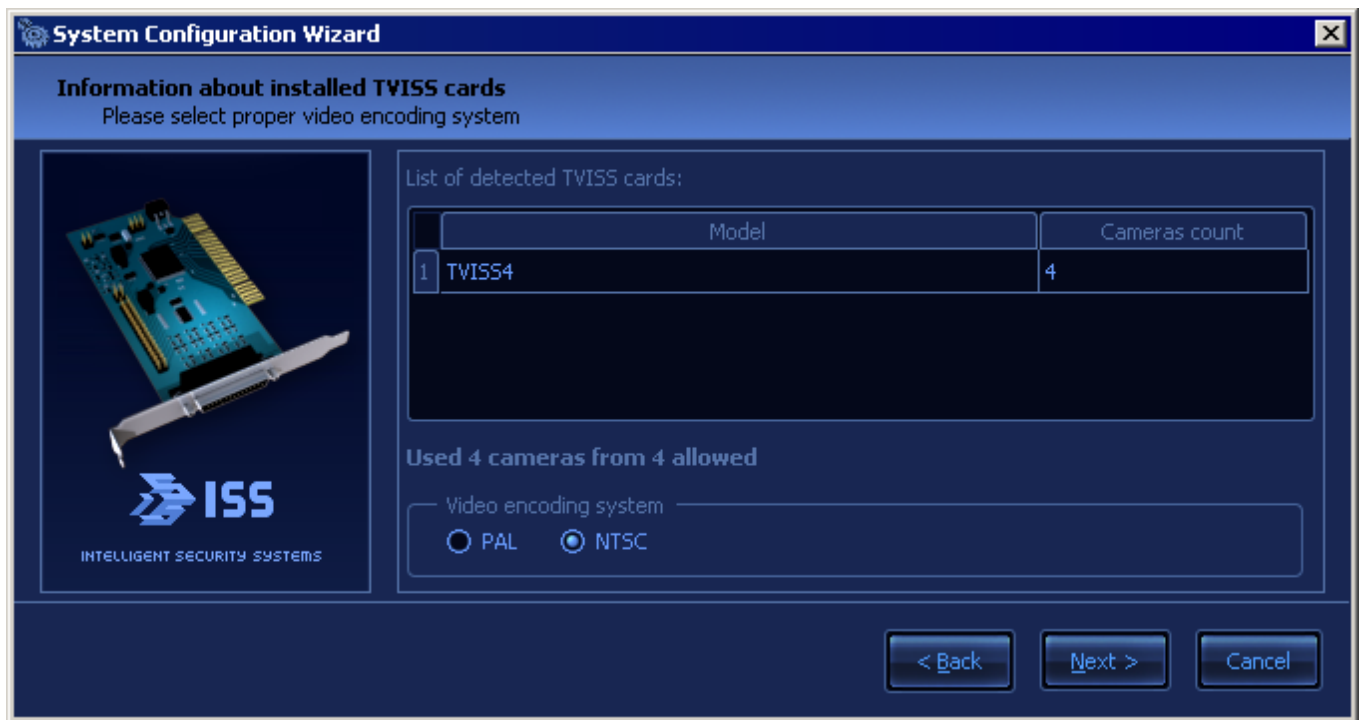


Figure 23. Information about installed TVISS cards window

In the **Video encoding system** block choose the required standard for encoding video signal. Click **Next** button to continue.

9. System will display the **Add operator workstations (OWS)** window (see figure 24).

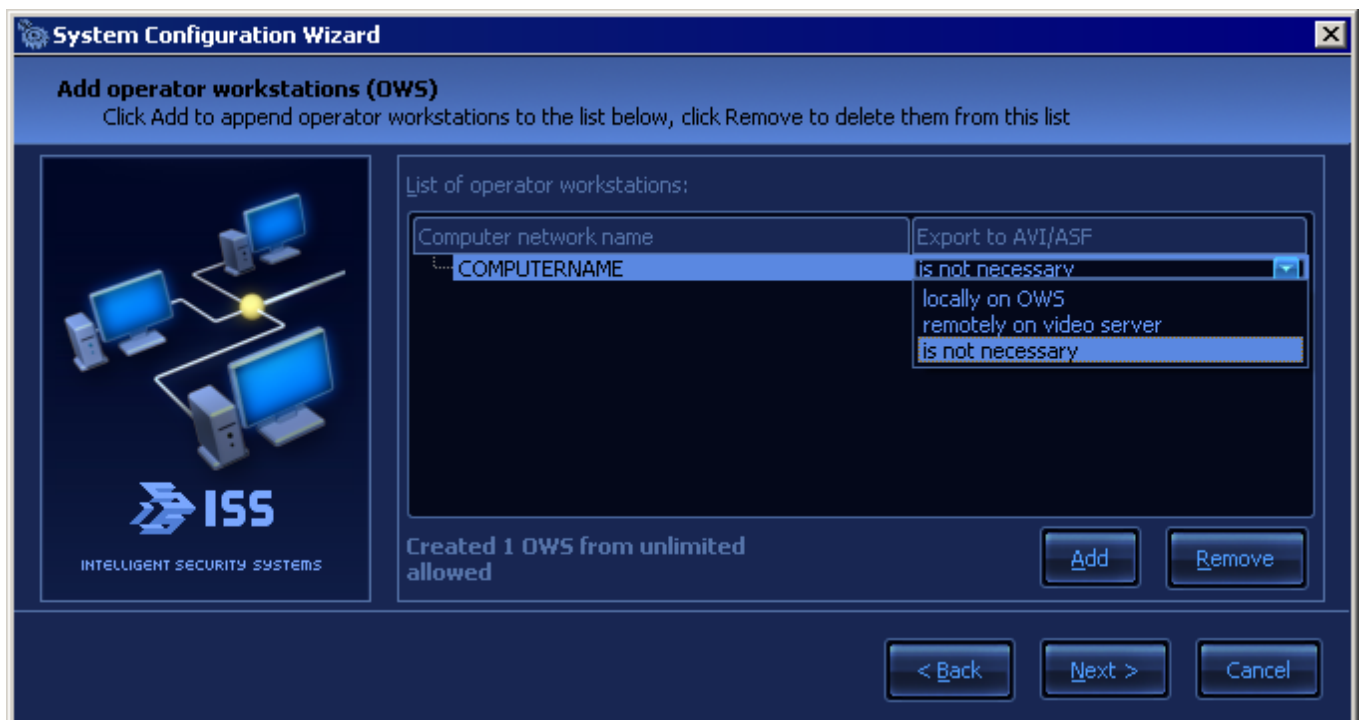


Figure 24. Add operator workstations (OWS) window

To add a *Operator workstation* to the configuration do the following:

- Click **Add** button. The system will add a new line to the **List of operator workstations** block. In the **Computer network name** field set computer name which will be connected to the SecurOS network as an *Operator workstation*.

Note. Computer name should correspond to the value set in the operating system configuration (see **My computer** → **Properties** → **Computer Name**).

Additional Information

The computer name also can be selected from the list of the computers connected to a network. To view the list click the  button in the **Computer network name** field.

- If on the added *Remote operator workstation* it is necessary to export video in the AVI/ASF format, then select the corresponding setting in the **Export to AVI/ASF** field:
 - *locally on OWS* – option to convert/export to AVI/ASF file will be available on an added remote operator workstation;
 - *remotely on video server* – option to convert/export to AVI/ASF file will be available on a video server;
 - *is not necessary* – option to convert/export to AVI/ASF file will not be available.
- Do the described above actions for each *Remote operator workstation* connected to the network. Click **Next** button to continue.

Note. *Remote operator workstations* configuration can be done later.

10. The **Summary information** window will appear (see figure 25).



Figure 25. Summary information window

Review the selected system parameters. If it is necessary to change anything click **Back** button. Set a new value. Click **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 26).

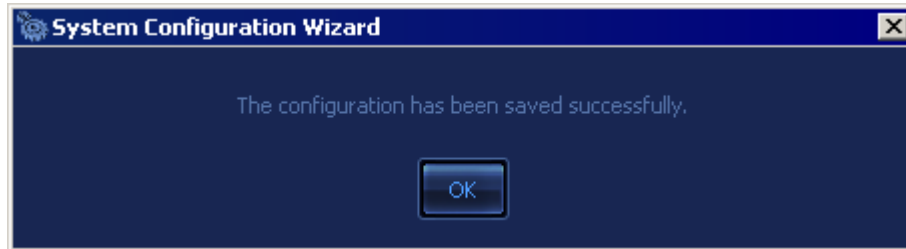


Figure 26. Successful configuration saving message

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

3.1.1.4.2 Restoring Configuration

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

Warning!

1. Version of the backup copy should comply with version of the currently installed SecurOS, otherwise it is not applicable.
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 27).

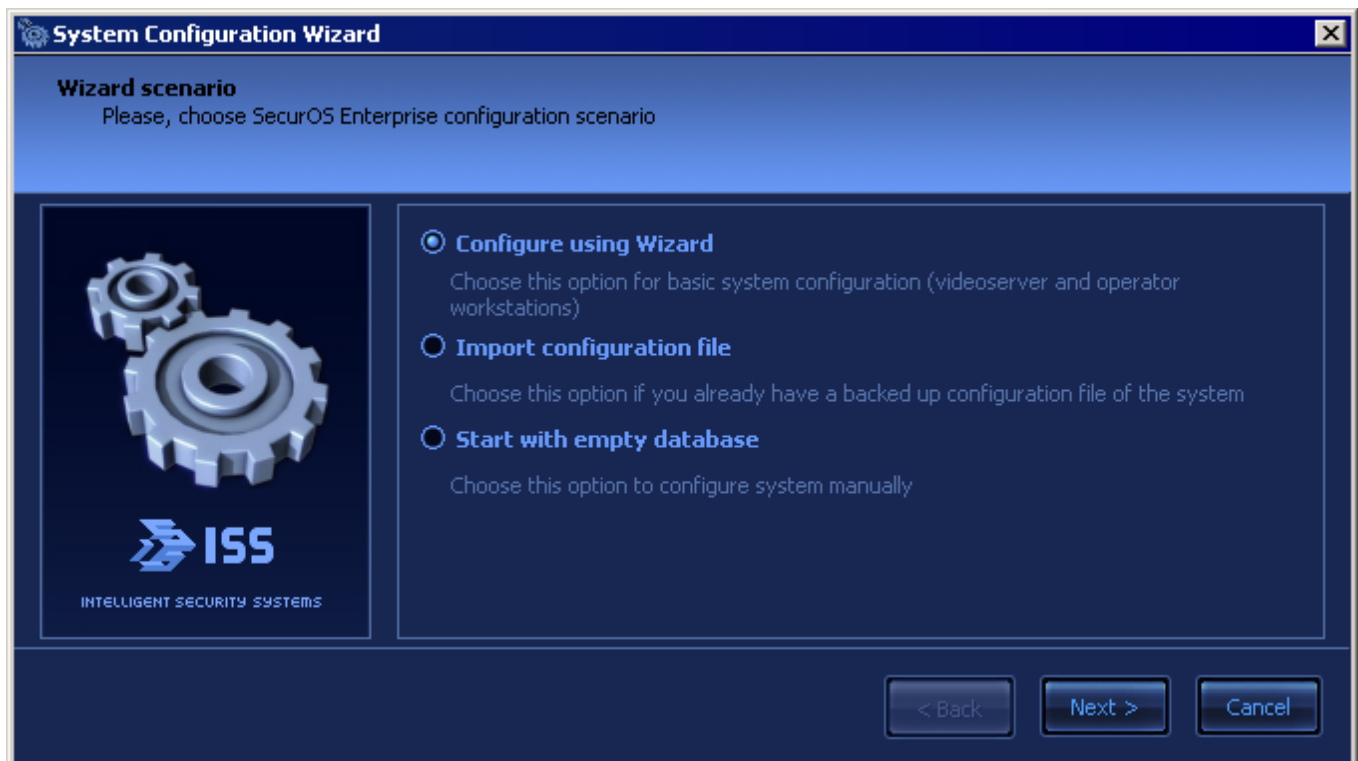


Figure 27. Wizard scenario Window

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

3.1.1.4.3 Start with Empty Database

To start system with empty database select appropriate scenario in the **Wizard scenario** window (see figure 27). If this scenario is used the system start with minimal configuration containing one of each following types: *Security zone, Computer, Desktop* and *Monitor*. Further system configuration is performed in manual mode.

3.1.2 Launching SecurOS On The Configuration Server

To start SecurOS in manual mode from the Windows **Start** menu, select the following menu items: **All Programs → SecurOS → SecurOS** (see figure 28).



Figure 28. Start menu (All programs)

Additional Information

The system also can be launched 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 29).

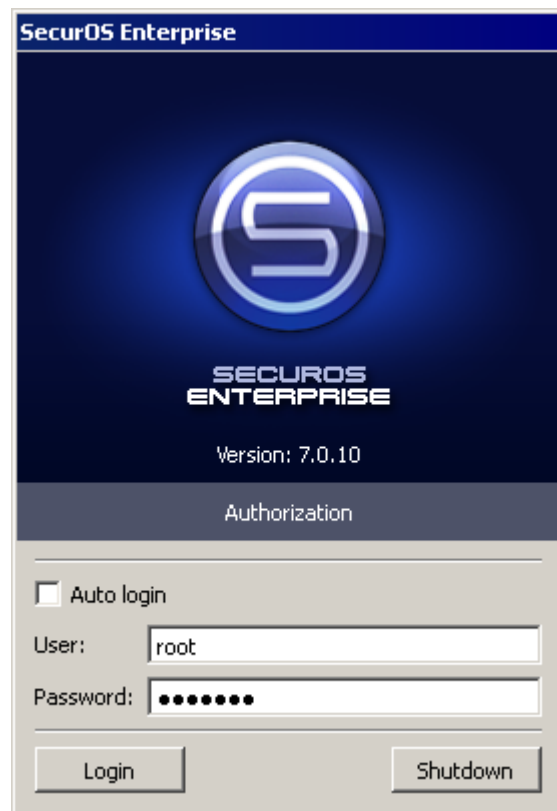


Figure 29. Authorization window

For logging in use the data of the superuser account:

- **User** – root;
- **Password** – securus.

Notes:

1. If superuser password was changed during system configuration (see 4 in [Using The System Configuration Wizard](#) section) use modified value.
 2. If the wrong login credentials are entered the **Authorization Error** window will be displayed. If the incorrect credentials are entered 3 times in a row, the system will enter a 30-second waiting mode after which the next attempt to login will be given.
-

3.2 Installing, Launching and Configuring Peripheral Servers and Operator Workstations

To add other *Video Servers*, *Administrator Workstations* or *Operator Workstations* to the network it is necessary to do the following:

1. Add computers to the a network for that create and set 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 computer purpose in the network (see [Types Of Servers And Workstations](#) section).
3. Launch SecurOS and configure the system with the Wizard.

Note. The very operation can be executed only for *Video Servers* and *Administrator Workstations*.

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 And Operator Workstations

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

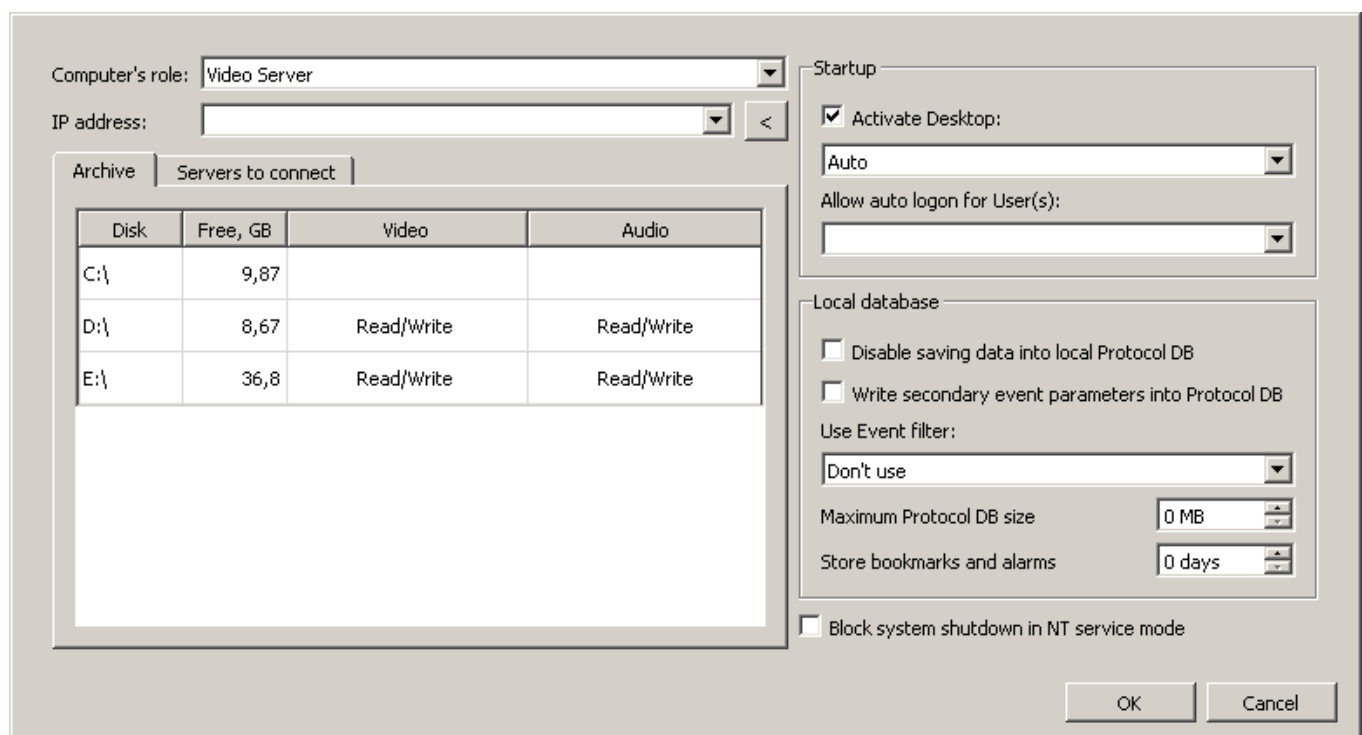
1. Enter the Administration Mode on the *Configuration Server*.
2. In the *Object Tree* select the *Hardware* group, create a *Computer* child object.
3. In the **Parameters of created object** window (see figure 30) set the required values:



The dialog box titled "Parameters of created object" contains three input fields: "ID" with the value "COMPUTER", "Title" with the value "Computer", and "Security Zone" with a dropdown menu showing "SecurOS". At the bottom right are "OK" and "Cancel" buttons.

Figure 30. Parameters of created object

- 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 **Title** field define the *Computer* object name as it will be displayed in the SecurOS *Object Tree*.
4. In the computer properties window (see figure 31) in the **Computer's role** field select the computer role in the network that should correspond to the SecurOS software installation type on the computer (see [Types of Server and Workstations](#) section).



The "Computer object settings window" is divided into several sections. At the top, "Computer's role" is set to "Video Server" and "IP address" is empty. Below this is a tabbed interface with "Archive" and "Servers to connect" tabs. The "Servers to connect" tab contains a table with disk information.

Disk	Free, GB	Video	Audio
C:\	9,87		
D:\	8,67	Read/Write	Read/Write
E:\	36,8	Read/Write	Read/Write

On the right side, the "Startup" section has "Activate Desktop" checked and "Auto" selected for the startup type. Below it is a field for "Allow auto logon for User(s)". The "Local database" section has checkboxes for "Disable saving data into local Protocol DB" and "Write secondary event parameters into Protocol DB", both unchecked. It also has a "Use Event filter" dropdown set to "Don't use", and spinners for "Maximum Protocol DB size" (0 MB) and "Store bookmarks and alarms" (0 days). At the bottom right are "OK" and "Cancel" buttons.

Figure 31. Computer object settings window

Set the following necessary parameters:

- **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** – disks to save video and audio records.

Notes:

1. Without the parameter definition the video records saving will be impossible.
 2. The parameter is a mandatory only for the *Video Server*.
-

- **Servers to connect** – the list of computers to which the created *Computer* object can be connected. It is recommended to include all accessible servers of the security network; for that to click the **Add all** button.
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

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

To install SecurOS software on additional servers (on other *Video servers* and *Administrator Workstations*) 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 setting type selection step in the **Install type** window steps of the procedure are similar to software setting on the video server (see **Software Installation** section).
3. In the **Install type** window (see figure 32) select the **Advanced configuration options** type.



Figure 32. Install Type window

4. In the **Setup type** window (see figure 33) select the required installation type.

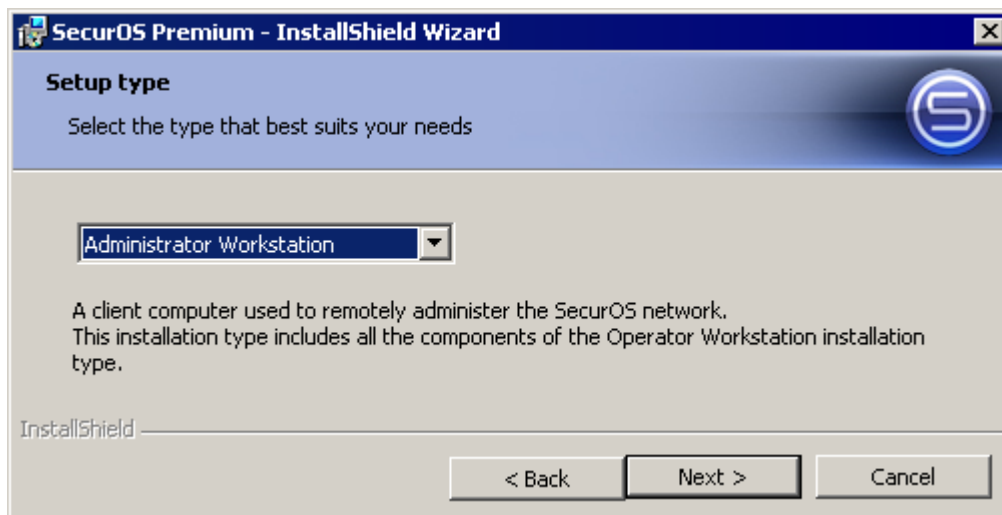


Figure 33. Setup type window Administrator Workstation

5. In the **Server type** window (see figure 34) set *Peripheral Server*.

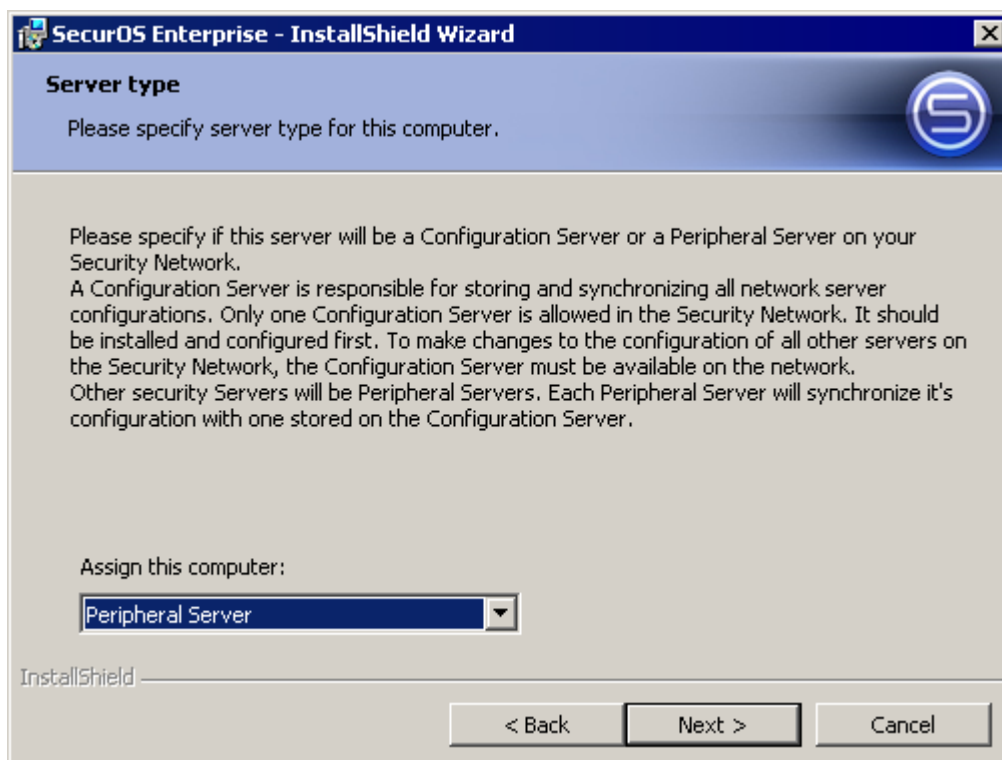


Figure 34. Server Type window

6. In the **Installation of the license key file** window choose appropriate scenario depending on the availability of the license key (for the details see [Software Installation](#) section).
7. In the **Destination Folder** window set the root directory to install SecurOS.
8. In the **Installation database type** window (see figure 35) choose one of the following values:

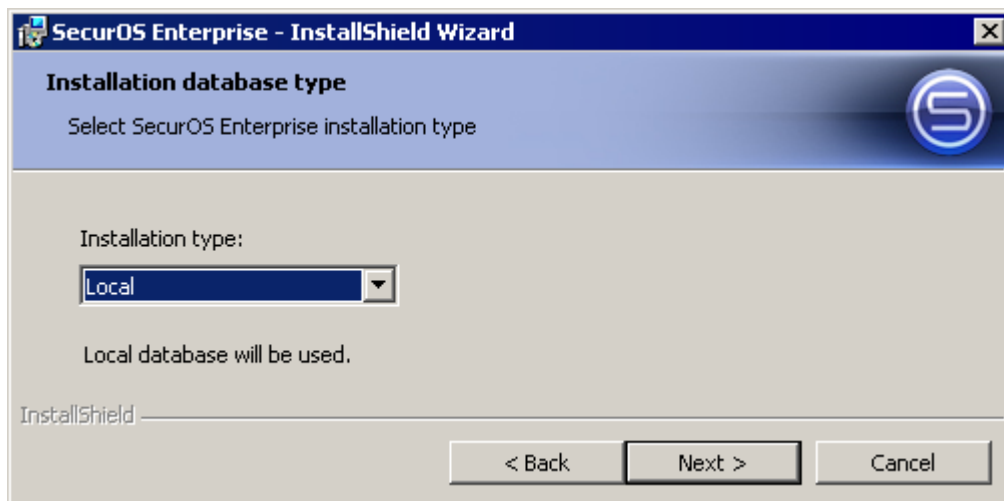


Figure 35. Installation database type window

- **Local**— the local SecurOS database will be created and used.
- **Remote**— the database from the remote server will be used.

9. If the **Local** value is set then the **PostgreSQL installation parameters** window will appear (see figure 36).

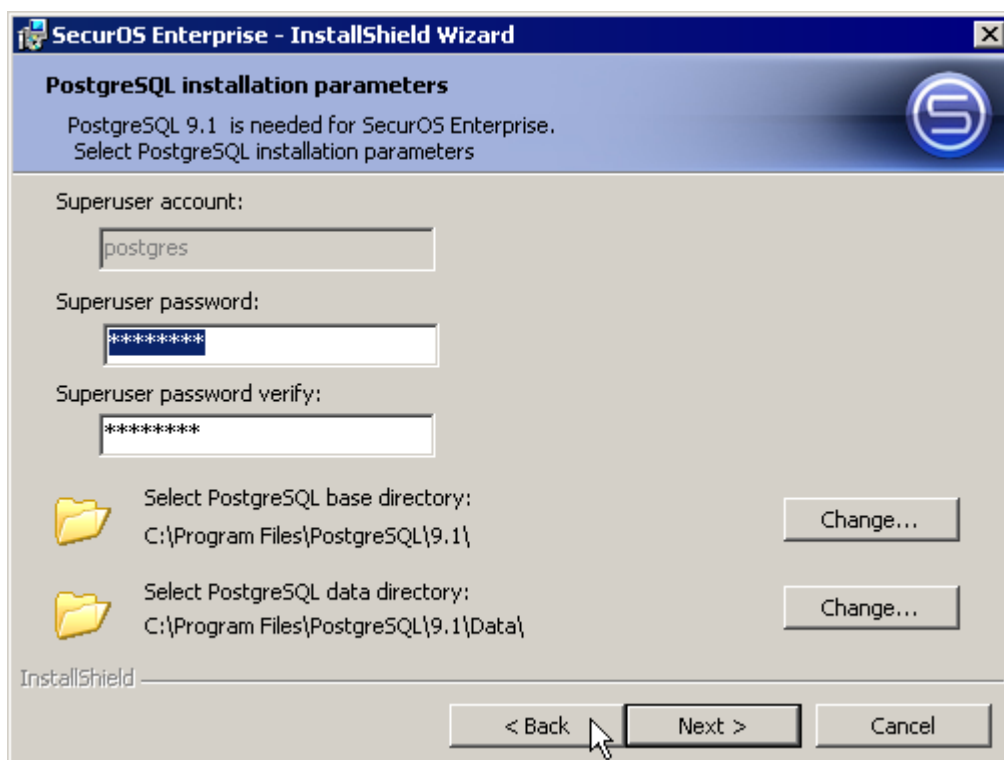


Figure 36. PostgreSQL installation parameters window

It is recommended to use default values in the **PostgreSQL installation parameters** window.

10. In the **Database** window (see figure 37) set a local database name. It is recommended to use default value.

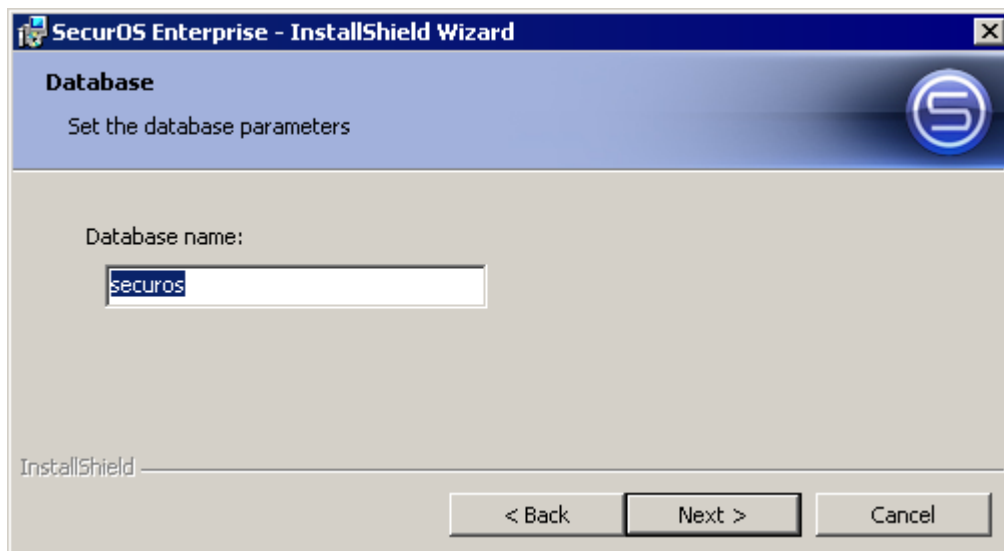


Figure 37. Database window

11. The further steps are similar to the software installation on the *Video server* (see [Installing And Configuring The SecurOS On Video Server](#) section). When setting parameters It is recommended to use default values.

Warning! The software language must be the one for all network computers.

3.2.3 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 38) select the **Operator Workstation** installation type.

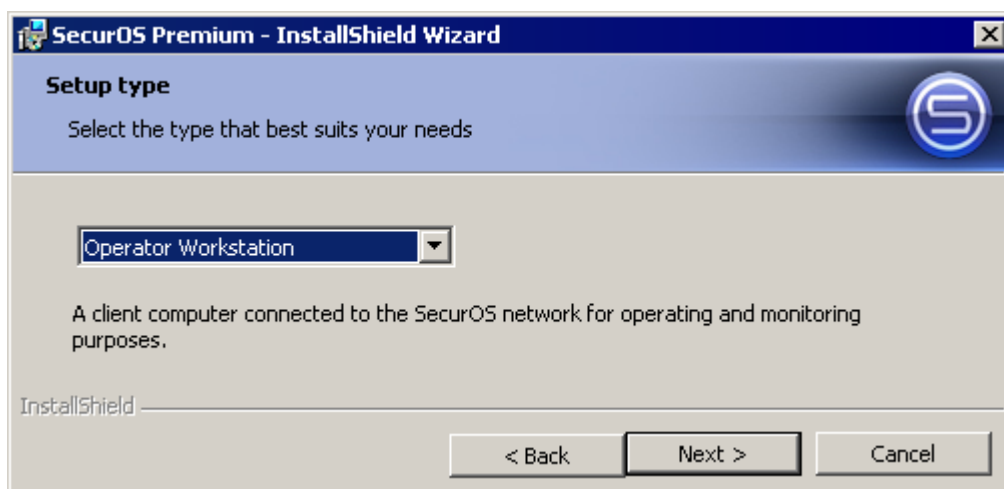


Figure 38. Setup type window

5. Follow the further InstallShield Wizard instructions.

Warning! The software language must be the one for all network computers.

3.2.4 Installing Additional Multimedia Components

If *Peripheral Server* and *Operator Workstation* 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).

3.2.5 Launching And Configuring SecurOS On Peripheral Servers

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

The SecurOS initial configuration on *Video Server* or *Administrator Workstation* is performed by the initial configuration Wizard that is run on system launching.

To launch and configure SecurOS do the following:

1. In the **Start** Windows menu consistently choose the following menu options: **All programs → SecurOS → SecurOS**.
2. In the **Join existing security network** window (see figure 39) do one of the following to choose the *Configuration Server* with the current network configuration:
 - Set *Configuration Server* name (see [Computer Name Restrictions](#)) 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! During the configuration procedure the *Configuration Server* must be active and the SecurOS security system should be launched on it.

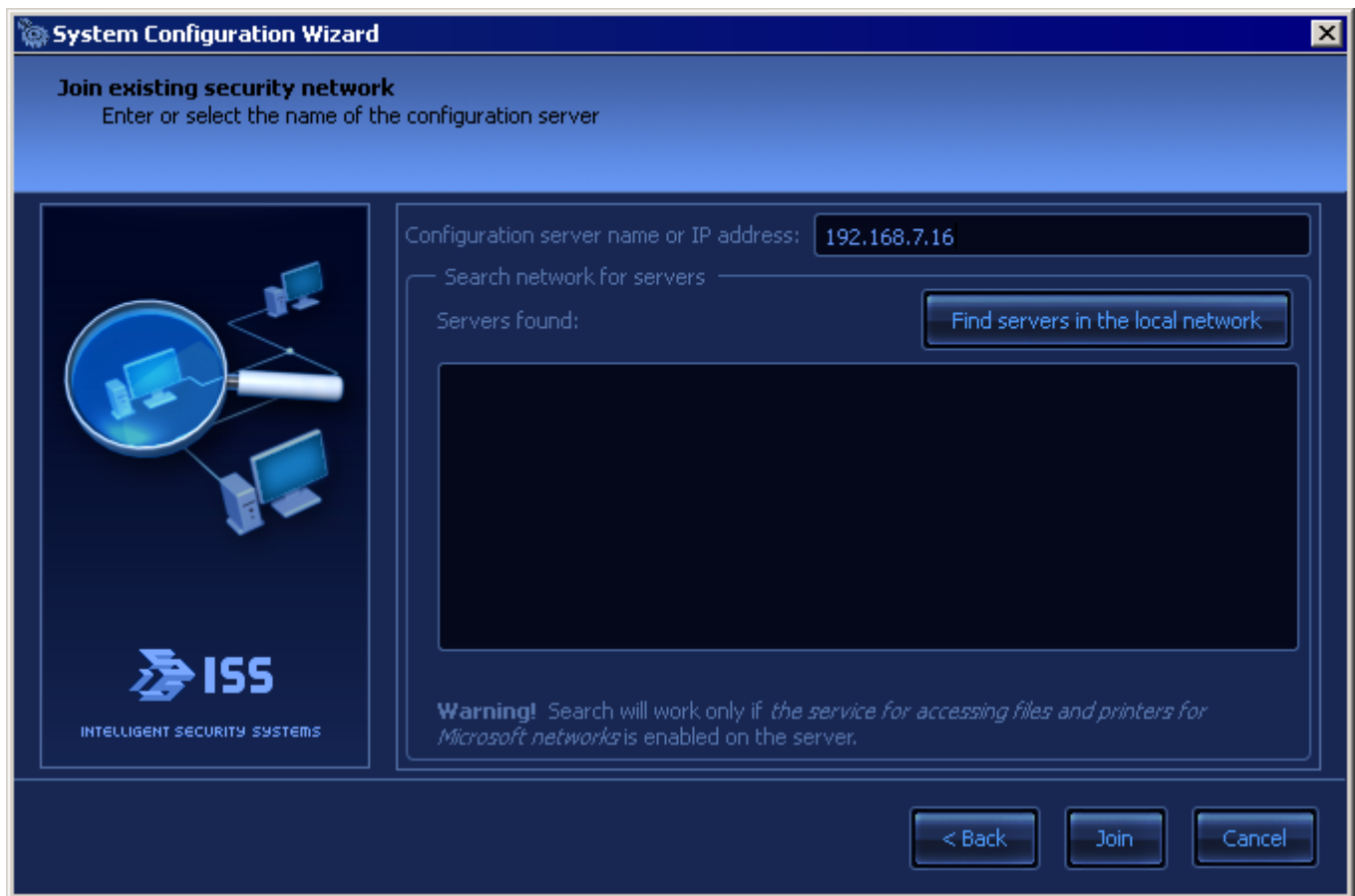


Figure 39. Join existing security network window

Click **Join** button. The **Loading configuration** window will appear that indicates the loading process (see figure 40).

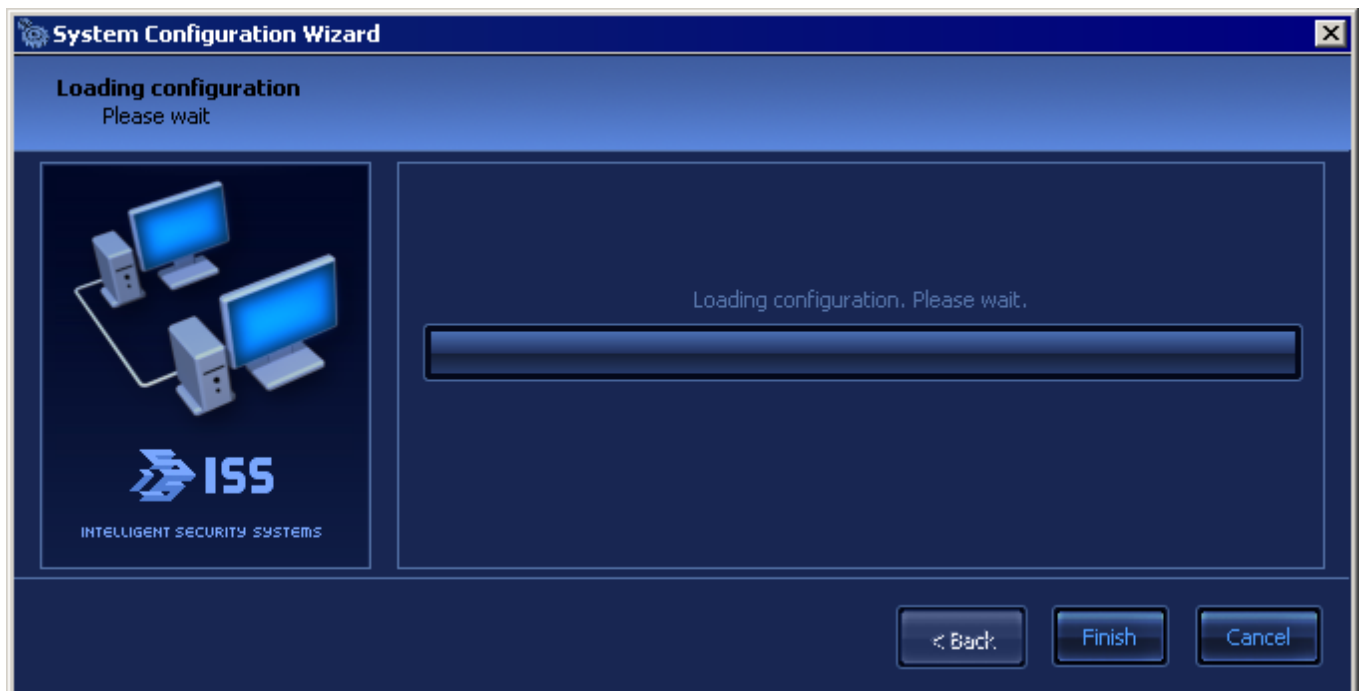


Figure 40. Loading configuration window

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

The further user authorization at start of the installed additional server is done similarly to the procedure described in [Launching SecurOS On The Configuration Server](#) section.

3.2.6 Launching SecurOS On Operator Workstation

To launch SecurOS system on *Operator Workstation* do the following:

1. In the Windows **Start** menu consistently choose the following menu options: **All programs** → **SecurOS** → **SecurOS**.
2. In the **Authorization** window (see figure 41) set the server to connect to IP address in the **Connect to** field, **User** and **Password** that corresponds to personal accounts.

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

Note. Connection is possible only to those servers which are set in the *Server to connect* list of the *Computer* object associated with the given *Operator Workstation*.

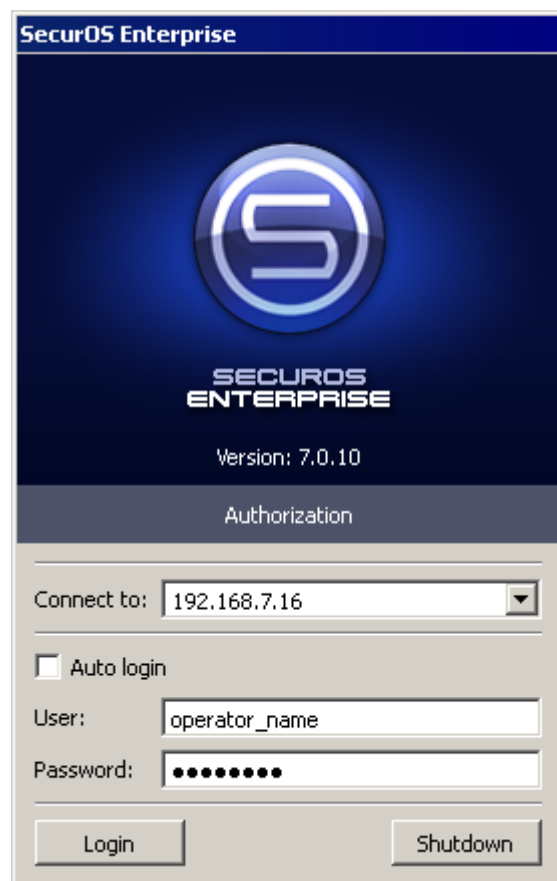


Figure 41. Authorization window

Note. Automatic authorization is possible for the user for which such possibility is specified by the administrator. To apply automatic authorization choose the **Auto login** check-box. For more information about the automatic authorization procedure see below.

4 SecurOS Administration Overview

Administration mode is used to configure security network and its components. It is accessible from any *Video Server* and *Administrator Workstation*. 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 selecting/switching Desktops, entering the administrative mode, and user session management. Control panel is represented on figure 42.



Figure 42. SecurOS Control Panel

Additional Information

The control panel also can be used to launch special system control commands (see [Macros](#) section).

Only active *Desktops* and *Macros* are displayed on the control panel (see [Disabling Objects](#)). Number of the displayed object of each type is defined by system settings and changes dynamically. If max value is exceeded all additional objects are hidden and can be activated from the appropriate menu:

-  – for the *Desktops*;
-  – for the *Macros*.

4.1.1 Control Panel Activation

By default after logging in the control panel is hidden. To display the control panel after logging in, hold the **Ctrl** key on the keyboard and move the mouse pointer so it touches the top of the screen.

Additional Information

The control panel also can be activated by double clicking on the application icon in the Windows taskbar (system tray), or by means of the application icon context menu.

4.1.2 Administration Mode

To enter the administration mode click the  button (**Configure the system**, see 42).

To leave the administration mode click the  button iteratively.

After entering the administration mode the system will display the *Object Tree* and *Administrator toolbar*. The *Administrator toolbar* is intended to perform typical operations with the security system elements which structure is present in the *Object Tree*. The appearance of the *Object Tree* and *Administration toolbar* is shown on the figure 43.

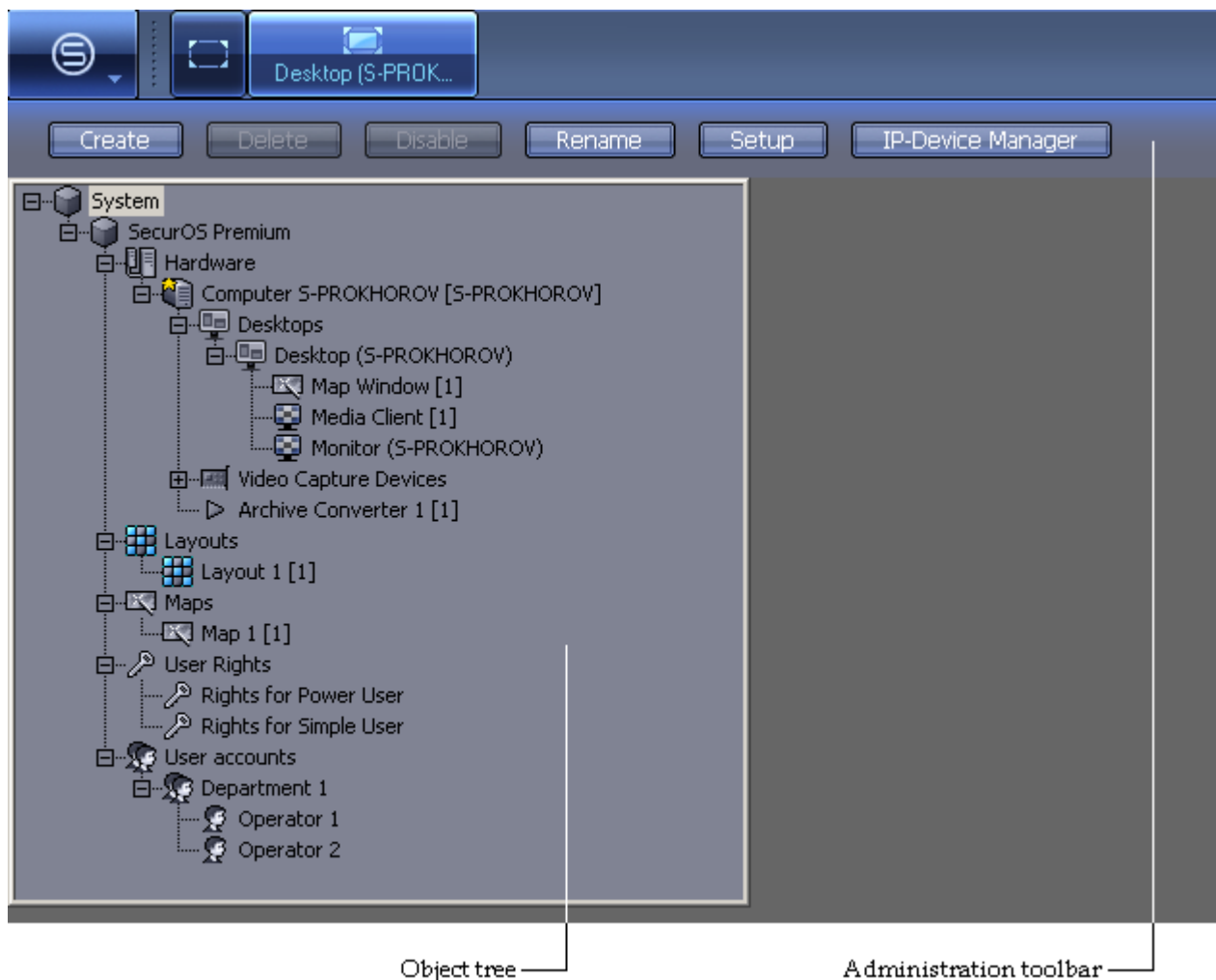


Figure 43. Object Tree and Administrator Toolbar

Additional information

On first entering the administrator mode after the system start the SecurOS *Object Tree* is hidden.

4.1.2.1 Object Tree

All security system elements are displayed in the form of a object tree – a hierarchical structure reflecting correlations between them. Similarly to the file system tree structure, the object tree has a root element (default name: *System*). Tree elements, that are children of the root, contain all the network objects grouped by their functional types. To display and control grouped tree elements the standard means are used (similar to OS file manager controls).

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 their functional types. The *Group* is predefined within system and is created automatically when creating its first element, but can be deleted by administrator including all children elements.
2. *Object* – the functional element of the security network. An object will be included in a *Group* only if it is of the same object type as the other objects in the Group. 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.

4.1.2.2 Administrator Toolbar

The Administrator Toolbar contains the controls (buttons) allowing one to make typical operations of the system administrator: create/delete/rename object, set object parameters, or temporarily disable an object from the security network.

To create and add a new object click the **Create** button.

Accessing an object's parameters and applying new settings is done with the help of the **Setup** button.

Note. A new settings also can be applied by clicking the **OK** button in the object settings window. Discarding changes is performed by clicking the **Cancel** button.

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.

4.1.3 User Session Administration

The control panel allows to switch users and shutdown the system. Click **Change user/Shutdown**

system button () and from the drop-down list select a necessary command (see figure 44).

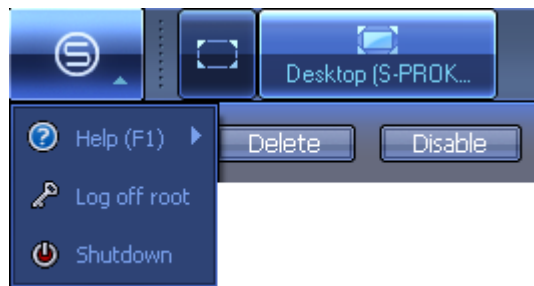


Figure 44. Change user/Shutdown system menu options

4.1.4 Getting Help

To get help for SecurOS, use one of the following methods:

1. From the SecurOS Control Panel (see figure 45):



Figure 45. Getting help from the Control Panel

2. From the Windows task bar (system tray), by right clicking on the SecurOS icon (see figure 46):

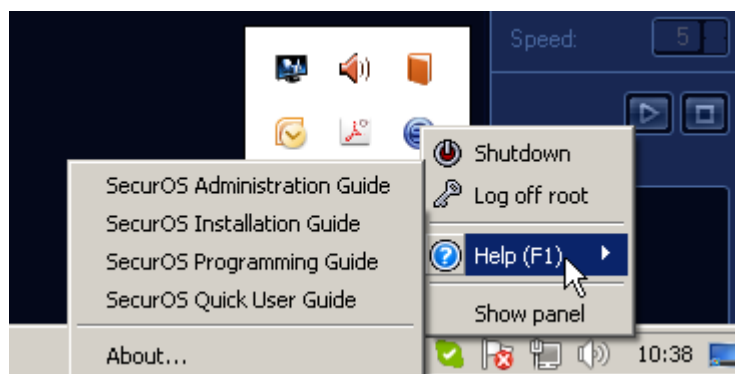


Figure 46. Getting help from the Windows system tray

3. By pressing the **F1** key when in administrative mode. You can get context help for a given object by pressing the **F1** key when its settings window is open;
4. From the Windows taskbar (**Start** → **All Programs** → **SecurOS** → **Documentation**).

4.1.5 Hide Control Panel

After control panel is activated it permanently displayed on the desktop over all other windows. To hide it manually click **Hide Control Panel** button ().

4.2 Working with Objects

To perform actions on objects, the Administration Toolbar provides a set of buttons (see figure 47):

- **Create** — create new child object under currently selected parent object;
- **Delete** — delete object;
- **Disable** — disable object;
- **Rename** — rename object;
- **Setup** — open/close object's settings window;
- **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.



Figure 47. Administration Toolbar buttons

To perform an action directly from the Object Tree (without using the Administration Toolbar), right click the object icon in the Object tree. The system will display an action context menu.

4.2.1 Creating Objects

To create a new object:

1. Select a parent object in object tree.
2. On the Administration toolbar click **Create** button and choose necessary object type from a drop-down list box.
3. A dialog window will appear containing base object settings (**ID** and **Name**). Enter these parameters and click **OK** button to confirm object creation or **Cancel** button to return without creating an object.

If current object cannot have child objects, in drop-down list box you will see object types for its parent. In this case newly created object will appear as a sibling node, as if you have selected the parent node prior to creating new object.

Once an object is created, its settings window will appear automatically.

4.2.1.1 Creating Objects Limits

The system configuration limits (amount of objects of each type within the security network) is specified in the license key file (`key.iss`). If you have created the maximum number of objects of a particular type, the ability to create additional objects of this type is blocked. 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.

4.2.2 Editing Object Settings

To edit or view an object's settings:

1. Select the object in the Object Tree and click the **Setup** button in the Administration Toolbar. A window with the object's settings will open on the right side of the screen.

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. Several object types do not have editable settings, so the **Setup** button will become disabled once an object of this type is selected.
-

2. Click the **Setup** button (or **OK** button in the object settings window) again to apply changes and close the object settings window.

4.2.3 Deleting Objects

To delete object:

1. Select it in the objects tree and click **Delete** button on the Administration toolbar or select **Delete** command in the context menu.
2. In the displayed window click **OK** button to delete object or **Cancel** button to return without deleting.

Warning! This operation cannot be undone, so use it carefully. If you delete object, its child objects will be deleted as well.

4.2.4 Disabling Objects

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

To disable object, select it in objects tree and click **Disable** button or choose **Disable** command in the context menu. Disabled objects are marked with "cyan cross" icon.

To enable object, click **Enable** button or choose **Enable** command in the context menu.

4.2.5 Renaming Objects

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

To rename object:

1. Select object in object tree and click **Rename** button or select **Rename** item from the context menu.
2. In a dialog window specify there a new object name.
3. Click **OK** button to apply changes or **Cancel** button to escape from this dialog without changing anything.

4.2.6 Searching Objects

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

1. Select any object in tree and right-click it.
2. Choose **Find by name** context menu item. System will display the search dialog window (see Figure 48).



Object type:
Camera

Text to find:
Entry

< Prev Search Next >

Figure 48. Searching by Name Window

3. Select object type and type in the name (or part of the name) of the required object and press the **Enter** key or click the **Search** button. The focus will switch to the first child object that matches the search string and the search window will close (if **Enter** key is pressed) or the **Prev** and **Next** buttons will become activated. The search window won't be closed if an object is not found.
4. Press **Enter** key (or **Prev** and **Next** buttons) to resume searching or **Esc** key to stop searching and close the window.

To find objects by their IDs, do the following:

1. Select any object in tree and right-click it.
2. Choose **Find by ID** context menu item. System will display the search dialog window (see Figure 49).



Object type:
Camera

ID to find:
14

Search

Figure 49. Searching by ID Window

3. Select object type and type in the ID of the required object and press the **Enter** key or click the **Search** button. The focus will switch to the object that matches search ID and the search window will close. Window won't be closed even an object is not found.

Note. Searching is performed until complete ID matching is reached.

4. To finish searching and close the window press the **Esc** key.

4.3 Working with Object Table Parameters

Object setting window can include both single parameter text boxes and tables. Example of the table parameter (**Disk** on the **Archive** tab) is shown on figure 50.

Disk	Free, GB	Video	Audio
C:\	9,87		
D:\	8,67	Read/Write	Read/Write
E:\	36,8	Read/Write	Read/Write

Figure 50. 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.
- To delete an entry from the table, select the required row and press the **Ctrl + Delete** keyboard shortcut.

4.4 Managing User Rights Within Security Network

Once deploying security network, you can manage its internal security scheme and restrict access to its administration interface, give some administrators the ability to administer only a part of SecurOS security network, or explicitly define, what UI objects each operator can see, what cameras she/he can control and what she/he cannot, etc.

When no individual user rights are set any user is granted with full (superuser) rights. Once you add at least one person and define its rights within the system, SecurOS will require user name and password when you launch server/workstation software next time. To get full access to all system components and load the whole system database, use password and name of system superuser.

To implement access control within SecurOS network:

1. Change the default SecurOS superuser password and keep it safe (see [Changing Superuser Password](#)).
2. Manage user rights for individual administrators/operators on per object basis (see [Defining Access Levels to Individual Objects](#)).
3. For these settings to take effect, force all administrator and operator workstations to reconnect to SecurOS network.

4.4.1 User Registration. Setting up User Rights

Users access to operation with the SecurOS security system is carried out on the basis of the login accounts defining the user rights in the system. At system installation the one user account having unlimited rights is created by default. New user accounts and their rights are set by the system administrator with the help of **System Configuration Wizard** or at the further configuration.

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

- *Department* object (**Security Zone** → **Users group** → **Department**) – contains a list of the *User* object. The name of each *User* object is used at authorization as the **User** parameter. New users can be registered both in the given *Department* object, and in any other *Department* object created by the system administrator which will be included in *Users* group automatically.

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

- *User Rights* group (**Security Zone** → **User Rightsgroup**) – contains the *User Rights* objects. Each of the existing *User Rights* objects can be used repeatedly (i. e. can be assigned to any new user).

Except a set of the user rights the password of the corresponding user account is defined and stored in the *User Rights* object settings.

4.4.1.1 Default User Accounts

System Configuration Wizard creates the only one superuser account with the following values: `root` (user name) and `securos` (password). The set of the rights of such account gives to the 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 a name and a set of the superuser rights is impossible.

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

4.4.2 Changing Superuser Password

A person that has full access to all SecurOS objects is called *superuser*. If no user rights are defined, SecurOS will not request password when starting system software of the server or workstation and allows operate as superuser.

Warning! Superuser login name is `root`. Default superuser password is `securos`. Change default superuser password to the new value (the minimal length is 7 symbols) and keep it safe before giving access to your security network for other personnel!

To change superuser password:

1. Log in as superuser.
2. Open settings window for the root *System* object (see Figure 51).

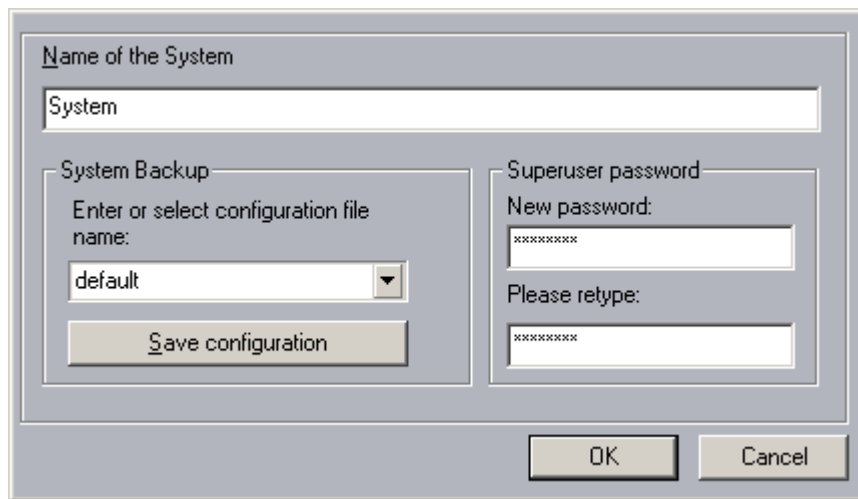


Figure 51. System object settings window

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

Note. After that, users other than superuser cannot see *System* object at all.

4.5 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* or *Administrator Workstation* this is it's own, local protocol database of the corresponding computer, and for the *Operator Workstation* — database of that *Video Server* or *Administrator Workstation*, 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.

4.6 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. Run SecurOS program on the *Configuration Server*.
3. 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.

4.6.1 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 52). 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).

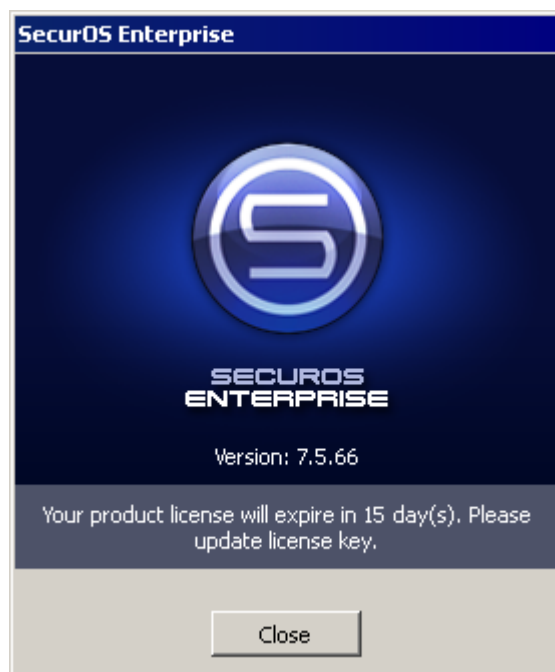


Figure 52. License expiration information window

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>
```

4.7 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 Parameters and Setting up IP Device Usage;**

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 Parameters and Setting up IP Device Usage;**
- **Deleting IP Device.**

4.7.1 Specification

The main application window is shown in figure 53.

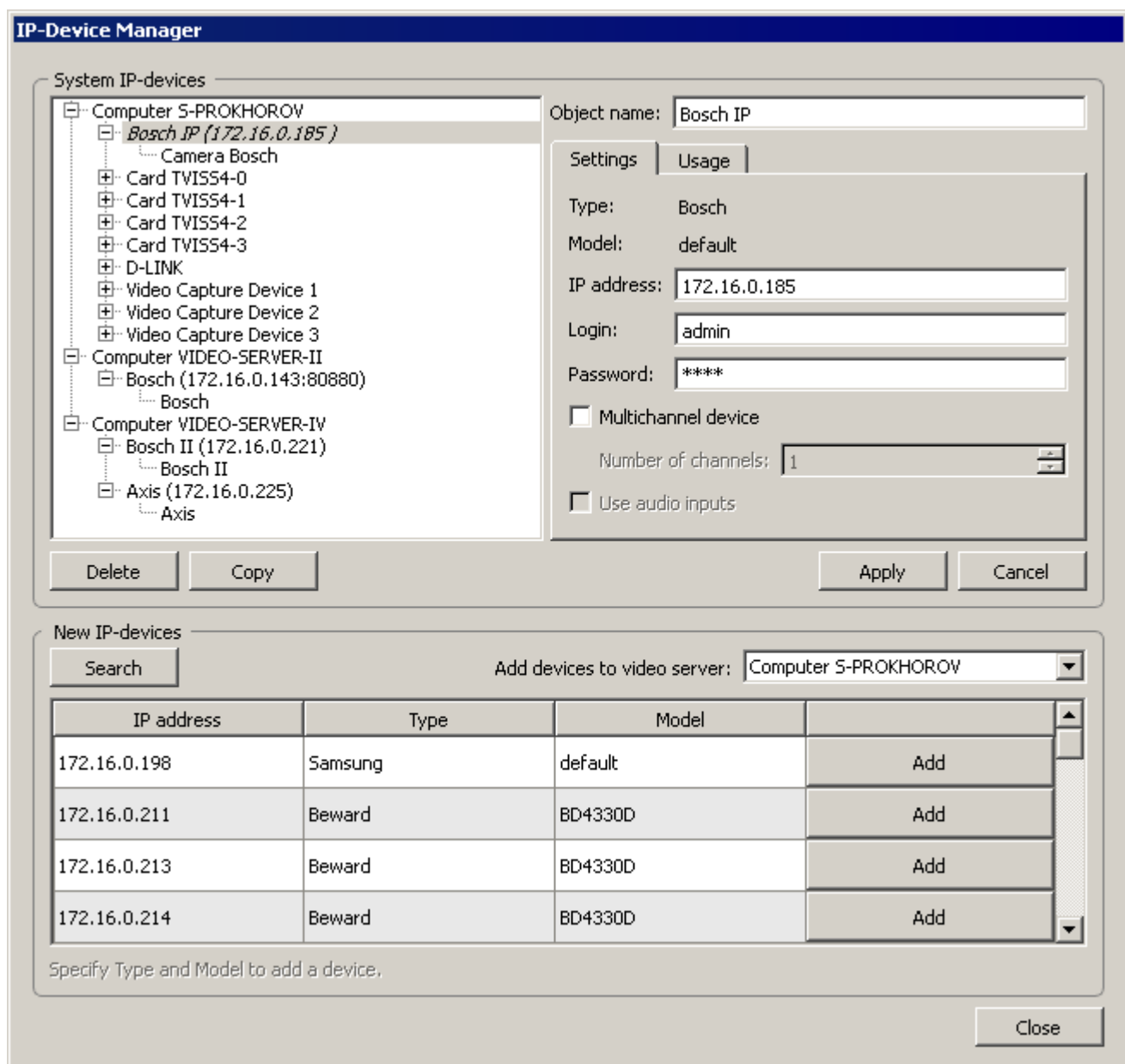


Figure 53. IP-Device Manager

The window consists of the following controls (see table 4):

Table 4. IP-Device Manager controls

Parameter	Description
System IP-devices	
Object Tree	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. Notes: 1. Objects whose 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 name	Name of the object selected in the Object Tree (see above). Note. Object names are restricted with the following: 1. Name cannot be empty. 2. Name should be unique.
Settings tab	
Type, Model	Type and model of the device, selected in the Object Tree . The Information field is not editable by the user.
IP address	IP address of the device.
Login, Password	Login/Password to access the device. By default when a device is added, the values are assigned to admin/admin. 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.
Multichannel device	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. Limitations. To use this functionality the system must meet the following conditions: 1. The device should support several independent video streams. 2. The device integration should support multichannel systems.
Number of channels	Number of used independent video channels of the multichannel device. Note. Max number of video channels depends on the device Type and Model.

Parameter	Description
Use audio inputs	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. Limitations. To use this functionality the system must meet the following conditions: 1. Device must be equipped with audio inputs. 2. Device integration in SecurOS should support audio.
Usage tab (see Figure 54)	
IP device Usage Tree	The tree consists of all the SecurOS objects, which can use the currently selected IP device. Root elements of the tree are the <i>Computers</i>, for which at least one of the following objects is configured: • <i>Desktop</i>; • <i>Monitor</i>; • <i>Audio Player</i>. While being displayed, the objects are grouped in compliance with their SecurOS hierarchy, i.e. similarly as in the SecurOS <i>Object Tree</i>. Note. If some of the above mentioned objects are disabled in the SecurOS <i>Object Tree</i>, they will not be displayed in the <i>Manager's Usage Tree</i>. Those SecurOS objects, which currently use the selected IP device, are displayed in the Tree with the appropriate mark. The state when not all devices of the object selected in the <i>Manager's Object Tree</i> (including children) are used by the object of the Usage Tree (including children), is called "partial usage". In this state, the field located on the left of such object is marked with the gray background in the Usage Tree (☐), or, in Windows 7, with the  mark. For example, if a <i>Camera</i> with a <i>Microphone</i> is placed on the <i>Monitor</i> of some <i>Desktop</i>, but this <i>Microphone</i> is not used by the <i>Audio Player</i> located on the same <i>Desktop</i> at the same time, this <i>Desktop</i> will be marked in the Usage Tree with the  () mark.
Buttons	
Delete	Delete a <i>Video Capture Device</i> , selected in the <i>Manager's Object Tree</i> .
Copy	Copy a <i>Video Capture Device</i> , selected in the <i>Manager's Object Tree</i> (see Copying IP Device).

Parameter	Description
Apply (Cancel)	Save the newly entered or edited device settings (Discard changes while saving previous settings). Notes: 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 <i>Computer</i> , 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	The table contains found non-configured IP devices. 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). • IP address — IP address of the found device. 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). • 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>.

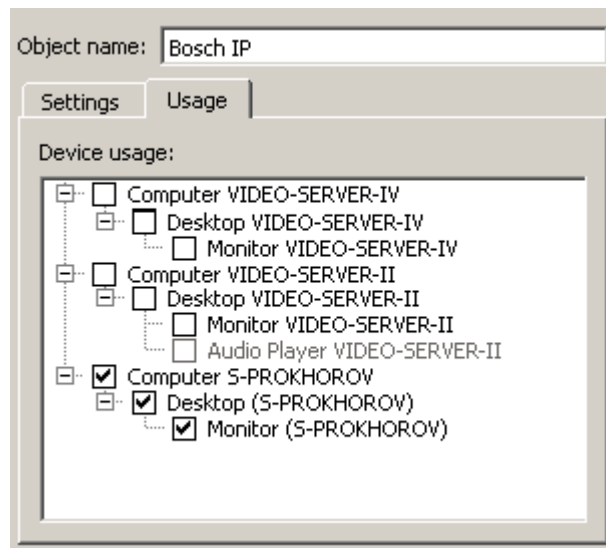


Figure 54. Usage tab

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

4.7.2 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 Parameters and Setting up IP Device Usage;**
- **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.

4.7.2.1 Launching IP-Device Manager

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

1. Enter the Administration Mode.
2. On the *Administrator Toolbar* (see Figure 55) click the **IP-Device Manager** button.

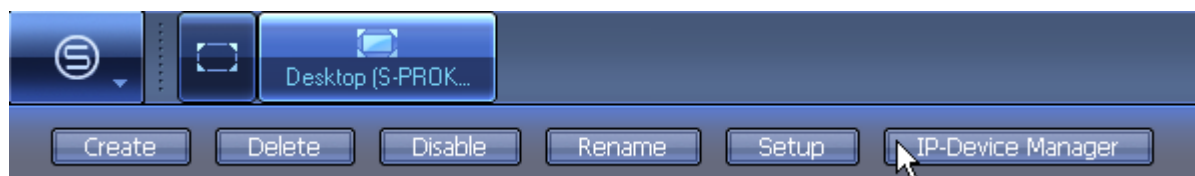


Figure 55. Launching IP-Device Manager

Note. When some SecurOS object settings window is open or connection with the *Configuration Server* is lost, the **IP-Device Manager** button is disabled.

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

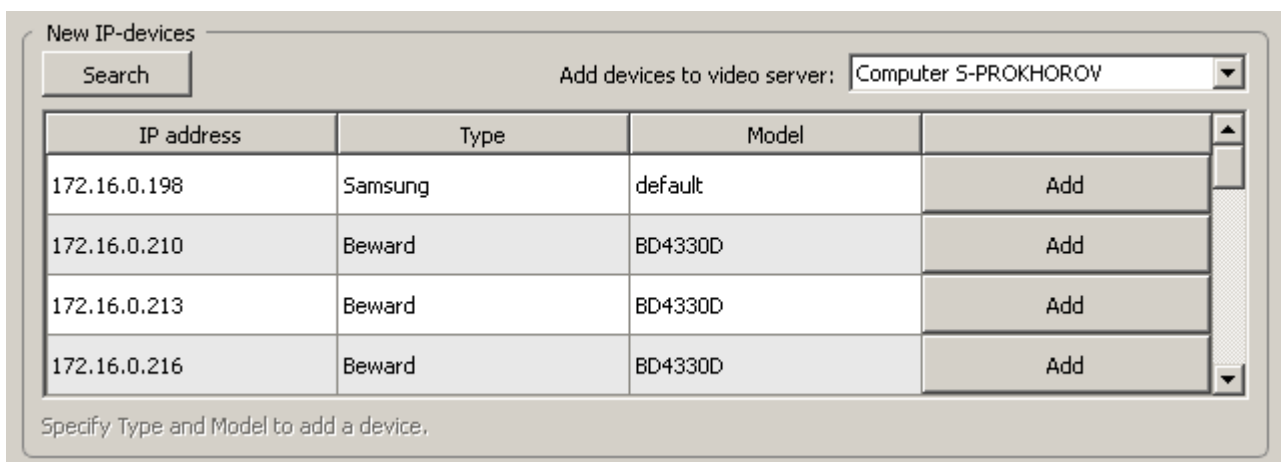
Warning! When the **IP-Device Manager** window is active, the SecurOS object settings mode is blocked (i.e. it is impossible to open a object settings window from the SecurOS *Object Tree*).

4.7.2.2 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 56).



The screenshot shows a window titled "New IP-devices". At the top left is a "Search" button. To the right is a label "Add devices to video server:" followed by a dropdown menu showing "Computer S-PROKHOROV". Below this is a table with four columns: "IP address", "Type", "Model", and an empty column with an "Add" button. The table contains four rows of data. Below the table is a text label: "Specify Type and Model to add a device."

IP address	Type	Model	
172.16.0.198	Samsung	default	Add
172.16.0.210	Beward	BD4330D	Add
172.16.0.213	Beward	BD4330D	Add
172.16.0.216	Beward	BD4330D	Add

Figure 56. 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.

4.7.2.3 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 57).

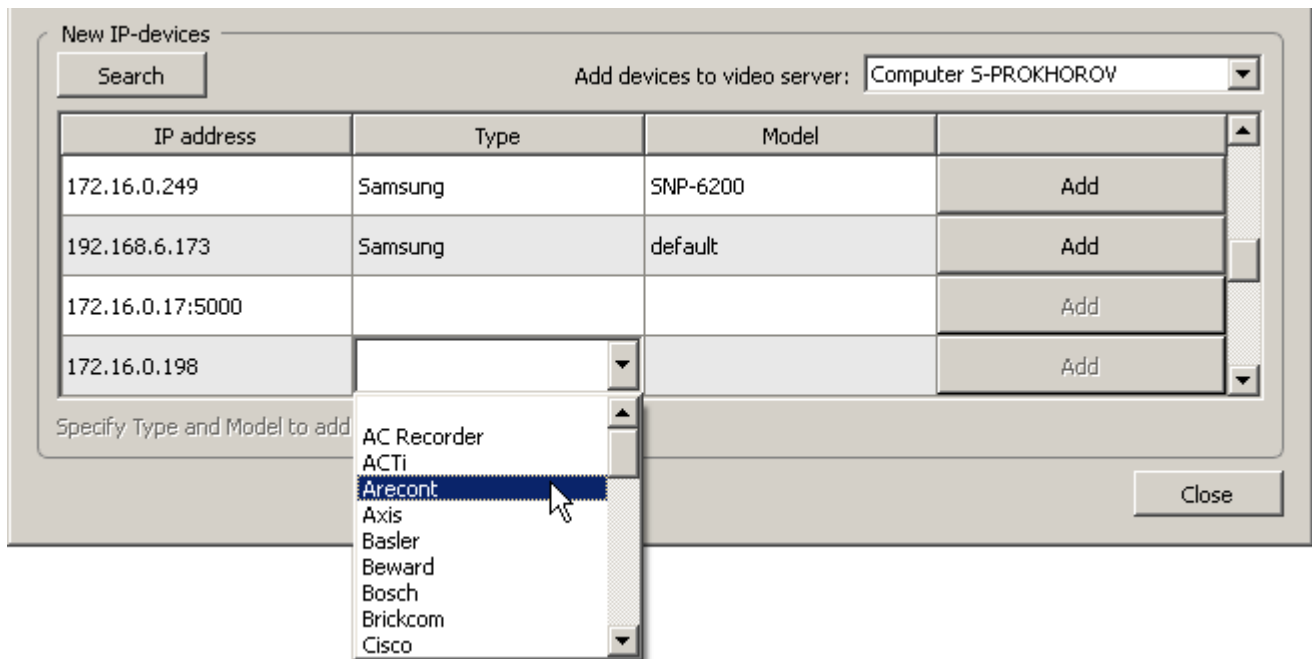


Figure 57. Select the Type of device

- Click the **Model** cell, and in the drop-down list select the model of the device. Select default if there is no required device 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. Perform the **Editing Parameters and Setting up IP Device Usage** operation.

4.7.2.4 Editing Parameters and Setting up IP Device Usage

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 **System IP-devices** block (see Figure 58).

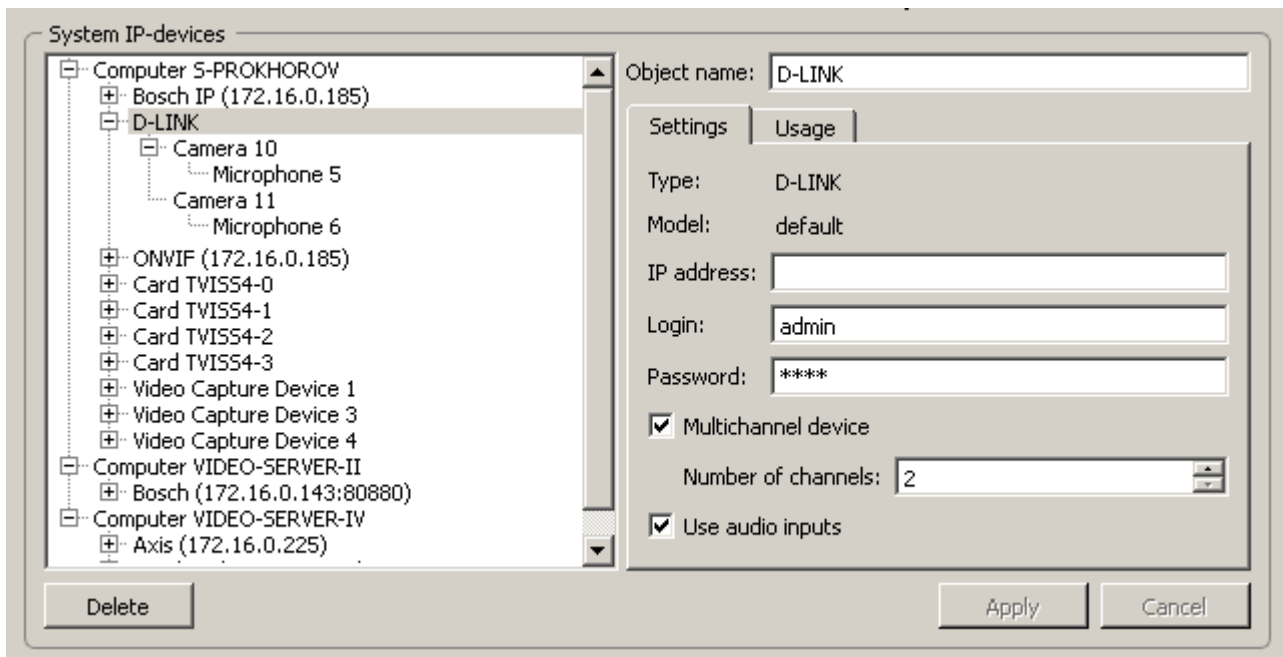


Figure 58. Setting up audio inputs

- If necessary, change device name in the **Object name** field.
- In the **Settings** tab:
 - 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 58), and in the SecurOS *Object Tree* will be specified in the settings of the appropriate *Cameras*.
- In the **Usage** tab:
 - Activate checkboxes for those SecurOS objects, which will use the currently selected IP device, or deactivate the checkboxes for those objects which should not use the device (see Figure 59).

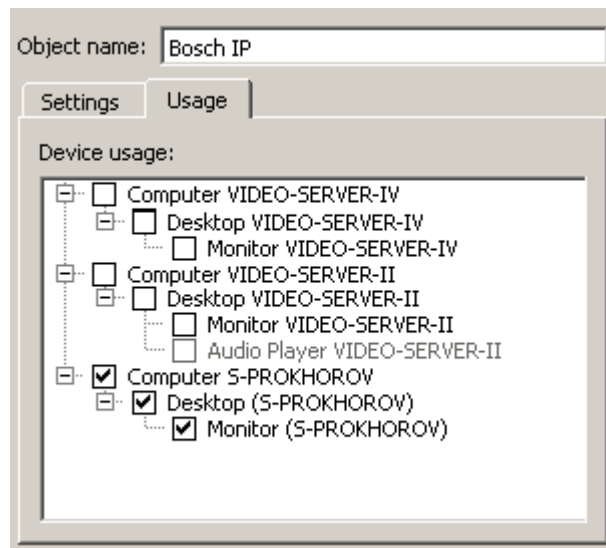


Figure 59. Usage tab

Notes:

1. Device usage can be specified even if the device is disabled in SecurOS.
2. Device usage may be specified for an individual device and a device group. To specify usage for all devices, added to the arbitrary *Video Server*, select it in the *Manager's Object Tree* then, in the **Usage Tree**, specify objects which should use these devices. After applying the settings, the selected object will use all devices of the specified computer.

3. Click **Apply** button.

4.7.2.5 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 *Video Capture Device*:
 - **Usage**.
4. The following parameters of the *Camera*:
 - **Microphone**;
 - **Pan/Tilt/Zoom** (if it is external);
 - **Presets**;

- **Tours;**
- **Wiper;**
- **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 Figures 60 and 61).

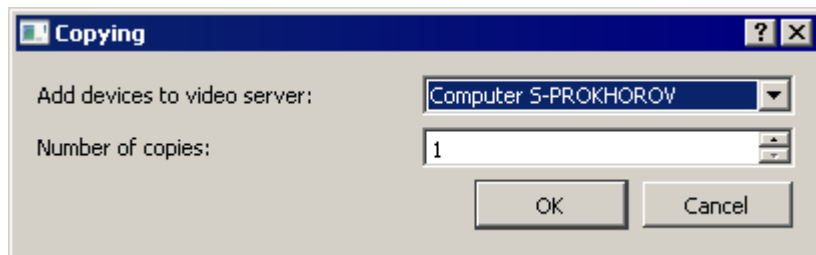


Figure 60. Copying window for the TVISS boards

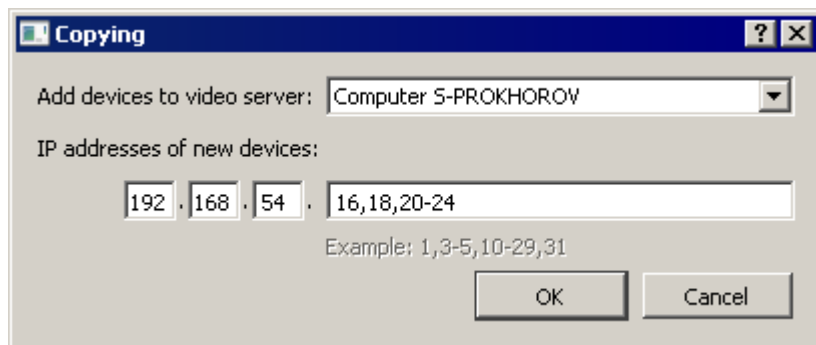


Figure 61. Copying window for the IP Cameras

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**, **Usage** tabs. Click the **Apply** button.

4.7.2.6 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.

4.8 Health Monitor self-diagnostic Module

The *Health Monitor* self-diagnostic Module is designed for system monitoring to identify critical issues, which can cause system failure and result in partial or full loss of video data. Upon detection of such problems, the module informs the administrator in real-time and generates a detailed description of each problem.

A standard Windows Notification generated in the system tray (see Figure 62) is used to notify about the problem. A detailed problem description can be displayed in a separate window (see Figure 64).



Figure 62. Problem Notification

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

To configure and launch the *Health Monitor* do the following:

1. Enter the Administration Mode.
2. In the SecurOS Object Tree select the *Computer* object, and create a *Health Monitor* child object.
3. In the **Parameters of created object** window specify the object Title.
4. Apply new settings.

Notes:

1. The new object is launched automatically after applying the settings.
 2. If the object exists in the system, it launches automatically when you start the SecurOS session.
-

By default the **Health Monitor** window (GUI) is hidden after the application is started. To display the window, right-click the SecurOS icon in the system tray, then select **Health Monitor** in the context menu (see Figure 63).

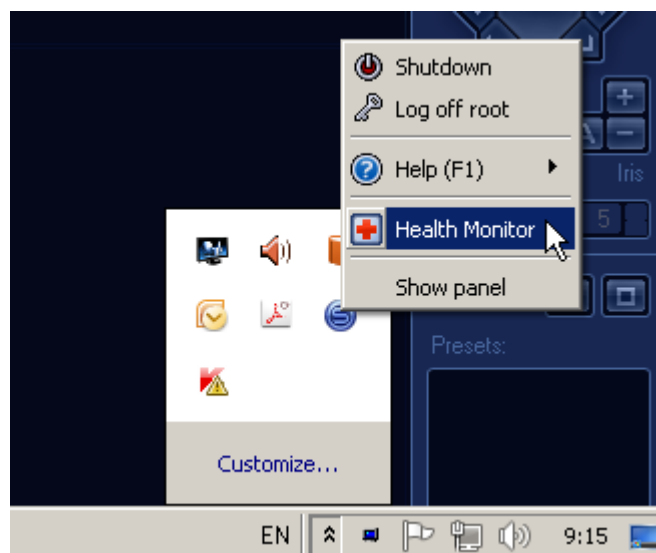


Figure 63. Open Health Monitor Window

The **Health Monitor** window will immediately be displayed (see Figure 64).



Figure 64. Health Monitor Window

SecurOS objects with current problems are represented as a tree and grouped in five main nodes, representing the type of the object: *Video servers*, *Concentrators*, *Cameras*, *Microphones* and *Sensors*. 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.

Main states describing critical failures are represented in the Table 5.

Table 5. States of the SecurOS problem objects

Object type	State	Description
Video server	disconnected	Connection with the server is lost. Warning! This message is also displayed if an invalid or incorrect IP address is specified in the IP address parameter in the <i>Video Server</i> settings.
	archive write error	Insufficient space on the hard drive to record archive

Object type	State	Description
	audio archive write error	It is impossible to save audio for the one of the following reasons: • Insufficient space on the hard drive to record audio archive; • Insufficient disk write speed; • hardware or driver error.
	insufficient speed write	Insufficient disk write speed: total speed (bitrate) of the recorded streams exceeds max allowed by physical disk write speed
	license expires in 24 hours	SecurOS license expires in 24 hours
	there are unanalyzed dump files	One or several of the following folders – <SecurOS_installation_folder>, <SecurOS_installation_folder> \Integrations or <SecurOS_installation_folder> \Modules (include subfolders) contain dump files. Warning! To help troubleshoot a problem it is recommended to send dump files to the Intelligent Security Systems Technical Support Team, then delete the dump files from the appropriate folders.
	disk is unavailable	It is impossible to save to one of the drives specified in the Archive tab of the <i>Computer</i> object settings for the one of the following reasons: • disk disconnected; • hardware or driver error. This message is also displayed if no disk to work with audio is specified in the Archive tab of the <i>Computer</i> object settings
	database query loss - insufficient database speed	An error occurs when trying to write data into the database
	critical CPU load	CPU load (one of the cores) exceeds 90%
Concentrator	disconnected	ISS Video Concentrator cannot receive a video stream from a remote system

Object type	State	Description
Camera	stream N is disconnected	Stream N is not being received from the camera
	camera is detached	Connection with the camera is lost
	archive integrity error	Cannot find/read archive file Note. Message is generated only when exporting video archive with the help of <i>Archiver</i> or <i>Archive Converter</i> .
	When using Edge Storage	
	Edge Storage not accessible	Failed to connect to the camera. Note. This message is generated for all connection errors, except errors caused by lack of connection with the camera. For example, when authorization failed.
	Edge: no information about archive	Response to a camera archive query does not contain any data or data structure does not meet the manufacturer's specifications
	Edge: requested records not found	There are no required records both in the camera archive and video server archive
	Edge: time isn't in sync	Camera's system time is not synchronized with the video server's system time
	Edge: error downloading archive	Error when copying archive from the camera to the video server
	Edge: archive corrupted	Camera's archive contains different records for the same time interval
Microphone	microphone is detached	No signal from microphone
Sensor	sensor is sabotaged	Sabotage

If the problem is not repeated during the specified time period, it is considered corrected. The corresponding entry in the **Health Monitor** window is removed.

4.9 Using Camera's Edge Storage

This functionality is available in the following editions: *SecurOS Enterprise*, *SecurOS Premium*.

Warning! In the current SecurOS version the Edge Storage functionality is available for use with AXIS cameras, supporting the AXIS VAPIX3 API, and Samsung cameras, supporting SUNAPI 2.0 and higher.

The SecurOS video archive can in some cases be used as crucial evidence in court proceedings. One of the significant attributes of the archive is its completeness, i. e. continuous records for the specified period. SecurOS can provide such complete archive only if there is continuous network connection between camera and video server during specified period.

Normally to provide such a connection is not always possible - connection loss can be caused by network failures, hardware problems or software run-time errors, etc. Thus, the occurrence of any of the problems listed above makes SecurOS's continuous archive recording impossible, which is unacceptable when securing critically important sites.

To ensure archive recording in such cases, a Camera's Edge Storage built-in technology is used within SecurOS. A camera's edge storage is a Digital Media, installed on the camera, where a video stream is recorded to. For example, it may be on-board SD-card, built-in digital media, etc.

The camera's edge storage is used as a source of information in the following cases:

- camera is connected to the network continuously, and video stream is recorded both on camera's edge storage and SecurOS's *Video Server*. This mode of connection is typical for fixed cameras;
- continuous network connection between camera and SecurOS's *Video Server* is not provided, camera connects to the network periodically. This mode of connection is typical for mobile cameras.

In the first case, when network failure occurs and connection with the SecurOS server terminates for some time, the video stream will be saved onto the camera's edge storage. When restoring system operability, an archive fragment missed on the server can be simply copied to the SecurOS's *Video Server* from the camera, that guarantees continuous archive in SecurOS.

In the second case, a camera equipped with edge storage is mounted on a vehicle (bus, train, police car, etc.), which carries out regular routes during the day, can be connected to the network only at the end of its route. In this case, while a vehicle is in route, temporary archive is created on the camera's edge storage. Each time when a vehicle arrives to the end of its route and the camera becomes accessible via network, SecurOS copies the recorded video from the camera's edge storage to the SecurOS's operative archive.

When using the camera's edge storage feature, SecurOS works in the following way:

1. The *Camera*, configured within SecurOS, continuously records onto its on-board edge storage. When using a fixed camera, a video stream is simultaneously transmitted to the *Video Server* as a stream for recording.
2. For each *Camera* disconnection, the *Video Server* creates a task, where it specifies the *Camera* disconnection period, i.e. start and end time of the fragment of the operative archive, which could not be saved on the *Video Server* due to the connection loss.
3. The **EdgeStorage Sync** application, running on the *Video Server*, requests the *Video Server* for a list of these tasks with the specified evaluation period.
4. After the *Camera* is reconnected, then *EdgeStorage Sync* starts copying missed fragments from the *Camera*'s local archive to the *Video Server* operative archive, if task list on the *Video Server* is not

empty.

Setting up system objects to use this functionality is described in the [Setting up System to Use Local Data Storage](#) section. *EdgeStorage Sync* object is described in the [Video Subsystem](#) section (see the [EdgeStorage Sync](#) sub-section).

4.9.1 Setting up System to Use Local Data Storage

To prepare the system to apply the Edge Storage feature it is necessary to perform the following operations:

1. [Setting up IP Camera Equipped with Edge Storage](#);
2. [Setting up SecurOS Objects](#);

It is recommended to perform the operations in the exact order above.

Note. Setting up system objects to save operative archive on the *Video Server* is not described in this section (see [Computer](#), [Archive Recording](#) sections).

Warning! After all settings are applied, it is necessary to synchronize the system time on *Video Server* and all local *Cameras*. To synchronize system time use an NTP server.

4.9.1.1 Setting up IP Camera Equipped with Edge Storage

Setting up recording to the Edge Storage is performed via the 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):

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 65).

The screenshot shows the web interface for the AXIS Q7411 Video Encoder. The top navigation bar includes the AXIS logo, the title 'AXIS Q7411 Video Encoder', and links for 'Live View', 'Setup', and 'Help'. A sidebar on the left contains a list of settings categories: Basic Setup, Video & Audio, Live View Config, PTZ, Detectors, Applications, Events, Recordings (with sub-items 'List' and 'Continuous'), System Options, and About. The 'Continuous Recording' settings are displayed in the main area, specifically for 'Video Channel: 1'. These settings include an 'Enable' checkbox (checked), a 'Disk' dropdown menu (set to 'SD card'), and a 'Stream profile' dropdown menu (set to 'Quality'). 'Save' and 'Reset' buttons are located at the bottom of the settings section.

Figure 65. 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 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, 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.

4.9.1.2 Setting up SecurOS Objects

EdgeStorage Sync

Create an *EdgeStorage Sync* object (child of the *Computer* object) on each *Video Server*, where the EdgeStorage Sync feature will be used.

Video Capture Device

If using Axis cameras, create a *Video Capture Device* and set its **Type** parameter to **Axis** and **Model** parameter to **VAPIX3**.

If using Samsung cameras create a *Video Capture Device* and set its **Type** parameter to **Samsung** and **Model** parameter to **SUNAPI 2.0**.

Camera

Select the **Fill archive gaps using camera edge storage** option on the **Recording** tab (see Figure 66) of the *Camera* object created.

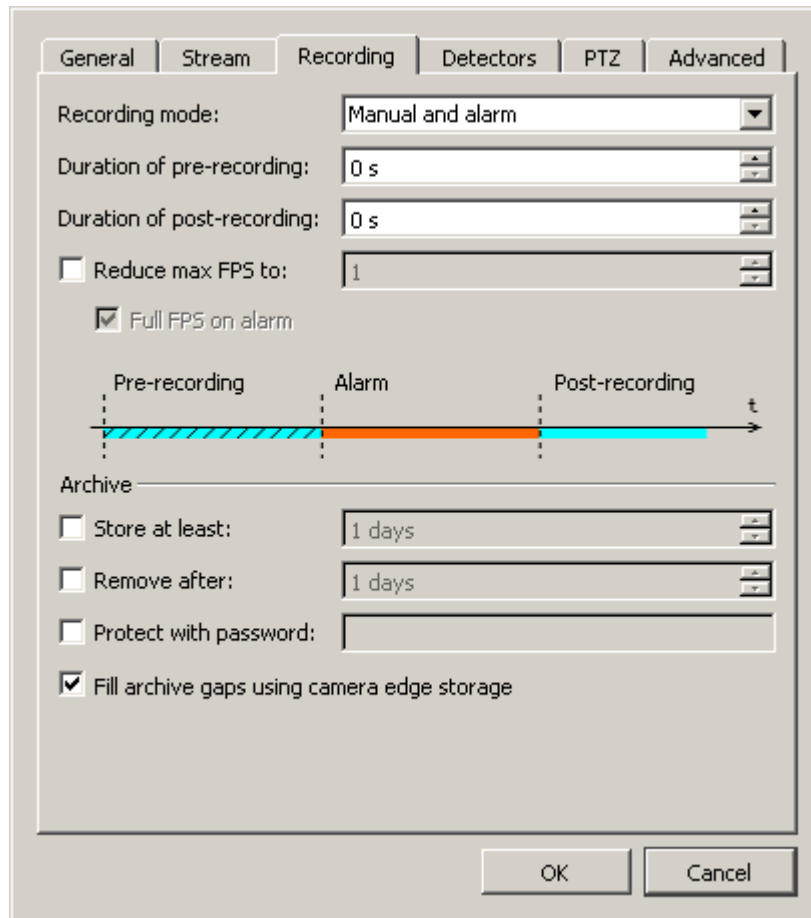


Figure 66. Recording Tab (for the Axis camera settings example)

4.9.2 Synchronization Procedure Features

The task queue to download video fragments from the *Camera's* local SD storage is generated by the *Video Server* at the moment when connection with the *Camera* is lost, and represents a list of time intervals by itself.

The start time of the interval corresponds to the *Camera* connection loss time. The end time of the interval corresponds to the reconnection time stamp or time stamp of the record termination command (REC_STOP, see [SecurOS Programming Guide](#)), if this command is allowed by the current *Camera* operation mode.

Note. In case the recording is started automatically when motion is detected, then the time interval is set to 2 seconds after connection is lost.

Once a *Camera* is reconnected, *EdgeStorage Sync* application refers to the *Video Server* and gets the task list to load *Camera's* local SD archive. If the task list is not empty, then the application searches the camera's local SD archive for the video fragments, that correspond with the time intervals specified in each task. If the corresponding fragment is not found in the archive, then the appropriate task is removed from the task list.

Downloading starts independently for each *Camera*, beginning with the oldest record. The task list is updated after each segment is successfully uploaded or connection with *Camera* is lost.

Task execution resumes when the *Camera* is reconnected.

Warning!

1. The same **Time Zone** must be specified in the camera's and SecurOS's Video Server settings.
2. Time on the camera and in SecurOS should be synchronized, otherwise archive synchronization will not start. Time synchronization should be done with the NTP server.
3. It is not allowed to manually change the time on the NTP server, otherwise synchronization will result in an error. Automatic Daylight Saving Time changes are not supported.

Notification about synchronization errors is performed via standard system tools (see **Health Monitor self-diagnostic Module** section).

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 Storage.**
- **User Rights.**

- **Computer.**
- **Monitoring center agent.**
- **Remote system.**
- **Event Filter.**
- **SNMP agent.**

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. This object is visible to the superuser only.

Parent object— none (root object).

Figure 67. System object settings window

Table 6. System object settings

Parameter	Description
Name of the system	Insert name of the object as it appears in Object Tree. Not used in any other way.
OK (Cancel)	Save/ discard changes.
System backup block	
Configuration	Select a saved configuration file from the drop-down list (all available XML-files are saved in the <code>sys_config</code> subdirectory of SecurOS program directory). Click on this field to change the name of the backup file (default name is <code>default</code>).

Parameter	Description
Save configuration	Click this button to save the current configuration (Object Tree and all object settings) to an XML-file, whose name is specified in the Configuration text box. Then, the <code>sys_config</code> folder will be created in the SecurOS root directory (if it was not there already). The SecurOS object database configuration will be saved to the <code>selected_name.xml</code> XML-file in the created folder. Warning! It is not recommended to save the configuration as <code>wizard.xml</code> because this file name is reserved and used to automatically save the last successfully loaded configuration.
Superuser password	
New password	Enter new password (see Changing Superuser Password).
Please retype	Retype new password to confirm.

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.

Also, there is a possibility to set filters for the messages being transmitted between the security zones. Using filters, message transmission can be completely or partially disabled between the different security zones. Thus, event filters between the zones are useful to apply when a zone must be completely isolated from the other ones (see detailed information in [Setting Up Event Redirection](#)).

System users can be also granted with different access rights to implement multi-level access control for the security objects (see [Defining Access Levels to Individual Objects](#)). 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.

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](#).

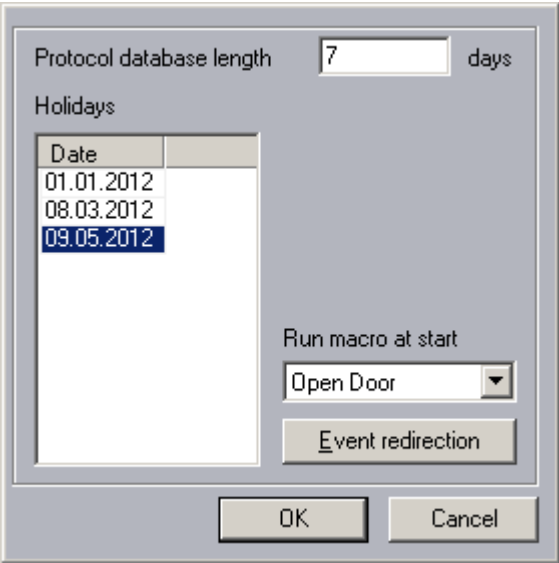


Figure 68. Security Zone object settings window

Table 7. Security Zone object settings

Parameter	Description
Protocol database length	Define length of the events database (in days, max). Event database stores events from objects that belong to this security zone only. Possible values: [0; 9999]. If this field is empty the protocol length default value is used (7 days). Messages will be deleted automatically when the retention period has expired. Removal is performed once a day at 00:00:00 a.m. (hh:mm:ss) or when SecurOS starts.
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. These holidays are also used in time zones (see Time Zone).
Run macro at start	Select from the list of accessible macros (<i>Macro</i> objects, see Macro) the one which will be activated on system startup (if necessary).
Setting Up Event Redirection	See Setting Up Event Redirection . This functionality is available in the following editions: <i>SecurOS Monitoring & Control Center</i> , <i>SecurOS Enterprise</i> , <i>SecurOS Premium</i> , <i>SecurOS Professional</i> .

5.2.2.1 Setting Up Event Redirection

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

SecurOS has the ability to setup event transmission filters between *Security Zones* or individual *Computers* within the security network. Event redirection allows to completely or partially isolate one *Security Zone* or *Computer* from another one and to setup specific event flow rules within the SecurOS network.

Warning! This feature is used to specify event redirection rules only between those computers where system core is started. In the SecurOS network these computers are the *Video Server* and *Administrator Workstation*.

Event redirection rules are specified in the **Event redirection** window (see Figure 69) which is called by clicking the **Event redirection** in the *Security Zone* object settings window (see Figure 68).

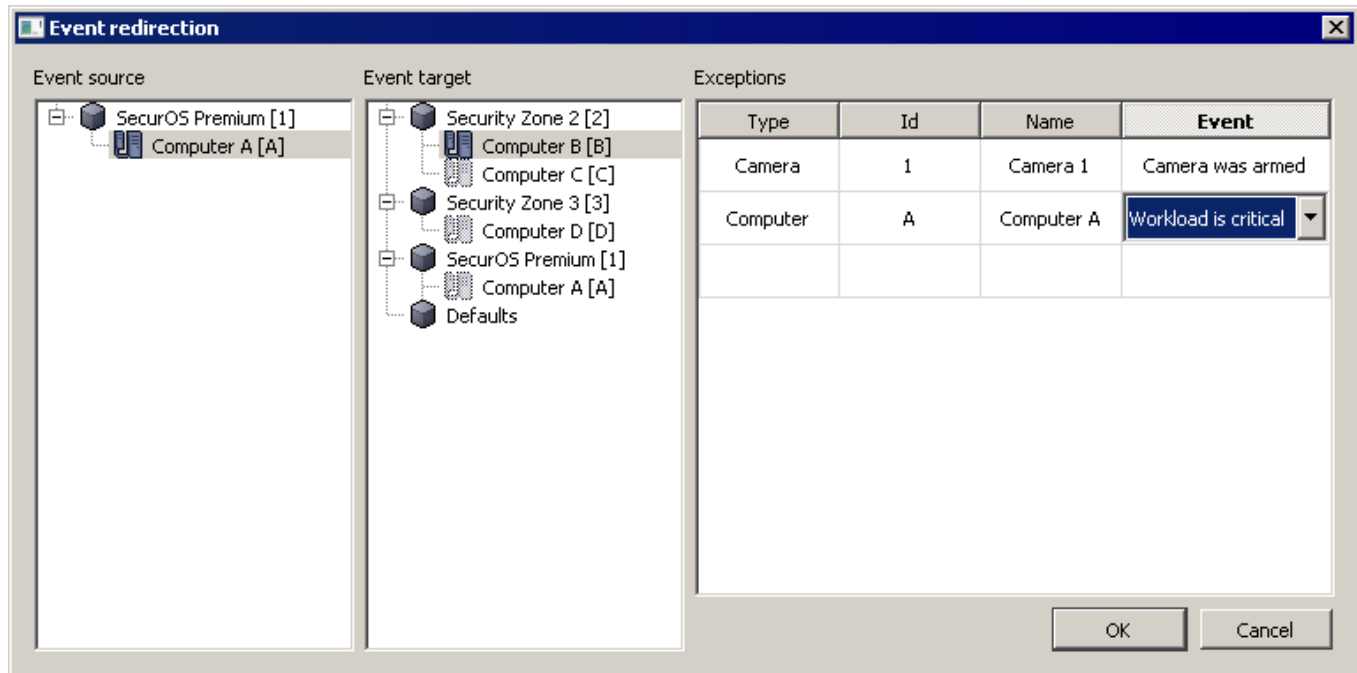


Figure 69. Event redirection window

Window has the following fields:

- **Event source** — tree of the event source objects. Includes *Security Zone* that is being configured and all its children *Computers*.
- **Event target** — tree of the event target objects. Includes all *Security Zones* within SecurOS security system and all children *Computers* grouped by *Security Zones*. In addition, the *Defaults* virtual object is displayed in the object tree (see below).
- **Exceptions** — list of events to be processed by special rules.

Event redirection rules are set independently for each pair of objects selected in the **Event source** and **Event target** blocks.

Warning! Configured rules are applied to events that are forwarded only in one direction - from event source to event target.

The following icons that define membership of the rule are available in the **Event source** block:

-  — event redirection rules are inherited from the parent security zone;
-  — computer has its own event redirection rules.

The following icons that specify general rules that affect all events are available in the **Event target** block:

-  — **receive events** — security zone receives all events from source;
-  — **do not receive events** — security zone receives no events from source;
-  — **receive events** — computer receives all events from source;
-  — **do not receive events** — computer receives no events from source;
-  — **inherited receiving** — rules are inherited from the parent security zone; computer receives events;

-  — **inherited non-receiving** — rules are inherited from the parent security zone; computer does not receive events.

Virtual *Defaults* object specifies rules that will be applied by default to each newly created event target when receiving events from the current event source object. Similarly to *Security Zone* and *Computer* both the general rules and exceptions can be specified for the *Defaults* object.

Warning! If created object will be an event source object, then the  and  (**do not receive events**) rules will be set by default for all event targets.

By default, the  type (receive events) is set automatically in the **Event source** and **Event target** fields for all *Security Zones* and the  type (inherited receiving) — for all *Computers*.

Exceptions to the general rules are specified in the **Exceptions** table. If it is necessary to specify own rule for some event within the system, this event must be added to the list of the **Exceptions** table. Such event will be handled directly opposite to the general rule. For example, if the general  (receive events) rule is set for a *Computer* and at the same time the **Exceptions** table contains some event, then the  (do not receive event) rule will be applied to this event. If the exceptions table is empty, then the general rule specified for an object in the **Event target** field will be applied to all events.

The rule specified for the *Security Zone* by initial settings is automatically used for all children *Computer* of this object. Moreover, their own, independent rules can be set for each of these *Computers* by additional settings.

To specify event redirection rules for a *Security Zone* or *Computer* do the following:

1. Open the settings window for the *Security Zone* object and click the **Event redirection** button from this panel (see figure 68). The **Event redirection** setup window will appear.
2. In the **Event source** field select a *Security Zone* or separate *Computer*.
3. Within **Event target** tree, select target object to filter events from the source object. Specify general rule for this object.
4. Specify a rule for the *Defaults* object, if necessary.
5. In the **Exceptions** table specify an events which will (or will not, depending on general rule) be delivered to the event target.

Note. Each **Event source** object may correspond to its own event list in the exception table. One can create exception table only if the **Event target** object has one the following states: , ,  or .

6. To accept the changes click the **OK** button. Click the **Cancel** button to discard all changes.

Event redirection rules example

In the network containing three *Computers* children to the one *Security Zone*, one computer is located in the main office, and the other two — one in each of the two branches, respectively. Let's the computer located in main office has the MAIN-OFFICE identifier, and computers located in branches have the BRANCH-1 and BRANCH-2 identifiers. Event redirection must be set in such a way, that the MAIN-OFFICE computer can exchange all events with the BRANCH-1 and BRANCH-2 computers, and the BRANCH-1 and BRANCH-2 computers can not exchange events themselves.

To set such rules do the following:

Note. It is supposed that no event redirection rules are not specified within the network earlier.

1. Open the **Event redirection** window. By default, all object in the object tree have a states illustrated on Figure 70.

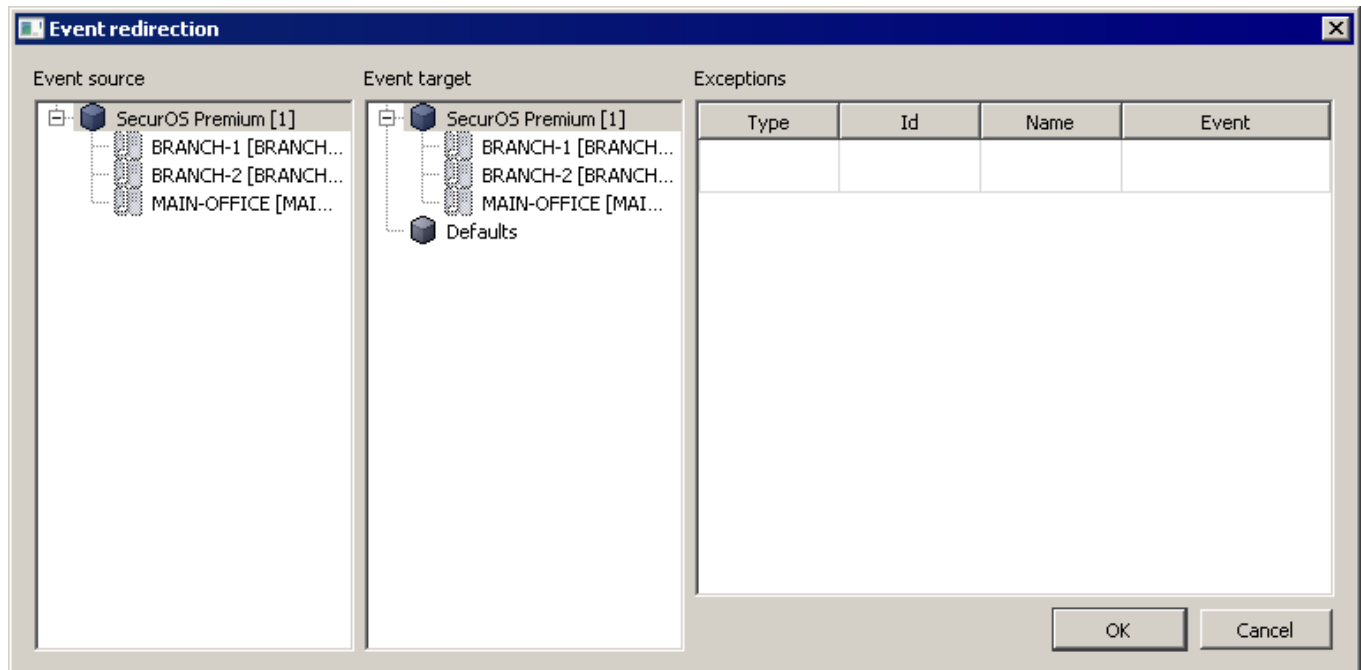


Figure 70. Event redirection window appearance at the first loading

2. Select the MAIN-OFFICE computer in the **Event source** field. Set the  state (computer has its own rules) for it. To make it possible to send event messages to the BRANCH-1 and BRANCH-2 computers, set for them the  (computer receives events) state in the **Event target** field, see Figure 71. To send all the messages leave the **Exceptions** table empty.

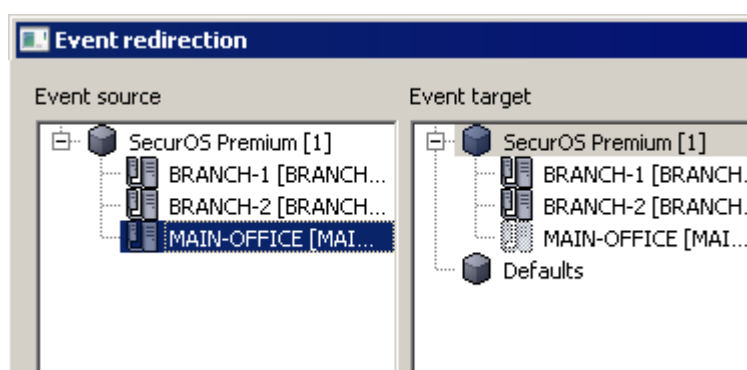


Figure 71. Setting up rules for the MAIN-OFFICE computer

3. Select the BRANCH-1 computer in the **Event source** field. Set the  state (computer has its own rules) for it. By the term, this computer must exchange messages with the MAIN-OFFICE computer, and should not exchange them with the BRANCH-2 computer. To do this, in the **Event target** field set the  (**receive events**) rule for the MAIN-OFFICE computer, and the  (**do not receive events**) rule for the BRAHCN-2 computer, see Figure 72. To send all the messages leave the **Exceptions** table empty.

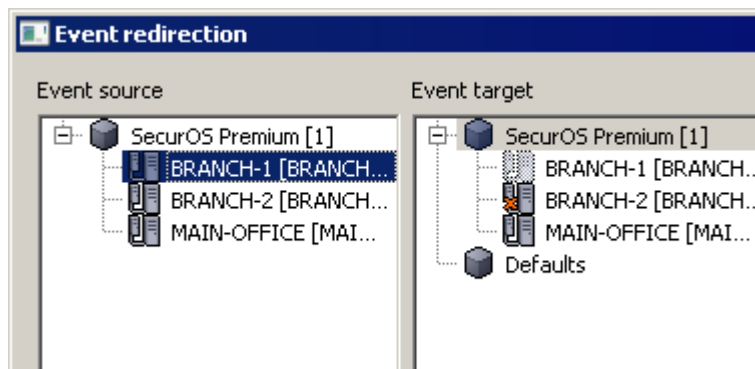


Figure 72. Setting up rules for the BRANCH-1 computer

4. Select the BRANCH-2 computer in the **Event source** field. Set the  state (computer receives events) for it. By the term, this computer must exchange messages with the MAIN-OFFICE computer, and should not exchange them with the BRANCH-1 computer. To do this, in the **Event target** field set the  (**receive events**) rule for the MAIN-OFFICE computer, and the  (**do not receive events**) rule for the BRAHCN-1 computer, see Figure 73. To send all the messages leave the **Exceptions** table empty.

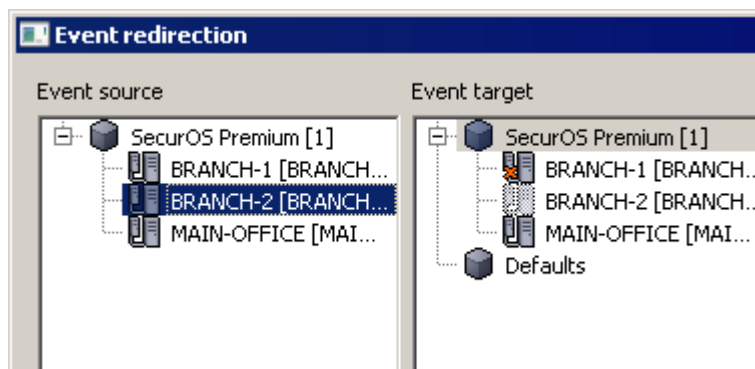


Figure 73. Setting up rules for the BRANCH-2 computer

5. Click the **OK** button to save the changes.

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**.

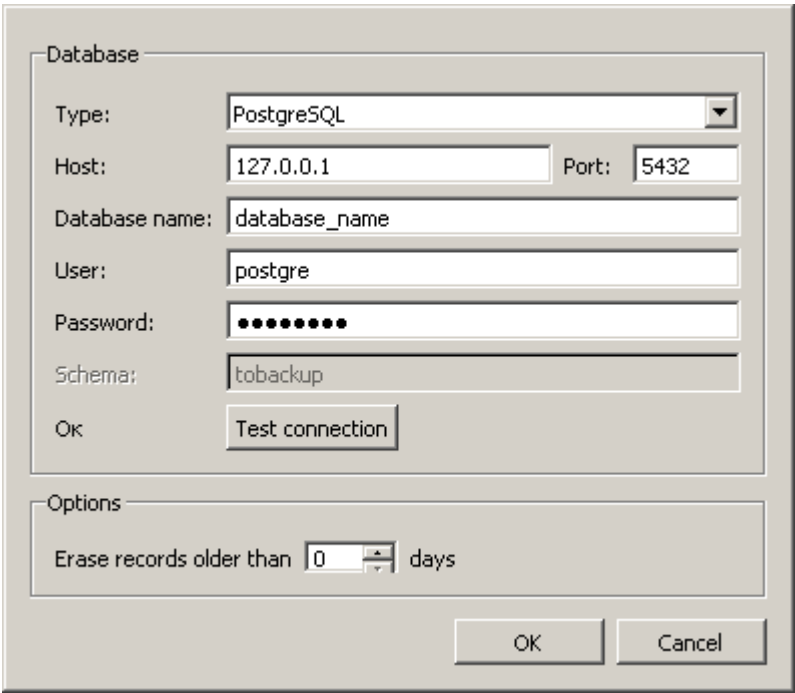


Figure 74. Database object settings window

Table 8. Database object settings

Parameter	Description
Database	
Type	Database type. Possible values: • PostgreSQL – provides connection with PostgreSQL database; • SQL Server – provides connection with Microsoft SQL Server database. Default value is PostgreSQL.
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	Database name, user name and password are as defined during the database installation. Warning! Use Latin characters only when specifying a Password. Latin-1 code page (Western European character set) is acceptable.
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	

Parameter	Description
Erase records older than	Retention period for records (in days). If set to 0, the records are not deleted. Note. When working with some of the SecurOS intelligent Modules parameter is ignored.
Buttons	
OK	Click to save the changes and leave administration mode.
Cancel	Click to discard the changes and leave administration mode.

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 [Managing User Rights Within Security Network](#)).

Note. Several *Department* objects within the same parent object are combined into the **User accounts** logic group in the Object Tree.

Parent object — [Security Zone](#).



Figure 75. Department object settings window

Table 9. Department object settings

Parameter	Description
Id	<i>Information field:</i> object identifier. Read-only.
Name	Enter meaningful object name as it appears in the Object Tree (e. g. department name).

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](#).

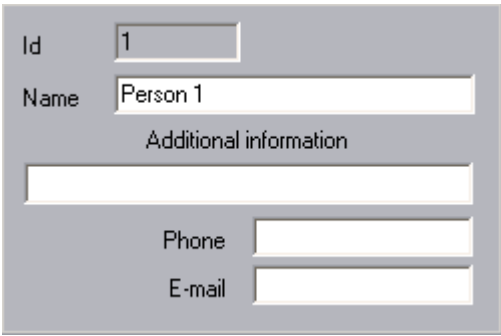
A screenshot of the 'User Account object settings window'. It features a grey background with several input fields. At the top, there is an 'Id' field containing the number '1'. Below it is a 'Name' field containing the text 'Person 1'. Underneath the 'Name' field is a section labeled 'Additional information' followed by a large empty text area. At the bottom, there are two more fields: 'Phone' and 'E-mail', both of which are currently empty.

Figure 76. User Account object settings window

Table 10. User Account object settings

Parameter	Description
Id	<i>Information field:</i> object identifier. Read-only.
Name	Insert meaningful person's name.
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.
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.

5.2.6 Active Directory Storage

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](#).

Note. Several *Active Directory storage* objects within the same parent object are combined into a **Active Directory storages** logic group in the Object Tree.

Parent object – [Security Zone](#).

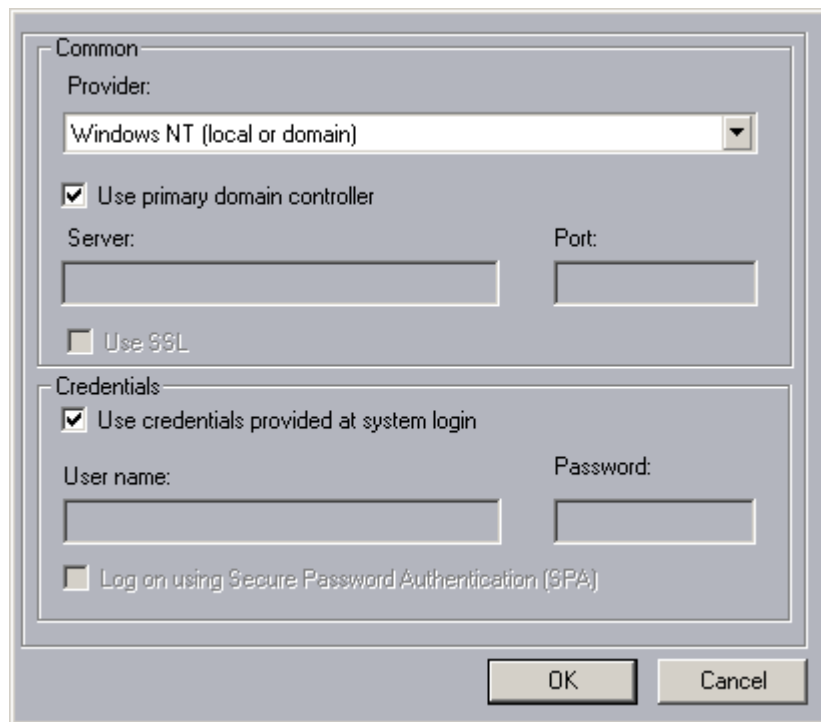


Figure 77. Active Directory Storage object settings window

Table 11. Active Directory storage object settings

Parameter	Description
Provider	Select the type of protocol from the drop-down list. Possible values: 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.
Server	Specify server or local computer name.
Port	<i>Optional:</i> specify server network port for connection. Used on specific server setting.
Use SSL	Reserved for future use.
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. These and the following fields are not active when the previous field is activated.

Parameter	Description
Log on using Secure Password Authentication (SPA)	Reserved for future use.

5.2.7 User Rights

This object is used for defining user rights within the system (see [Defining Access Levels to Individual Objects](#) for detailed description).

Notes:

1. 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.
 2. Several *User Rights* objects within the same parent object are combined into the **User Rights** logic group in the Object Tree.
-

If in the system configuration there is at least one *User Rights* object with an installed provider (the *Active Directory Storage* object, see [Active Directory Storage](#)) and the **Users and Groups** field is not empty, then the user logging into SecurOS must be currently logged into Windows. Thus the password check is delegated to the Operating System, and it is not important to enter a password when starting SecurOS.

Parent object – [Security Zone](#).

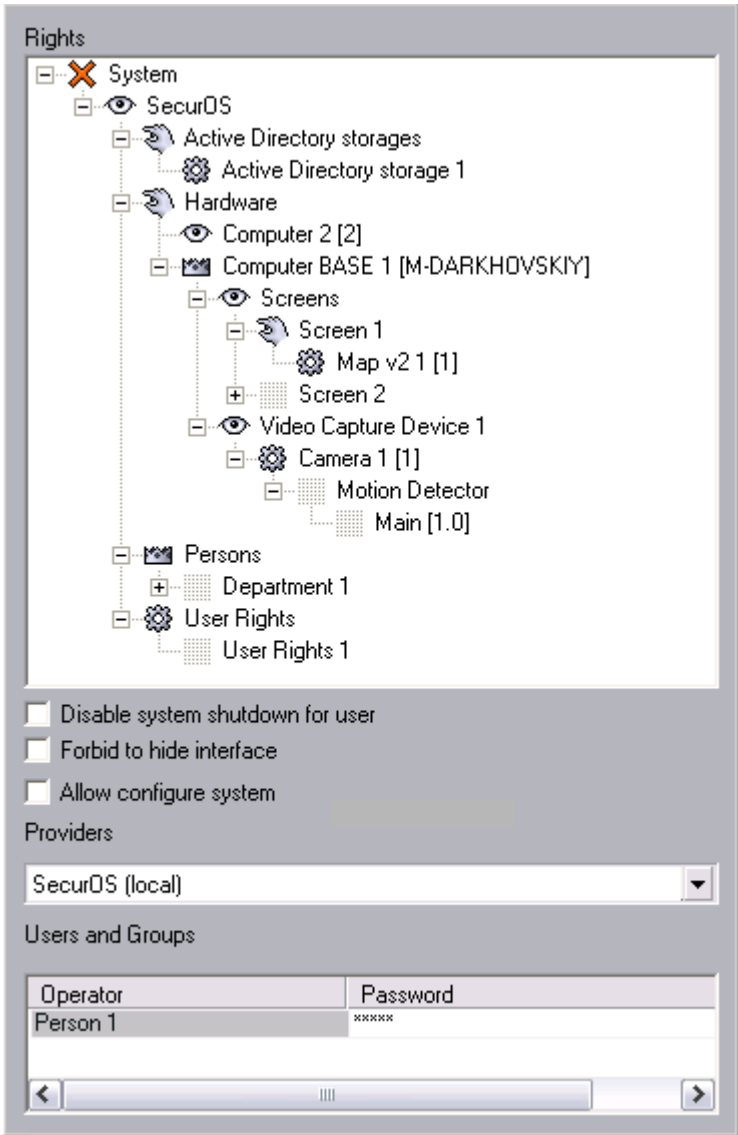


Figure 78. User Rights object settings window

Table 12. 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 consecutively, until the required icon is displayed. See Fig. 79 below for all possible icons.
Disable system shutdown for user	Select this field to disable quick shutdown via control panel (menu  (Change user/Shutdown system)→ Shutdown). Note. To shutdown client/server software, the user should select Log Off command from  menu (Change user/Shutdown system). In the authorization window the user name and password which allows system shutdown must be provided. Click the Shutdown button to confirm shutdown.

Parameter	Description
Forbid to hide interface	Select this field if user is not allowed to hide user interface objects.
Allow configure system	Select this field to allow access to the Object Tree and Tool Bar for these users.
Providers	Choose SecurOS (local) value to accept rights to access the selected objects for users from the Users and Groups table (see below) or choose the <i>Active Directory Storage</i> object name as it appears in the Object Tree to accept certain rights to user / user groups of the network domain (see Active Directory Storage).
Users and Groups (list of users and groups that have the above rights). On selecting the <i>Active Directory Storage</i> object from the Providers list, the list should be formed as described in Configuration of Network Domain User Rights .	
Operator	Double click and select an existing <i>User Account</i> object. The name of the person will be used as the username when logging into SecurOS. Note. The same user (<i>User Account</i> object) cannot be added to 2 or more different <i>User Rights</i> objects.
Password	This field cannot be left blank.

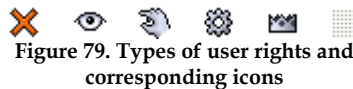


Figure 79. Types of user rights and corresponding icons

Each user access level corresponds to an icon from the following list (see Figure 79 from left to right):

- **No access**— the user has no access to the object neither in administrative or operator mode. The object, though, is still visible as a node in system Object Tree when in administrative mode.

Warning! If such access level is configured for a certain Computer object and a number of users, then these users cannot log into the system on this computer.

- **View**— the user has no administrative access to the object, but the object (if it is a user interface object like *Monitor* or *Audio Player*) can be visible in the operator interface. *Macros* (Macro objects) that have this level of access can be executed from within the operator interface.
- **Control**— same as View rights, but the user can additionally control the object from within the operator interface (i. e. arm/disarm video cameras).
- **Configure**— same as Control rights, but the user can view and change object settings from within the administrator interface (user cannot delete existing object and cannot create child objects under this object).
- **Full access**— same as Configure rights plus ability to delete this object and create child objects.
- **Inherited rights**— rights for this object are inherited from parent object (when new objects are created, they have this access level by default).

Notes:

1. Several object types (like *System*, *Program*, *Department*) that do not have visual representation within the user interface on operator workstations, cannot have *View* and *Control* access level types.
2. If a user creates new a User Rights object, he/she cannot define the rights for this object to exceed the current user rights of the user.

5.2.8 Computer

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

The servers and workstations in the SecurOS network are registered and represented as *Computer* objects in the system Object Tree. The servers run the SecurOS server application, and the workstations run the SecurOS client application.

The SecurOS workstations can send and receive events from all the other security network nodes. Filters can be used to select the events that will be transmitted from one SecurOS network computer to the other ones. This can help limit the network load caused by event transmission (see [Setting Up Event Redirection](#)).

Warning! Servers that the current computer is forbidden from connecting to, are marked by a green cross in the Object Tree on this computer (see figure 80 and **Servers to connect** parameter in the *Computer* object settings below). With this setting, system event transmission is not completely closed but only limited by the event transmission settings.

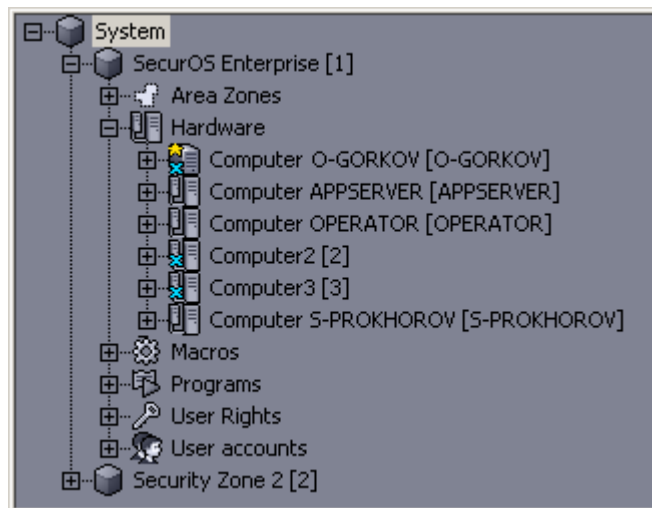


Figure 80. Object Tree containing Computers with blocked connection

Note. Several *Computer* objects within the same parent object are combined into the **Hardware** logic group in the Object Tree.

Parent object – [Security Zone](#).

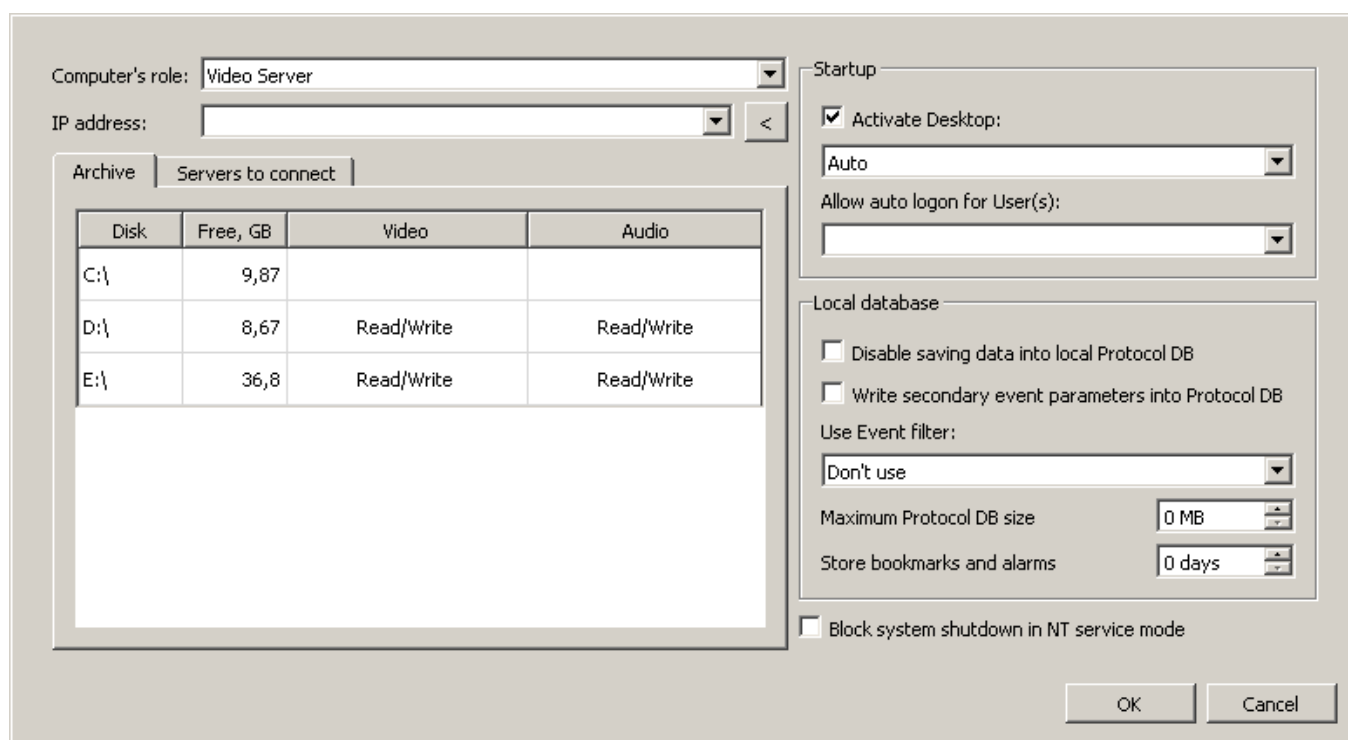


Figure 81. Computer object settings window

Table 13. Computer object settings

Parameter	Description
Computer's role	This value should correspond to the computer setup type, selected during software installation. Possible values: - Operator Workstation — computer will operate as network client (even in case of other type of SecurOS installation); - Video Server, Administrator Workstation — computer will operate as a 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.
Archive Tab (table of available local hard disks (HDD) or logical drives with permission to store video and audio data)	
Warning! The tab is available only if computer's Computer's role parameter is set to <i>Video Server</i> .	
Drive	Drive name to store archives (letter of drive). If local computer is being configured the list consists only of available drive letters. Select required letter. If a remote computer is being configured the list consists of all letters from A to Z. In this case select required letter. Select the required disk letter. Besides hard drives, removable media drives and mounted network folders can be displayed in the table.

Parameter	Description
Free GB	<i>Information field:</i> current free space on selected disk in GB.
Video	Choose settings for video archiving (by double clicking in the white space corresponding to the necessary drive letter). Possible values: • <code>empty</code> — access denied. • <code>Read Only</code> — video archive can be read from this disk, but writing to this disk is disabled. • <code>Read/Write</code> — reading from and writing to this disk is allowed.
Audio	Choose settings for audio archiving (by double clicking in the white space corresponding to the necessary drive letter). Possible values: • <code>empty</code> — access denied. • <code>Read/Write</code> — reading from and writing to this disk is allowed.
Servers to connect Tab See Servers to connect 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 login for User(s)	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 <code>root</code>. It is impossible to set up the field value to <code>root</code>. Note. For detailed information about setting order and rules of the procedure see the Auto login section. User group can be specified if an Active Directory Storage object is configured within the system. When specifying user group name use the @ prefix before its name, for example, @usergroup.
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 losing events.

Parameter	Description
Write secondary event parameters into Protocol DB	Select this checkbox to enable message parameters to be recorded into the <code>PROTOCOL_PARAMS</code> database. Warning! This option is used in conjunction with the ISS analytics modules only (see www.isscctv.com). 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).
Store bookmarks and alarms	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. [0; 3660]. Default value is 0 (parameter is not used). If 0 value is set bookmarks and alarms will be deleted along with the operative archive. Warning! Field is available only if Computer's role parameter is <i>Video Server</i>.
Block system shutdown in NT service mode	Turn this option on to forbid the user to shutdown the system (Shutdown command of the Change user/Shutdown system system menu ( on the <i>Control Panel</i> is unavailable), if SecurOS is started as a Windows service (see ISS Startup Configuration Utility). This functionality is available in the following editions: <i>SecurOS Monitoring & Control Center</i>, <i>SecurOS Enterprise</i>, <i>SecurOS Premium</i>, <i>SecurOS Professional</i>.

5.2.8.1 Servers to connect

Parameter is used to connect *Operator Workstation* to the SecurOS network, and also to configure a type of connections that defines message exchange routes between SecurOS servers within security network

Note. The "SecurOS server" term is used to designate a computer, where system core is started. In the SecurOS network these computers are the *Video Server* and *Administrator Workstation*.

Appearance of the tab is represented on figure 82.

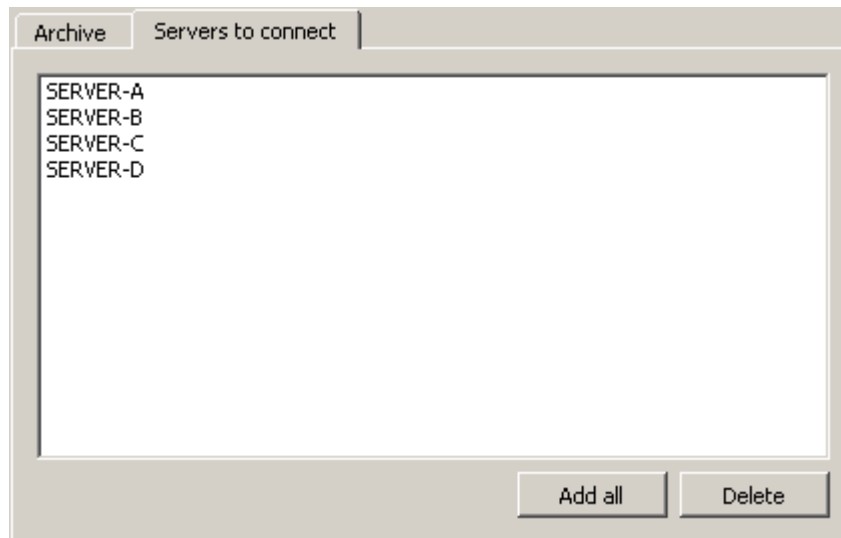


Figure 82. Servers to connect tab

Using parameters when configuring SecurOS Operator Workstation

Operator Workstation is a client application and must be connected to the SecurOS server. List of servers to which operator's computer can connect is shown in the **Servers to connect** parameter. Connection to the SecurOS server can be performed in automatic or manual mode.

Note. When *Operator Workstation* is started for the first time, it can be connected only in manual mode. Each next time you start the computer the connection is performed according to its current settings.

In manual mode server to connect is specified by operator in the **Authorization** window (see [SecurOS Quick User Guide](#)). In automatic mode connection is performed in order the servers are enumerated in the list which determines the priority of connection. So, in first turn connection will be established with the server that is located at the top of the list. If this server is currently unavailable, an effort to connect to the second server from the top of the list will be performed, etc. When current connection with a server is lost reconnection will be performed in a similar way.

Using parameters when configuring SecurOS server

Two type of connections between SecurOS servers can be used to exchange the messages within SecurOS network – "each-to-each" connection and "direct connection".

"Each-to-each" connection

If "each-to-each" connection is used, event message is transmitted from the source server to all servers within network (or within separated network segment). When message is delivered to the target server it is not transmitted further (if message itself contains no other rules). To provide such type of connection the **Servers to connect** parameter must be empty for all servers within network (is the default value).

This type of connection is most efficient to transmit messages from the viewpoint of system cores loading, speed and reliability of data transmission, etc. Furthermore, no additional settings of the **Servers to connect** parameter are required to use this type of connection, that is a nontrivial task in each case. Thus, it is recommended to use this type of connection each time, if there are no special requirements to use "direct connection" (see below).

"Direct connection"

As opposite to "each-to-each" connection, "direct connection" supposes that messages are transmitted only between selected servers. In simplest case, if direct connection is configured between two servers, then message will be transmitted only from one server to another and will not be delivered to any other server within network. At the same time, depending on the settings, connection between these servers can be both single-sided and double-sided, i.e. messages can be transmitted either in one, or in both directions. To provide such type of connection it is necessary to specify identifiers of the selected servers in the **Servers to connect** parameter list (see [Operations with the Servers to connect List](#)).

Thus, using "direct connection" one can limit general number of messages on a certain segment of the network.

Warning! This feature is not designed to limit message exchange. To provide partial message exchange use events filtering feature (see [Setting Up Event Redirection](#)).

It is recommended to use this type of connection only in following standard cases:

1. Connection between network segments is provided through public communication channel;
2. Network segments are connected with the help of private communication channel that has low throughput.

In these cases it is reasonably to set up separated server in each network segment to provide data transmission. Identifier of the opposite server must be specified in the **Servers to connect** parameter of each server. At the same time, to provide message transmission between separated server and all other servers within it's segment it is necessary to specify identifiers of these servers on the separated server. In addition, to provide message transmission between all other servers within network segment, it is necessary to specify identifiers of other servers on each server, including identifier of separated server. Schema of connection for such data transmission type is illustrated on Figure [83](#).

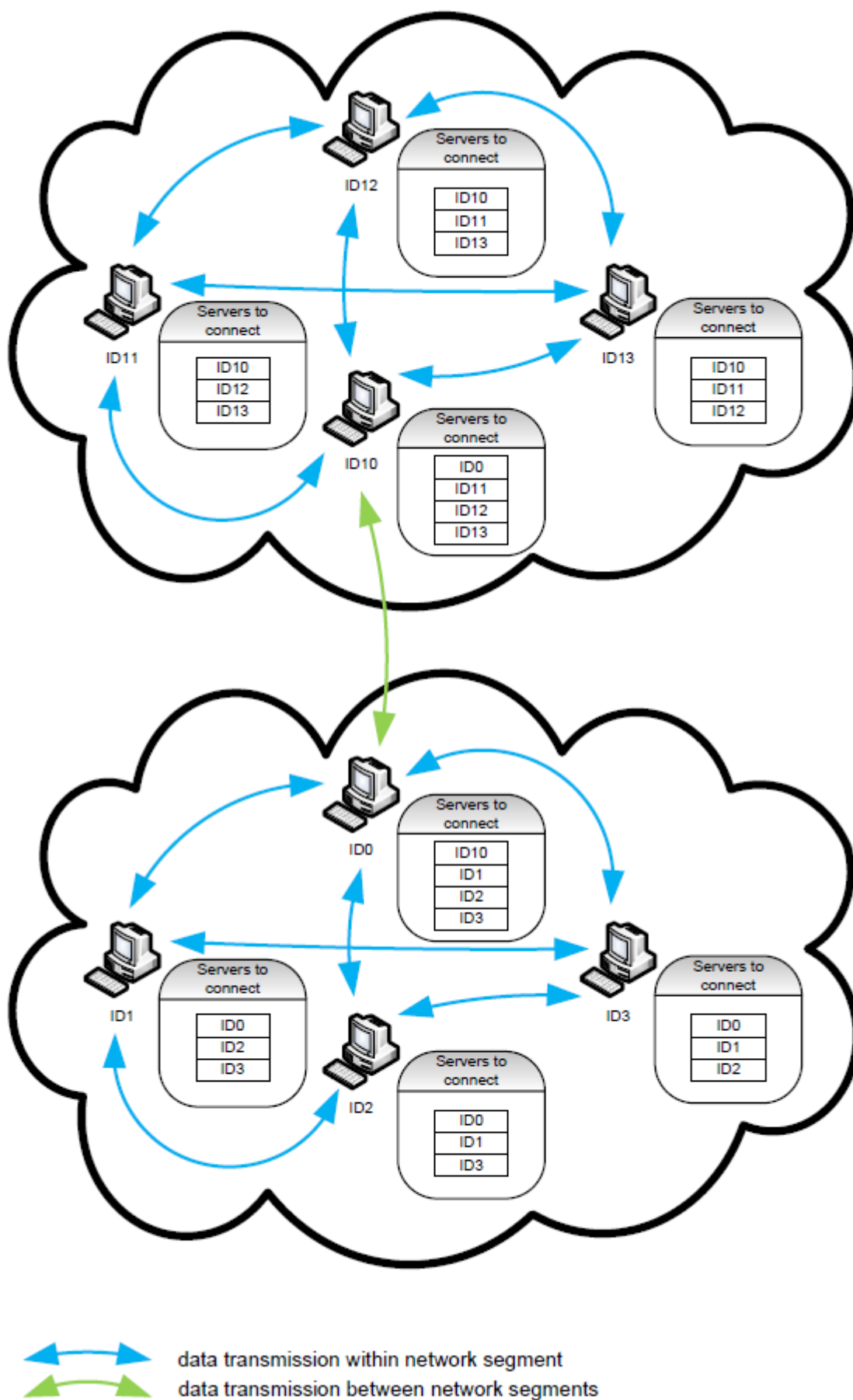


Figure 83. Using direct connection to provide internetwork communication

Main imperfection of direct connection is the impossibility to transmit the messages when communication between separated servers is lost. To improve the reliability one can create redundant direct connection using couple of other separated servers (see Figure 84). Then, if one of the communication channel is broken, a message will be delivered over redundant one.

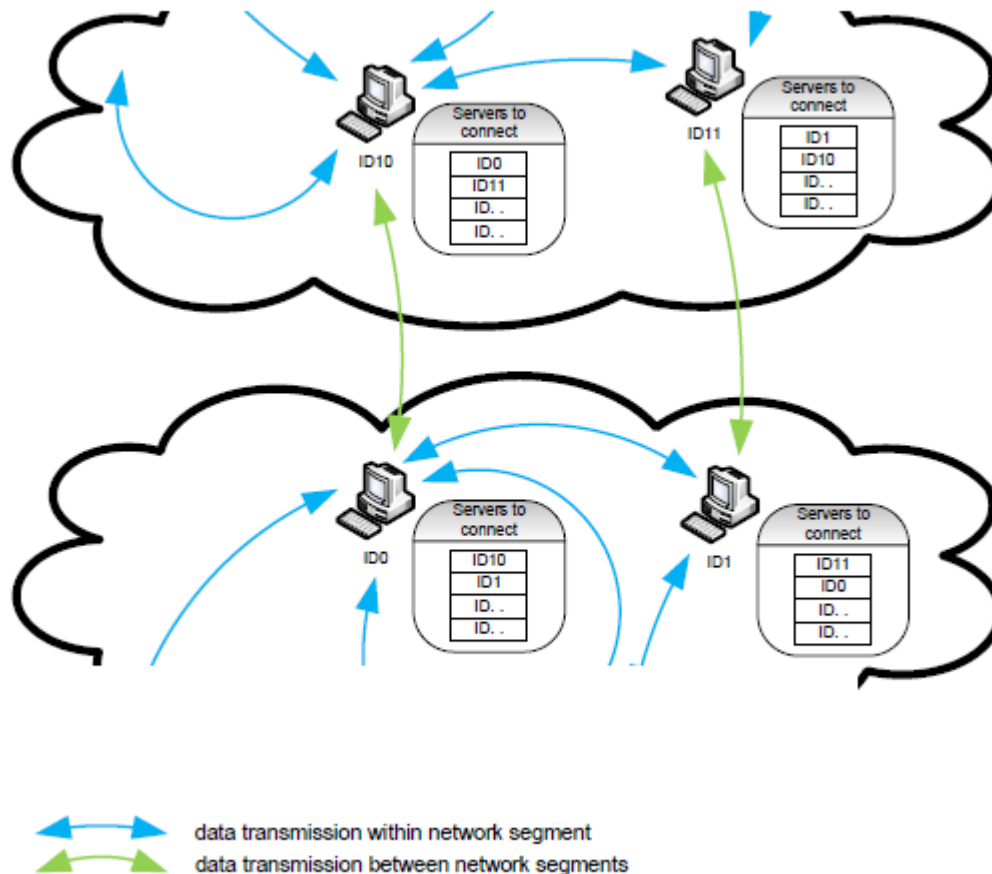


Figure 84. Redundant direct connection between segments

At the same time an additional settings of the **Servers to connect** parameter are required on each server of each network segment.

5.2.8.1.1 Operations with the Servers to connect List

The following operations are available with the list:

1. *Add server to list* — to add a server to the list double click the upper table entry, then select required server from the drop-down list.
2. *Delete server from list* — to delete a server from the list select the required table entry, then press the **Delete** key or click the **Delete** button.
3. *Add all available network servers* — to add all network *Computers* to the list click the **Add all** button.
4. *Change server entry position in the list* — to move server entry within the list use drag-and-drop method to change its current position.

Note. The sequence of connections is defined by the position in the list, starting from the top.

The following rules must be followed when working with the list:

1. When a server is added to the list, the *Computer* that is currently being configured automatically is added to the similar list of the other server.

Note. If the **Servers to connect** list of the added server is empty, the configured *Computer* will not be added to it's list.

2. When deleting a server from the list, the *Computer* that is currently being configured will not be automatically deleted from the list on that server.

5.2.8.2 Auto login

The auto login feature in SecurOS depends on the user authentication method used.

In the case of the authentication process that uses the SecurOS DB, the **Allow auto logon for User(s)** parameter can be set to:

- Name of any user, registered in the current *Security Zone* object within the SecurOS network (**Object Tree → User Accounts → Department → User Account**), excluding the `root` superuser.

Notes:

1. The system will display an appropriate information message if the entered user name is not registered in the SecurOS DB.
 2. The system will display an appropriate information message if the entered user name is registered in the SecurOS DB, but *User rights* are not defined for that user.
-

- "Not set" (default value).

Warning! Auto login is impossible if default value is used.

In the case of the authentication process that uses Windows Network Active Directory domain the **Allow auto logon for User(s)** parameter can be set to:

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 Storage](#)).

- 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.
- "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 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 provide a connection between the current and other SecurOS security systems (i.e. Monitoring Centers, see [Video Surveillance Using Remote SecurOS Security System](#)).

Parent object – **Computer** – any of the SecurOS network Servers.

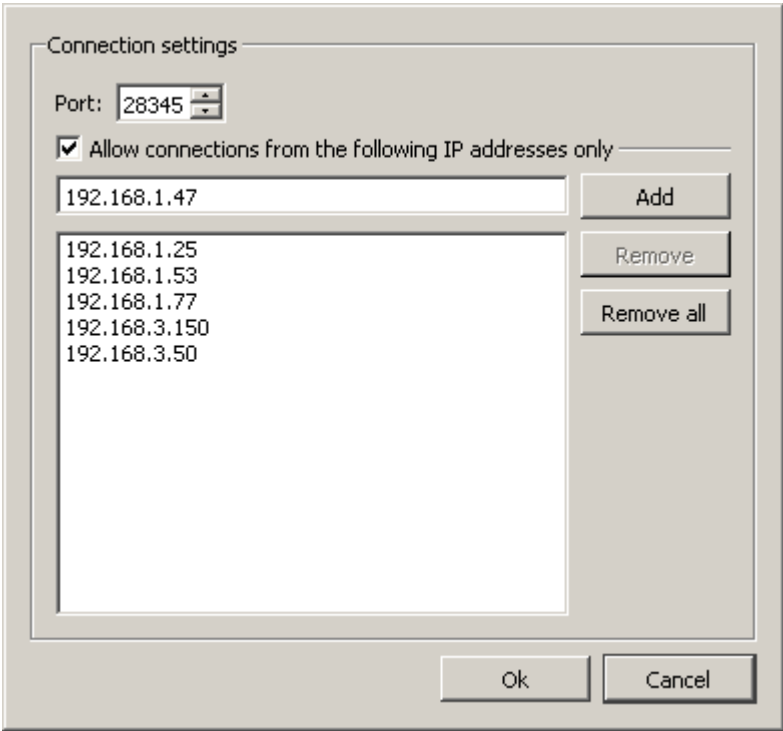


Figure 85. Monitoring center agent object settings window.

Table 14. Monitoring center agent object settings

Parameter	Description
Connection settings	
Port	Communication port for interaction between two SecurOS security systems. Default value is 28345.
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	List of the IP addresses of computers, that are allowed to connect to the given SecurOS security system.
	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.

5.2.10 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 a remote SecurOS security system.

Parent object – **Computer** – any *Computer* of the SecurOS network which has a *Video Server* role.

Figure 86. Remote system object settings window

Table 15. Remote system object settings

Parameter	Description
Integration settings	
Host	Is used to select a <i>Computer</i> within the SecurOS security system to connect to. Specify the IP address. Required parameter.
Port	Communication port for interaction between two SecurOS security systems. Required parameter. Default value is 28345.
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 Monitoring Center's server, then all <i>Cameras</i> , that are not listed will be removed when updating configuration.
Use remote Camera IDs	Select this checkbox to import <i>Cameras</i> and keep the IDs, assigned to the objects in remote system.

Parameter	Description
Update configuration (button)	Update configuration on the Monitoring Center's server in accordance with specified parameters. Warning! The button becomes enabled by reopening object settings window after current settings are applied.

Setting up Monitoring Center To Work with Remote Archives

To configure Monitoring Center to work with remote archives do the following:

1. Create and configure *Monitoring center agent* object on any of remote system's server and *Remote system* object on any of the Monitoring Center's server;
2. Click **Update configuration** in the *Remote system* object settings window.

When receiving or updating a configuration, the system will create the following objects:

1. *Proxy-computers* - "copies" of all of the *Computer* objects existing within the remote security system. All created proxy-computers are children of the *Remote system* object and have names of the following format: <Remote system Name>:<Computer Name>.
2. *Video Capture Devices* with *ISS Video Concentrator* device type 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.

Notes:

1. The channel number for each of the created cameras will possess the **ID** value of the appropriate *Camera* existing within the remote security system.
 2. No Motion Detection Zones are created for the *Cameras* (related to the cameras of the remote configuration).
-

Setting up Monitoring Center To Work with Local Archives

To configure Monitoring Center to work with local archives change the type of the created *Video Capture Devices* (see p. 2). To do this, open the object settings window of all the created *Video Capture Devices*, select the *Video Repeater* value in the **Type** box, and 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.

Created objects make it possible for the operator to monitor the events generated by the *Camera* and *Computer* objects of the remote security system with the help of the *Map Window*, *Monitor*, and *Event Viewer* objects of the Monitoring Center.

5.2.11 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**.

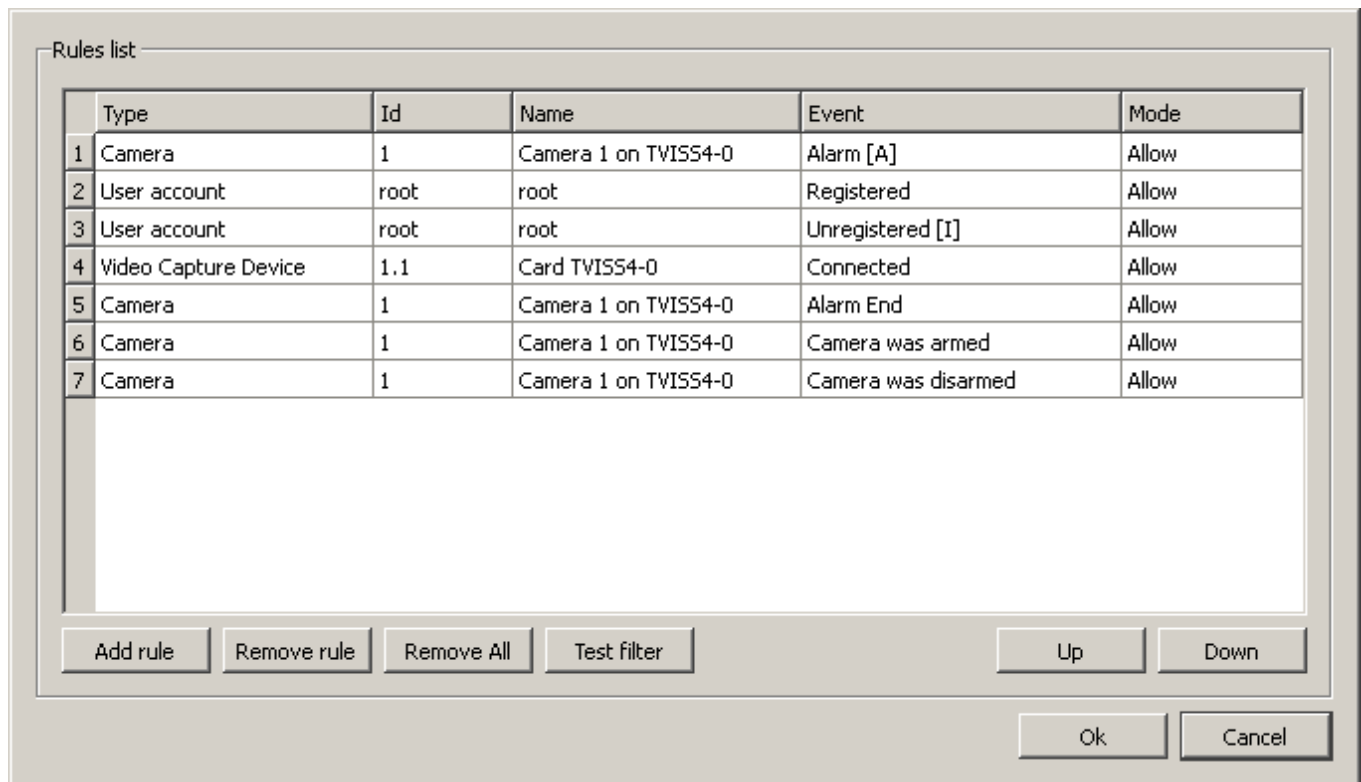


Figure 87. Event Filter object settings window

Table 16. Event Filter object settings

Parameter	Description
Rules list	
Type	Type of the system object (that is the event source).
Id	ID of the system object (that is the event source).
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).
Event	Event to process. List of values depends on the object type. If not set, rule affects all objects' events. Notes: Besides an individual or all events of an object, one of the following predefined event groups can be selected as well: 1. Alarm only. 2. Information only. 3. Alarm and information. • To create a filter rule for the individual objects' event, select it from the list of possible object events. • To create a filter rule for the all objects' events select the blank string. • To create a filter rule for one of the predefined event groups, select that group (in the top of the list).

Parameter	Description
Mode	Rule result. Possible values: • 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.
Down	Button is used to sort rules manually. Click to move the rule one position down.
OK	Click to save the changes and leave administration mode.
Cancel	Click to discard the changes and leave administration mode.

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

1. Click **Test filter** in the Event Filter object settings window (see fig. 86).
2. System will display **Events to test** section (see fig. 88).

Rules list

	Type	Id	Name	Event	Mode
1	Camera	1	Camera 1 on TVISS4-0	Alarm [A]	Allow
2	User account	root	root	Registered	Allow
3	User account	root	root	Unregistered [I]	Allow
4	Video Capture Device	1.1	Card TVISS4-0	Connected	Allow
5	Camera	1	Camera 1 on TVISS4-0	Alarm End	Allow
6	Camera	1	Camera 1 on TVISS4-0	Camera was armed	Allow
7	Camera	1	Camera 1 on TVISS4-0	Camera was disarmed	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
2	Camera	1	Camera 1 on TVISS4-0	Alarm [A]	Event is allowed by rule 1.

Add event Remove event Remove All Run test

Ok Cancel

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.

5.2.12 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**.

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.

5.2.12.1 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.

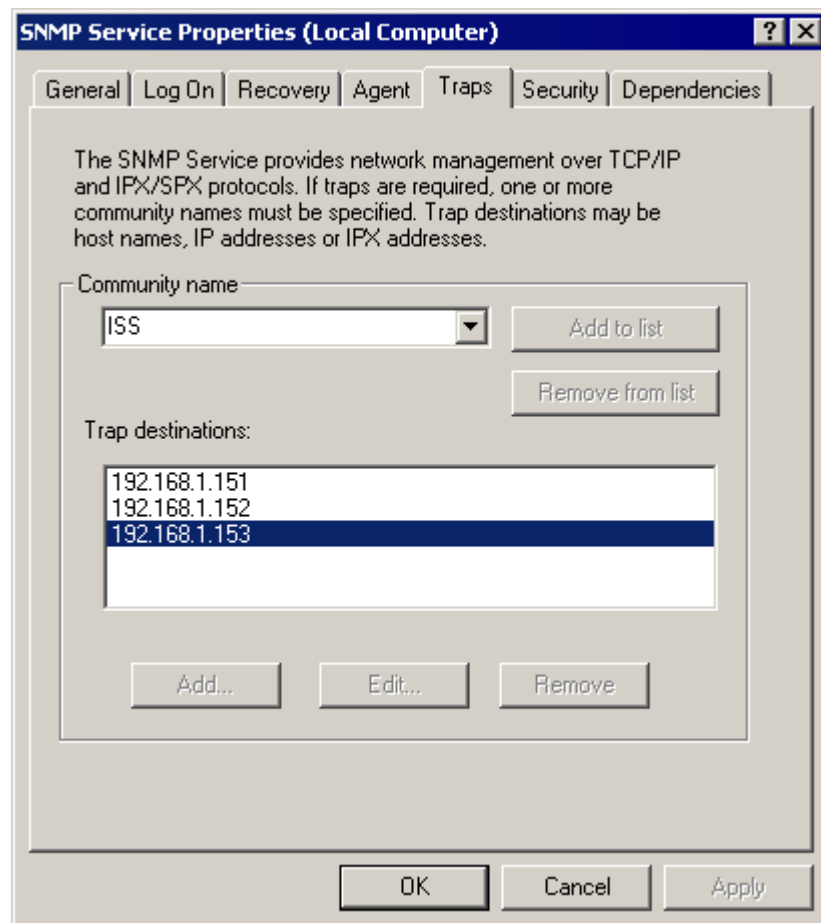


Figure 89. Traps tab of the SNMP Service settings window

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

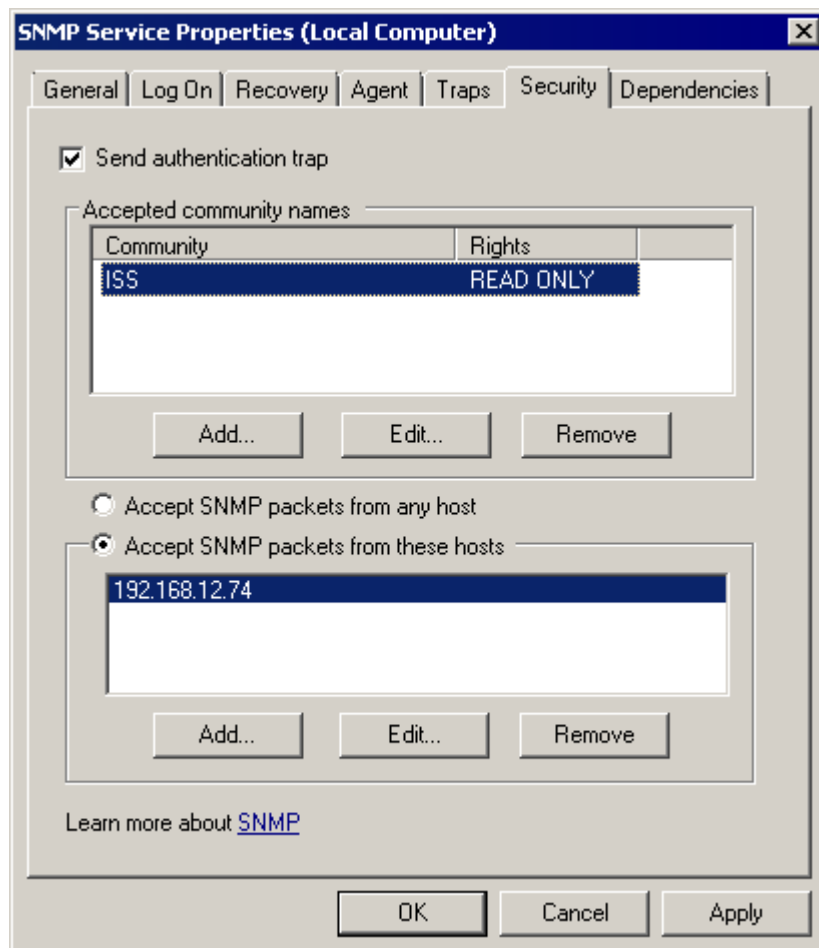


Figure 90. Security tab of the SNMP Service settings window

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.

5.3 Configuration Examples

This section describes specifics of the core subsystem objects and includes examples of their configuration.

5.3.1 Defining Access Levels to Individual Objects

SecurOS supports managing administrator and operator rights for individual persons and individual objects. This is done via the configuration of *User Account* objects (which define real user accounts) and *User rights* objects – sets the access levels for users / user groups, for each object within the SecurOS security network.

Also, the access level rights can be configured for the users of an already created network domain, which includes computers of a certain security zone (see [Configuration of Network Domain User Rights](#)). In this case, local security zone user accounts will be disabled.

Warning! If the security system has more than one security zone, you must define user rights for each security zone, otherwise you will be able to automatically login to the system with system-wide superuser rights from any computer that belongs to the unrestricted security zone!

After you have defined user rights within the security network, SecurOS will require to enter a username and password on software startup. Since every computer belongs to some security zone, you can login under users that belong to the same security zone as the computer in question. Other username/password combinations will not work, even if they are valid within other security zones.

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 a *Department* object (see [Department](#)) under a *Security Zone* object.
3. Create the necessary number of *User Account* objects (see [User Account](#)) within this *Department* object by the required number of SecurOS system users (administrators/operators).
4. Create *User Rights* objects within the *Security Zone* object. Its settings window (see [User rights](#) section) contains the exact copy of the system Object Tree. Edit the access rights (for one or more users) by clicking the icons next to the object's name consecutively until the preferred level of access is selected.
5. Repeat steps 2–4 for each security zone within your network. For each security zone the Object Tree would contain elements shown in figure 91.

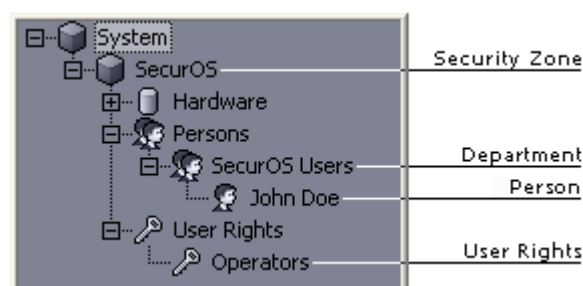


Figure 91. Objects Tree with Department, User Accounts and User Rights objects

5.3.2 Configuration of Network Domain User Rights

In this section the procedure of *Active Directory* storage (see [Active Directory storage](#)) and *User rights* object parameter configuration is described for the domain provider (Windows NT or LDAP) that receives the SecurOS user authorization request.

5.3.2.1 Settings for Windows NT Provider

To set domain parameters for Windows NT provider:

1. In *Active Directory storage* (see [Active Directory storage](#)) 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 **Log on using Secure Password Authentication (SPA)** checkbox.

To set user rights for a user, fill the **Users and Groups** field in the *User rights* object settings window (see [User rights](#) section) with a series of network domain user login names separated by commas (e. g. j-smith).

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.

5.3.2.2 Settings for LDAP Provider

To set domain parameters for LDAP provider:

1. In the *Active Directory storage* object settings window (see [Active Directory storage](#) section) 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. Optional: fill Port field with value of 389 (number of LDAP server port).
4. 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).
5. If the **User name** and **Password** fields are filled, select the **Log on using Secure Password Authentication (SPA)** checkbox.

To set user rights for a user, fill the **Users and Groups** field in the *User rights* object settings window (see [User rights](#)) with a series of the following strings: &(objectClass=user) (sAMAccountName=j-smith).

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 is a system folder where Users users group is placed.

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.**
- **HTML Dialog.**

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.**

Warning! All user interface visual components 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 PTZ control dialog window, video displaying monitor and an audio player to work with the microphone. On the second Desktop there could be a second monitor to watch cameras from the second room, and a map of the whole territory to provide visual access to all the security devices and to control their states.

Note. Several *Desktop* objects within the same parent object are combined into the **Desktops** logic group in the Object Tree.

Object has no settings to configure.

6.1.2 Map

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

Parent object – **Security Zone.**

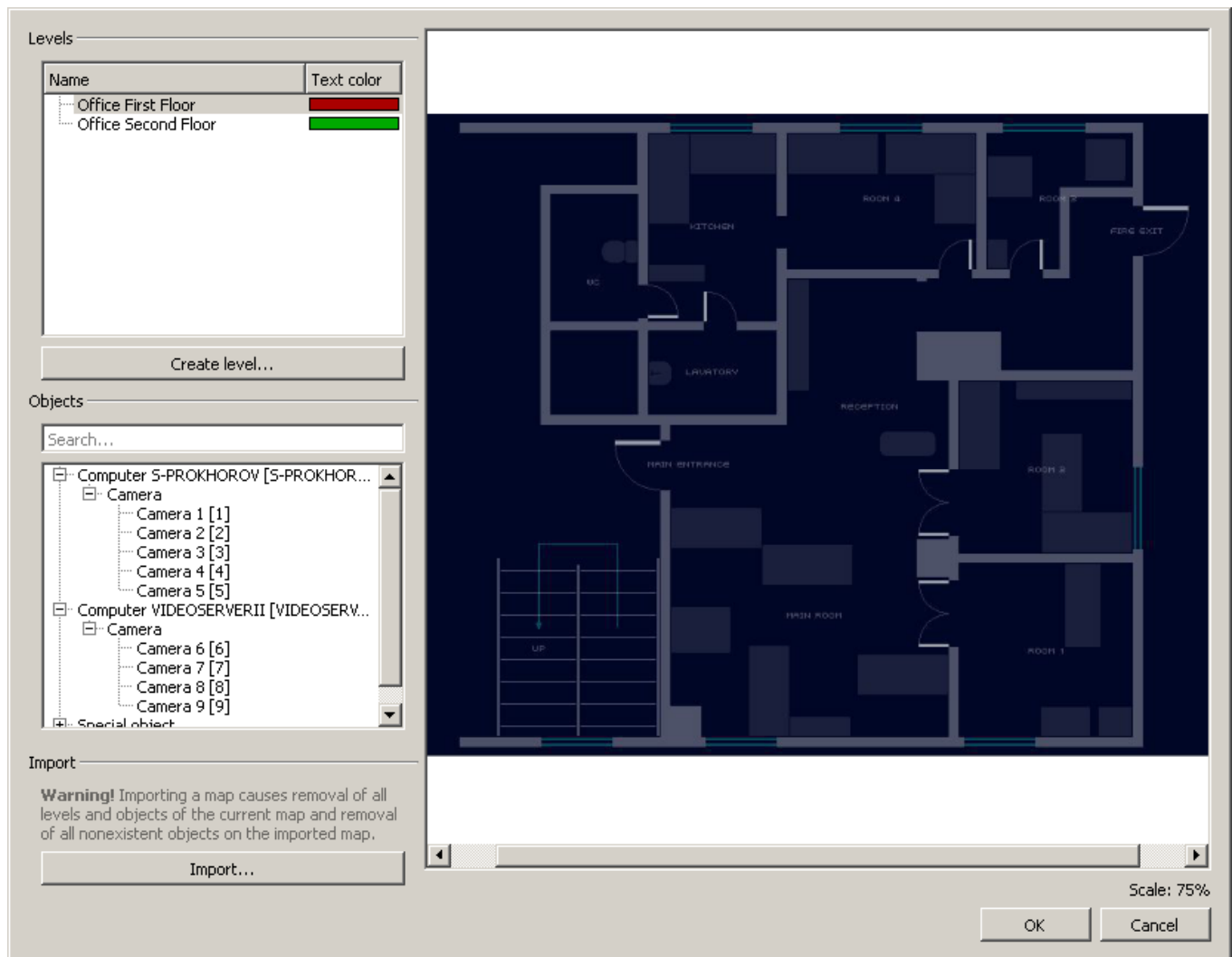


Figure 92. Map object settings window

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.
Objects	
Search	Is used to search for objects (see Working with Map Objects).
Object Tree	This box displays an SecurOS <i>Object tree</i> , that contains all system objects, 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 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.
OK (Cancel)	Save specified values and close object settings window (Close object settings window without saving changes).

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 level** button in the object settings window. The level settings window will appear (see Figure 93).

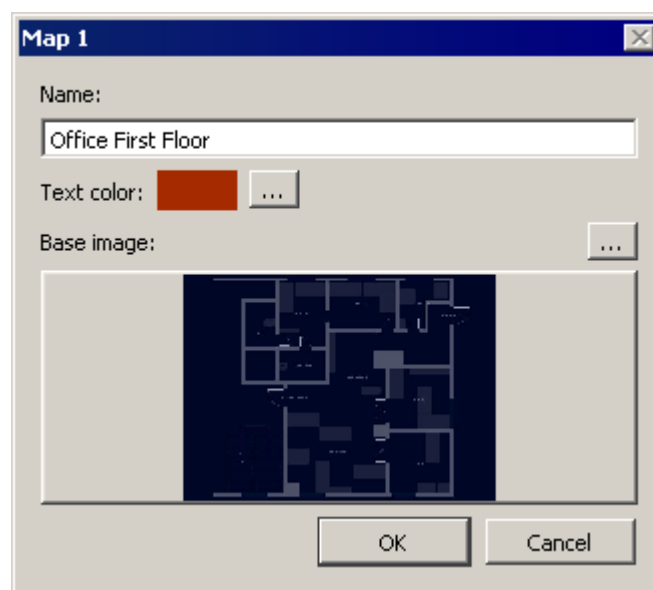


Figure 93. Levels settings window

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 94).

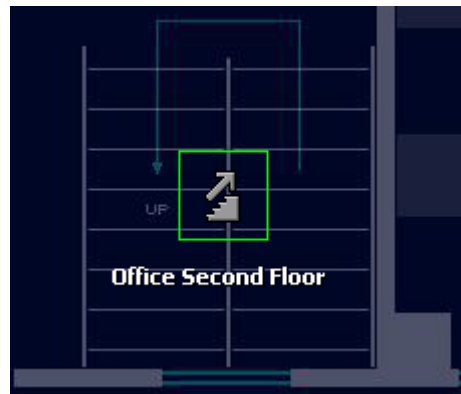


Figure 94. Map object link icon

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 94). 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 95):

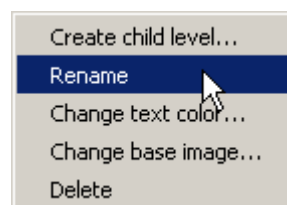


Figure 95. Map level context menu

- **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 96).

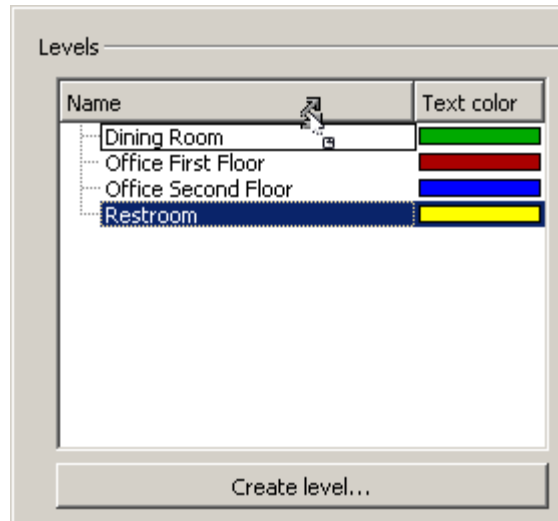


Figure 96. Creating child level by drag-and-drop

6.1.2.4 Working with Map Objects

To place an object on a map, select the object in the **Name** list (*Level Tree*) in the *Map* object settings window, then drag-and-drop object to the required location on the map.

To move the icon around,, click on the icon in the *Map* and, holding the left mouse button, move the mouse pointer to the new location.

To rotate a Camera icon:

1. Click on icon to select object.
2. Move the mouse pointer to the double-sided arrow on the right side of the icon (see Figure 97).

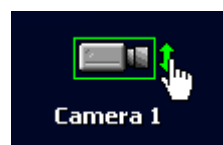


Figure 97. Rotating object on Map

3. Dragging the left mouse button rotate the icon.

To delete an object from the map, click on icon to select object, then press **Delete** key. Also one can use **Remove** context menu command to delete an object.

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

6.1.3 Map Window

This object provides a GUI to display a **Map**.

Parent object – **Desktop**.

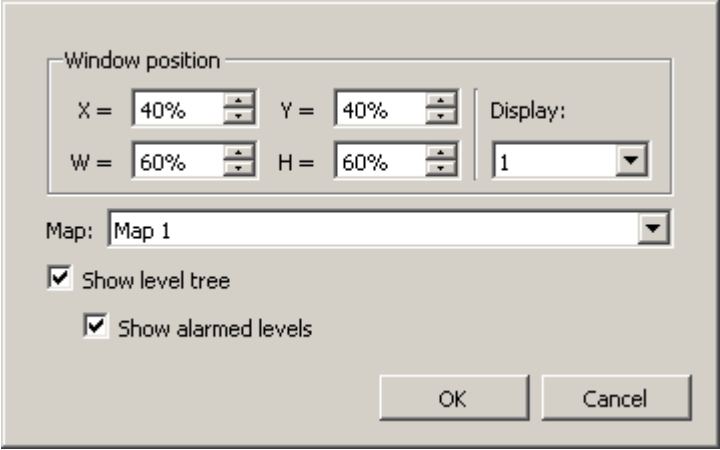


Figure 98. Map Window object settings window

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.
Show level tree	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. By default it is selected. 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).
Show alarmed levels	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. Note. A level is considered alarmed if at least one of the objects placed on this level is alarmed. By default it is selected. Unavailable if Show level tree is not checked.
OK (Cancel)	Save (Discard changes).

6.1.4 Event Viewer

Object represents a visual log of the events that occur within the entire system.

Parent object – Desktop.

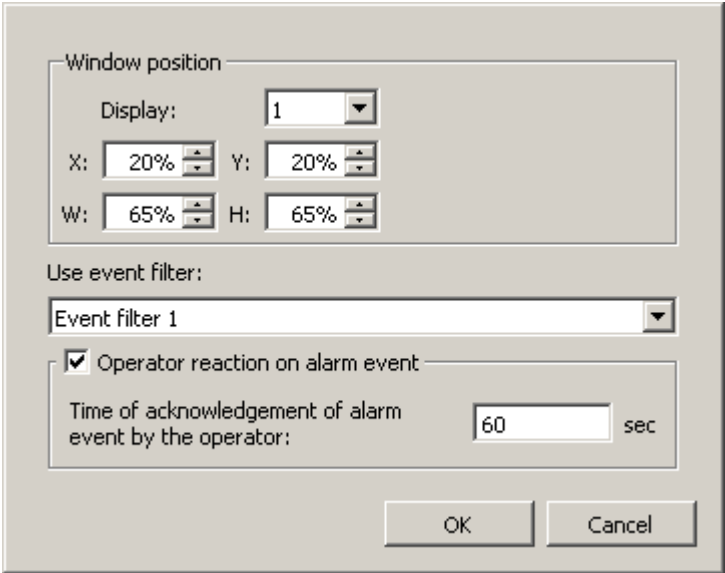


Figure 99. Event Viewer object settings window

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 not set all system events will be displayed. If set, only events allowed by selected filter (see Event Filter section) will be displayed.
Operator reaction on alarm event	Check this option to enable operator reaction on alarm events.
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.

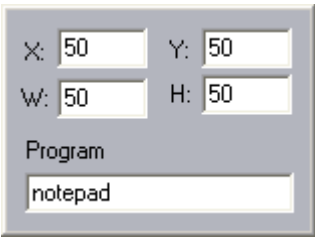


Figure 100. External Window object settings window

Table 20. External 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. Window size may not be set for all applications when they are called by an external program.
Program	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.

6.1.6 HTML Form

Use this object to define HTML forms permanently displayed on the screen of a parent desktop object.

Object is intended for integration of any custom user interface created by means of HTML forms. SecurOS includes a number of HTML forms ready to use, most often to display custom PTZ control panels on a desktop (see [SecurOS User Guide](#)). Object is displayed while screen is active or until SecurOS system shutdown.

Otherwise, a new HTML form can be also programmed for specific means (see [SecurOS Programming Guide](#)).

Note. All system HTML forms are in the \dialogscript subfolder of the SecurOS folder.

Parent object – [Desktop](#).

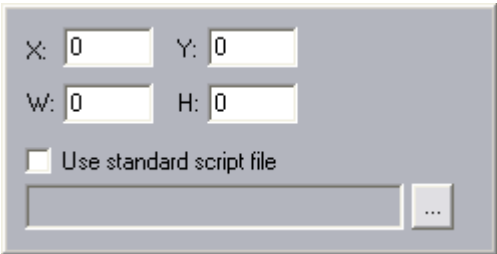


Figure 101. HTML Form object settings window

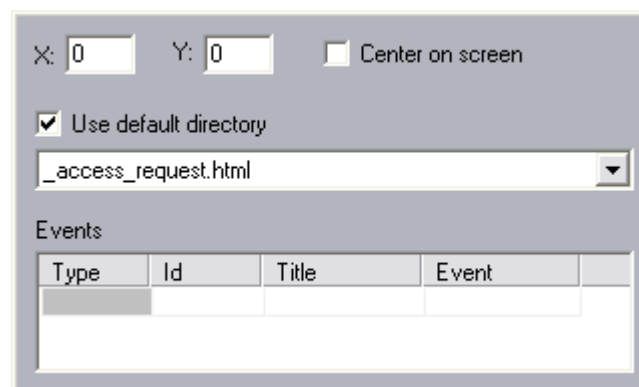
Table 21. HTML Form object settings

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.
Use standard script file	Enable this option to select a target HTML form file from the drop-down list of files located in the \dialogscript subdirectory of the SecurOS program folder (if this option is not active, you can select HTML files from any folder by using the [...] button that invokes the standard Open dialog.). Note. To display a PTZ camera control HTML form, select the file with the name corresponding to the PTZ protocol of that camera.

6.1.7 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 SecurOS script when processing events. Objects of this type can be closed manually or automatically by the system (and also by scripts).

Parent object – **Computer**.

**Figure 102.** HTML Dialog object settings window**Table 22.** HTML Dialog object settings

Parameter	Description
X, Y	Specify coordinates of the window's top left corner on the screen in percent, relative to the desktop top left corner.
Center on screen	Enable this option to attach dialog position to the center of the desktop.

Parameter	Description
Use default directory	Enable this option to select a target HTML dialog file from the drop-down list of files located in the \dialogscript subdirectory of the SecurOS program folder (if you uncheck this option, you can select HTML files from any folder by using the [...] button that invokes the standard Open File dialog). Note. [...] button is displayed only when object is configured on the local computer. For a remote computer, including the remote Operator Workstation, this button is not displayed.
Events	Deprecated, do not use.

7 Video Subsystem

The video subsystem is used to operate and configure the video devices (video capture cards, IP and analog cameras, PTZ devices) within the SecurOS network. In addition, it is responsible for transmitting video streams between servers, concentrators, 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 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.

The introduction of video hardware acceleration technology can be attributed to the time when the first models of discrete graphics cards entered the market. However, completely CPU independent hardware decompression of the H.264 video stream at all stages of the process became available only recently.

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) and above (based on the GT3e cores) graphics adapters.

All listed graphics adapters use Intel Quick Sync Video 2.0 technology.

All above listed graphics adapters are integrated with the Intel Core 3xxx and 4xxx CPUs (based on Ivy Bridge or Haswell architecture). Thus, any of the listed CPUs with integrated GPU can perform hardware decoding independently of its model (i3, i5 or i7). 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 103).

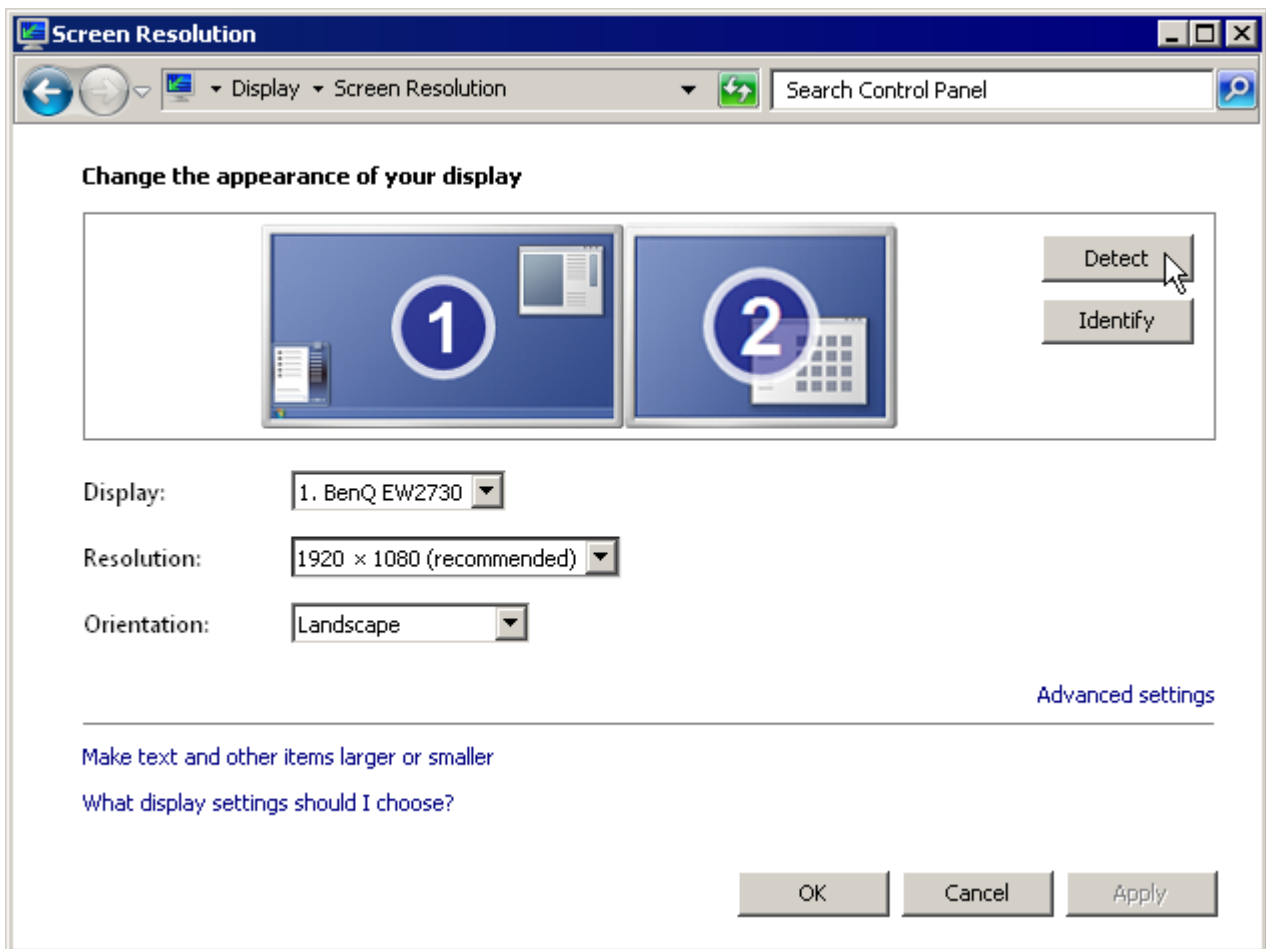


Figure 103. Detecting Intel HD Graphics adapter

- 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 104).

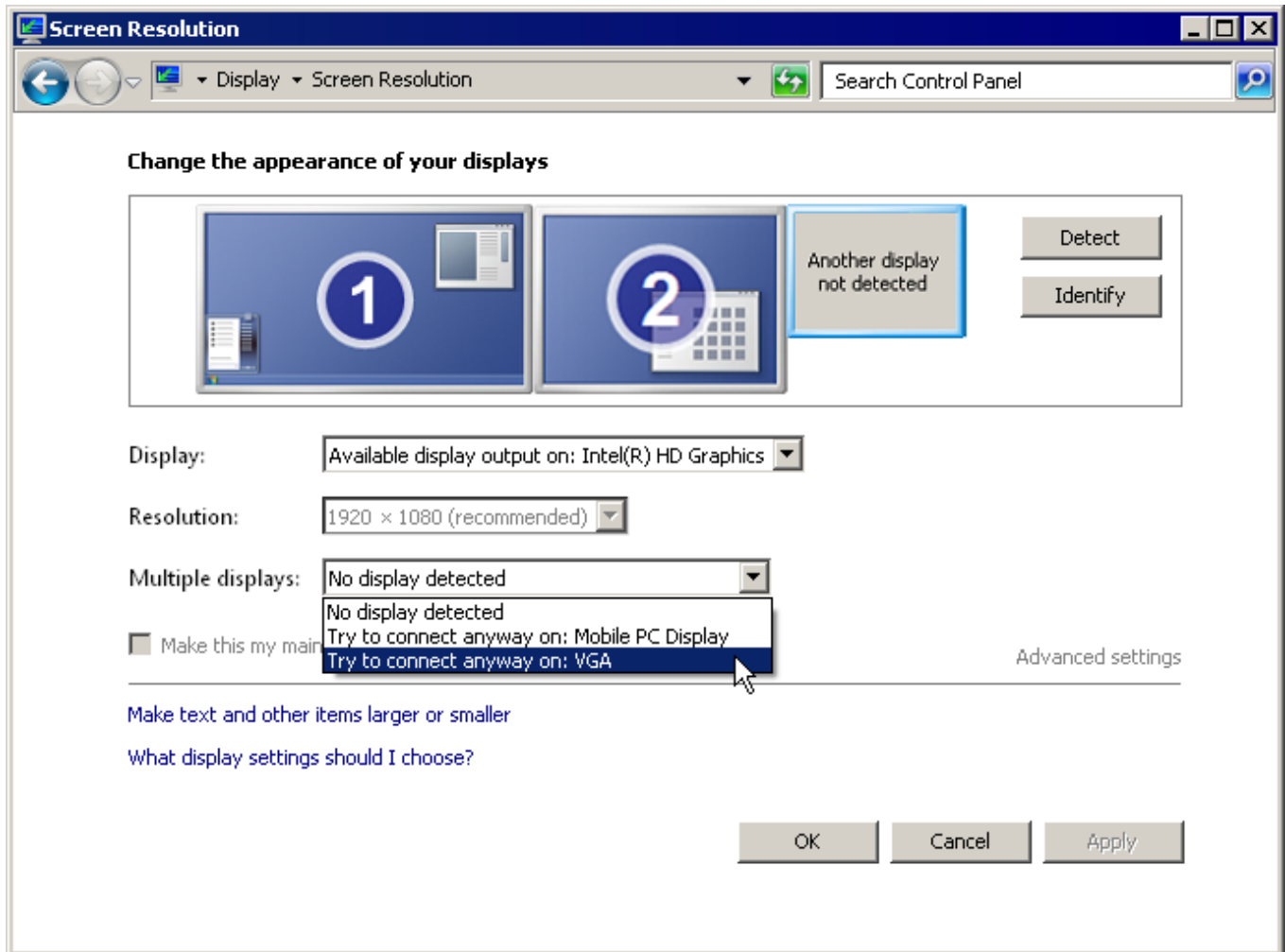


Figure 104. Choosing display to connect to

- Click dummy display to select it. From the **Multiple displays** drop-down list choose **Extend desktop to this display** (see figure 105). Click **Apply** button.

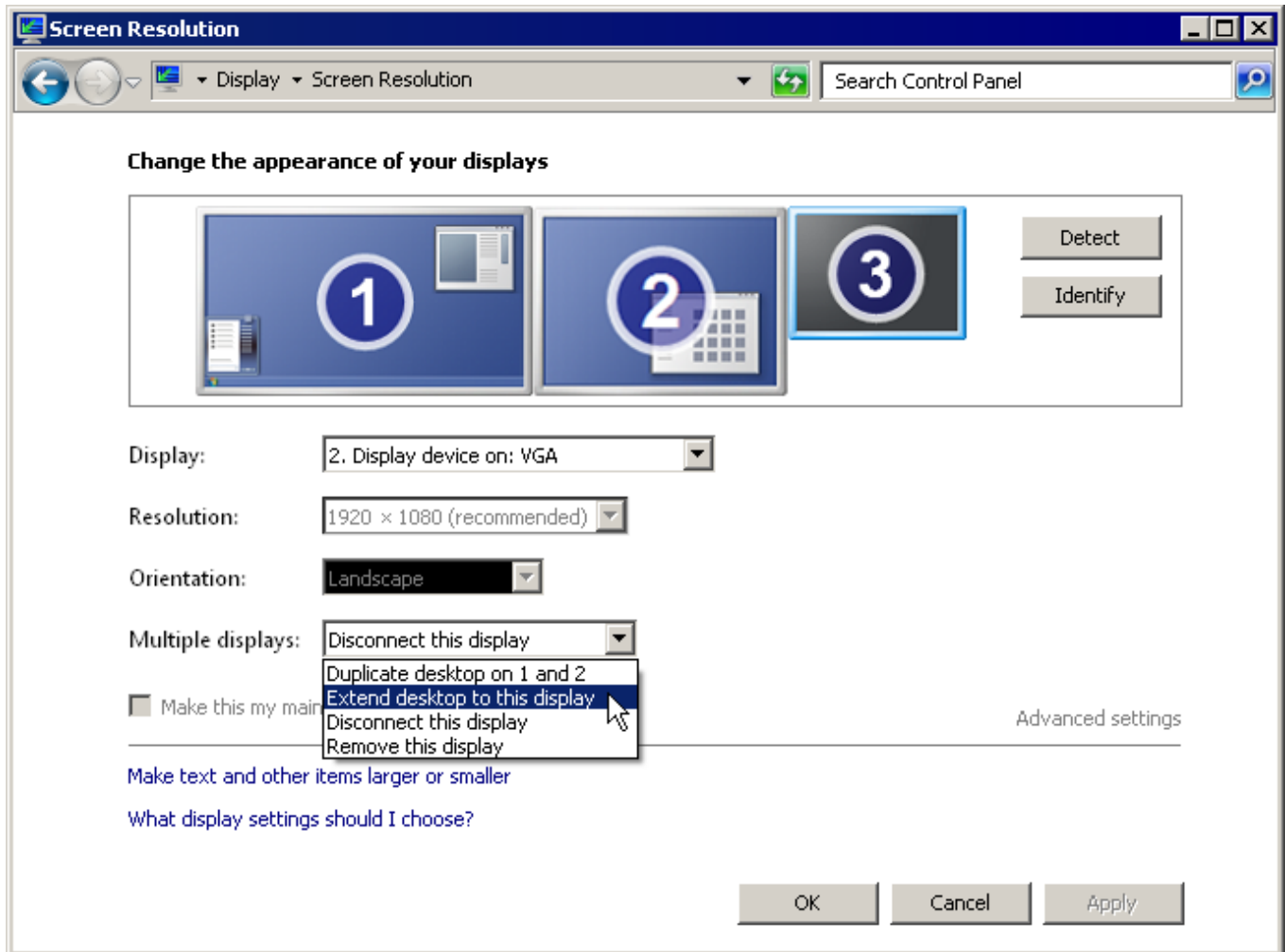


Figure 105. Expanding desktop to the selected display

Note. If single monitor, plugged in discrete adapter connector is used, choose *Extend these displays*.

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 *Monitor*, 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 *Monitor* 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 *Monitors*. For example, in one *Monitor*, 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 *Monitor*, 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 *Monitor*, *Camera* or *Zone* (**Zone settings** tab) 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 *Monitor*, *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, such as object size threshold or alarm states.

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 Managing Motion Detection Zones

This section describes basic operations with Motion Detection Zones.

7.4.1.1 Creating Zones

Separate from the *Main* zone, you can create additional *Zones* for each secured area within the camera view.

7.4.1.2 Showing Zones



Figure 106. Camera cell with alarmed zone

To show all zones for a camera:

1. Right-click the **Armed** button of the desired camera cell.
2. Choose the **Always show zones** menu item. The zones, where motion has been detected, will be highlighted in red (see [figure 106](#)).

7.5 Special Settings for Video Subsystem Components

This section describes specifics of the video subsystem objects configuration procedure.

7.5.1 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 User Guide](#)). Assuming that a *Video Capture Device* and a *Camera* object have been created, an administrator has to create a *Desktop* and a *Monitor* in order for the camera frame to appear.

7.5.2 Video Monitor Settings

On activation of a camera cell and when using its archive mode on a video monitor, some control elements appear (see [SecurOS User Guide](#)). They are hidden after some period of inactivity.

When a mouse is placed over the inactive camera cell, the control buttons will re-appear on the cell. The control buttons may be deactivated for every cell of a certain monitor.

To disable the control buttons for a certain monitor, perform the following steps on the computer with the monitor:

1. Shutdown SecurOS.
2. Launch the system utility for registry editing (type `regedit` in **Start** → **Run** box and click **OK**).
3. Create a new branch: `\HKLM\SOFTWARE\ISS\SecurOS\iss-video-gui\strings`.

Note. When operating on 64-bit OS create the `\HKLM\SOFTWARE\Wow6432Node\ISS\SecurOS\iss-video-gui\strings` branch.

4. Create `lo-<nnn>-auto_deactivation_interval` parameter in the new branch, where the identifier of the corresponding *Monitor* object must be substituted for `<nnn>`. Specify for the new parameter a value of time for control buttons deactivation in milliseconds (default value is 10000).
5. Close the **regedit** utility.
6. Launch SecurOS again.

7.5.3 Record Buffer Settings

If using a low speed network (see requirements in [SecurOS Installation Guide](#)) it is recommended to configure the record buffer size by setting its parameters.

To set the record buffer parameters, perform the following steps on the computer recording the video archive:

1. Shutdown SecurOS.
2. Launch the system utility for registry editing (type `regedit` in **Start** → **Run** box and click **OK**).
3. Open the `\HKLM\SOFTWARE\ISS\SecurOS\NISS400\Video` branch, and create the `mpayer_queue_min` parameter and set it to the minimal number of video frames in the buffer (default value is 40).

Note. When operating on 64-bit OS open the `\HKLM\SOFTWARE\Wow6432Node\ISS\SecurOS\NISS400\Video` branch.

4. In the same branch create the `mplayer_queue_max` parameter and set it to the maximal number of video frames in the buffer (default value is 70).
5. Close the **regedit** utility.
6. Launch SecurOS again.

7.5.4 Archive Recording

This section describes specifics of the archive recording operation and its configuration.

7.5.4.1 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 (operative video archive), one should previously allocate mandatory free disk space.

To set up a recording buffer, perform the following steps on the computer storing the video archive:

1. Shutdown SecurOS.
2. Launch the system utility for registry editing (type `regedit` in **Start** → **Run** box and click **OK**).
3. Open the `\HKLM\SOFTWARE\ISS\SecurOS\NISS400\Video` folder. Create a `FreeMb` key there and define mandatory free disk space (in MB) for archive recording as its value. Now the video archive will be recorded on the defined disk until its free space reaches the `FreeMb` value.

Notes:

1. When operating on 64-bit OS open the `\HKLM\SOFTWARE\Wow6432Node\ISS\SecurOS\NISS400\Video` branch.
 2. The same `FreeMb` parameter determines free space threshold for audio archive records.
-

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! The `FreeMb` parameter is also used for long-term video archive (associated with the Archiver module). Define this parameter within the `\HKLM\SOFTWARE\ISS\SecurOS\NISS400\Archiver` registry key on the computer keeping long-term video archive. When operating on 64-bit OS create the parameter in the `\HKLM\SOFTWARE\Wow6432Node\ISS\SecurOS\NISS400\Archive` branch.

4. Close the **regedit** utility.
5. Launch SecurOS again.

7.5.4.2 Video Recording Settings

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 operative video archive disks:

1. Shutdown SecurOS.
2. Launch the system utility for registry editing (type `regedit` in **Start** → **Run** box and click **OK**).
3. Open the `\HKLM\SOFTWARE\ISS\SecurOS\NISS400\Video` folder. Create a `MaxFrames` key and define the maximum number of frames for any new video record file.

Note. When operating on 64-bit OS open the `\HKLM\SOFTWARE\Wow6432Node\ISS\SecurOS\NISS400\Video` branch.

4. Close the **regedit** utility.
5. Launch SecurOS again.

When recording video, the video frames queue may cause a computer RAM overflow. By default, the RAM allocated of video recording is — 100 MB. This value can be changed by the `MaxMemMb` parameter in the following registry folder: `\HKLM\SOFTWARE\ISS\SecurOS\NISS400\Video\FS`.

Note. When operating on 64-bit OS open the `\HKLM\SOFTWARE\Wow6432Node\ISS\SecurOS\NISS400\Video\FS` branch.

Warning! 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.

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.".

7.5.4.3 Long-term Archive Settings And Archive Converter

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

A system administrator can configure the duplication of the locally recorded video from certain cameras to a long-term video archive (e.g. NAS, SAN) in SecurOS format on any available disk by the help of the *Archiver* module (see [Archiver](#)).

If the free space threshold is reached (`FreeMb` system registry parameter, see [Disk Volume Settings](#) section) 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).

Note. A system administrator can configure video archive conversion from SecurOS format to AVI or ASF formats from certain cameras with the help of the *Archive Converter* module (see [Archive Converter](#)). During this process, files are stored in a temporary file folder and are converted then.

7.6 Export Video Using Monitor

The *Monitor*'s standard tools allow to export video recordings labeled with specific markers. These markers are *Alarms* and *Bookmarks*.

- *Alarm* — sign of detected motion in motion detection zone.
- *Bookmark* — manually set time stamp relevant to the position (or the segment) of the recorded video which attracts operator's attention or may be of interest for further analysis and so on.

Video and relevant markers are stored separately — video is saved to a folder in a dedicated hard drive / partition, while *Alarms* and *Bookmarks* are saved into the database.

Additional Information

- *Operative archive* — rewritable archive. Once the max archive size is reached the oldest data will be overwritten with the newest. By default it is stored in a VIDEO folder on the disk, selected in the *Computer* object settings.
- *Long-term archive* — permanent data storage, produced by conversion of *Operative archive* with the help of the *Archiver Dialog* module. By default long-term archive is stored in the \Archive\VIDEO folder on the disk, selected in the *Archiver* object settings. For a detailed description of the Long-term archive creation procedure see the SecurOS User Guide.

Video recordings relevant to the *Alarms* and *Bookmarks* stored in the database can be exported from *Operative* and *Long-term* archives. Export is available only if the **Archive Converter** object (with all necessary parameters configured) was already created in the Object Tree. This **Archive Converter** must be selected in the **Monitor** object settings (**Export engine** parameter).

Because the video and relevant markers are stored separately the following algorithm is used when exporting the data:

1. If the video recordings relevant to the given time period and camera are stored both in the *Operative* and the *Long-term* archives, then only files stored in *Operative* archive will be exported.
2. If some video recordings relevant to the given time period and camera are missing in the *Operative* archive, but are present in the *Long-term* archive, the recordings of the *Operative* archive will be exported first, then recordings of the *Long-term* archive will be exported.

Notes:

1. In this case two independent export tasks are created - one for the *Operative* archive, which is executed first and the second for the *Long-term* archive.
 2. If the *Operative* archive conversion procedure failed or export task was canceled by an operator then the *Long-term* export task will not be executed.
 3. By default, recordings are exported to the \Exported Fragments folder of the software root directory.
 4. Names of the files produced by the *Long-term* archive conversion have long_term file type extension prefixes. For example, 1 (2012-04-17 13'23'35 - 2012-04-17 13'23'36).long_term.asf.
-

3. If the *Operative* archive does not contain recordings relevant to the given time period and camera, then the *Long-term* recordings will be exported.

To start the export press the  (**Export entries**) button from the **DVR Search Panel** of the *Monitor* (see **SecurOS User Guide**).

7.7 Object Reference

The video subsystem includes the following object classes:

- **System Objects.**
- **User Interface Objects.**

7.7.1 System Objects

The following are the System objects:

- **Video Capture Device.**
- **Camera.**
- **Defocus detector.**
- **Layout.**
- **Zone.**
- **Light Detector.**
- **PTZ Controller.**
- **PTZ Device.**
- **Archive Converter.**
- **Archiver.**
- **Image Processor.**
- **RTSP Server.**
- **EdgeStorage Sync.**

7.7.1.1 Video Capture Device

This object represents an IP device (camera, encoder, etc..) connected to a TCP/IP network, or it can also represent a TVISS video capture card installed in a server (or a single chip on a TVISS video capture card in the case of the older models).

Example. In the case of video capture cards, calculate the total number of chips on all video capture cards and create N objects with N unique **PCI channel** parameters. For example, TVISS-4MX1 board has one video capture chip and should be represented as a single *Video Capture Device* object. TVISS-16MX4 cards have two independent video capture chips onboard and should be represented within the system as two *Video Capture Device* objects. There is no correspondence between the chips and the *Video Capture Device* objects.

Note. It is recommended to always start **PCI channel** parameters number from 00 and avoid gaps in numbering. For example, if there is one TVISS-16MX4 card and two TVISS-4MX1 cards on the computer, create four *Video Capture Device* objects and set their **PCI channel** parameters to 00, 01, 02 and 03, respectively.

Warning! This object and its children objects are accessible only when the Video Server **Computer's role** is selected in the parent *Computer* object settings (see **Computer**).

Parent object — **Computer**.

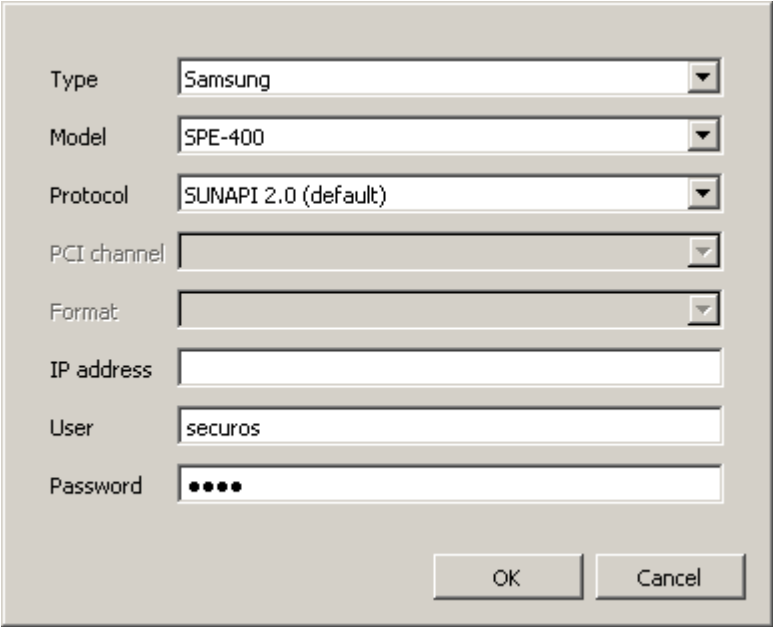


Figure 107. Video Capture Device object settings window

Table 23. Video Capture Device object settings

Parameter	Description
Type	If you are connecting an analog camera — select TVISS-RT/MX (depending on the TVISS card installed), If connecting an IP-device — select the value corresponding to the brand of the device.
	Functionality to support analog cameras is available in the following editions: <i>SecurOS Enterprise, SecurOS Premium, SecurOS Professional, SecurOS Xpress.</i>
	To identify <i>Video Servers</i> of a remote system within the <i>Monitoring Center</i> , working with remote archives (see Remote system), 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 local archives (see Remote system), 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, that uses specially prepared video clips as a video source. This option can be used to test or demo the system without real cameras installed.
Model	If enabled, select the model of the <i>Video Capture Device</i> for the given Type.

Parameter	Description
Protocol	Select version of data transmission protocol used by camera that is being connected. 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.
PCI channel	If the TVISS-RT/MX or Virtual values are 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.
IP address	Specify the IP address or DNS/WINS name of the video device in the TCP/IP network for all device Types excluding TVISS-RT/MX and Virtual. Note. Never use IP address if the device uses DHCP (dynamic IPs); use symbolic DNS name of the device instead!
User	Specify a user name for the IP device connection. Default value is <code>securos</code> .
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).

7.7.1.1.1 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 a *Video Capture Device* child object.
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. Add created *Camera* on the *Monitor* or *Media Client* of the given *Computer*.

7.7.1.2 Camera

This object represents a single video stream from an IP device or from an analog camera connected to an ISS TVISS video capture board.

Parent object – **Video Capture Device**.

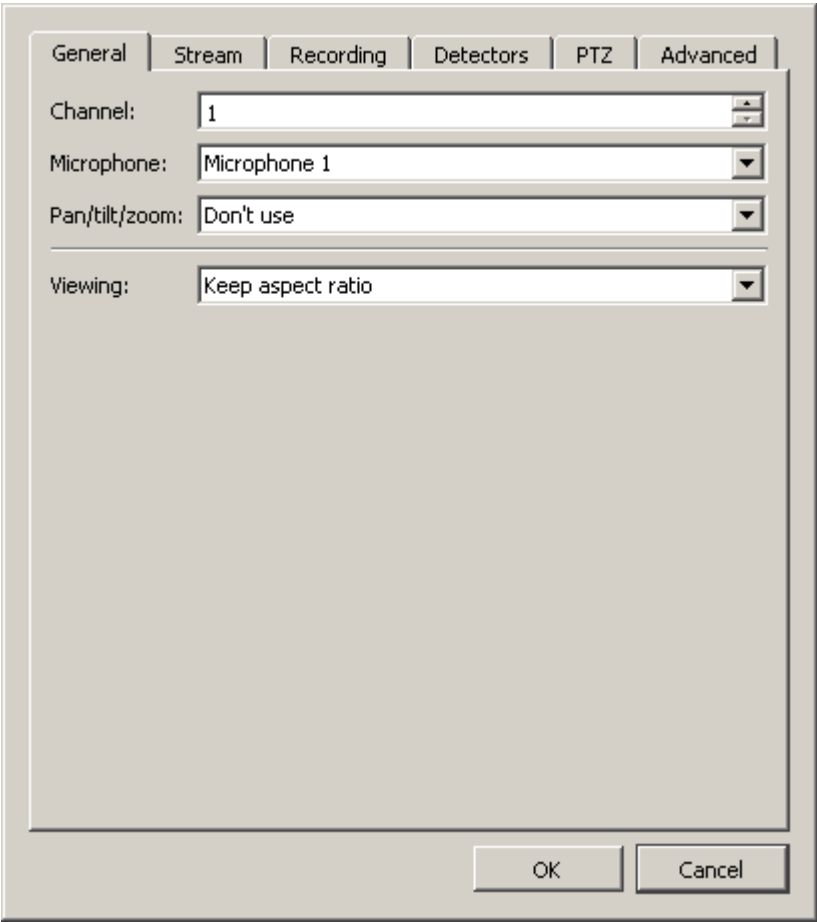


Figure 108. Camera object settings window. General Tab

Warning!

- 1. The *Camera* object includes general (required for each *Camera*), and specific parameters.
- 2. Set the specific parameters of the *Camera* object according to the **Type** and **Model** of the parent *Video Capture Device* object.
- 3. In the settings below, only the more important (most commonly used) parameters are described.

Additional Information

The settings that are in the form of a checkbox are optional. Some of these parameters can also be set externally (especially for IP devices), i.e. through the web-config of the camera. Enabling the checkbox of an optional parameter overwrites the default value (or value from the camera web-config). If you need to change the current value of a optional parameter after deactivating it from the object settings window, the camera web-config must be used.

Table 24. Camera object settings. General Tab

Parameter	Description
Channel	Select the camera's channel number from the list.

Parameter	Description
Microphone	Select a <i>Microphone</i> object to record audio and video synchronously. This will allow you to playback synchronized video and audio from an operator interface when choosing an appropriate camera from the <i>Monitor</i> camera list.
Pan/Tilt/Zoom	To enable an IP device's native telemetry control, select the <code>Use</code> value from the drop-down list in the box or, for analog cameras, select a previously created additional <code>PTZ device</code> object (see Setting up telemetry section). By default the <code>Don't Use</code> option is selected. Note. PTZ control panel becomes active when operator selects this camera on a video monitor.
Viewing	This parameter defines the video image display format in the <i>Camera</i> cell for all <i>Monitors</i> throughout the SecurOS security system. At the same time, for each <i>Monitor</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: • <code>Keep aspect ratio</code> — original format of the video frame will be used when displaying video. Is the default value; • <code>Stretch to cell</code> — the frame is stretched to full size of the <i>Monitor's</i> cell; Exception. If the Layouts type parameter of the <i>Monitor</i> is set to <code>special</code>, and the <code>1*1</code> layout is selected (<i>Camera</i> cell takes all <i>Monitor</i> working area) then the image will be displayed as <code>4:3</code>, even if the Viewing parameter is set to <code>Stretch to cell</code>. • <code>Force 4:3</code> — when displaying, video will be scaled to <code>4:3</code>.
OK (Cancel)	Saving specified values and closing object settings window (Closing object settings window without changes).

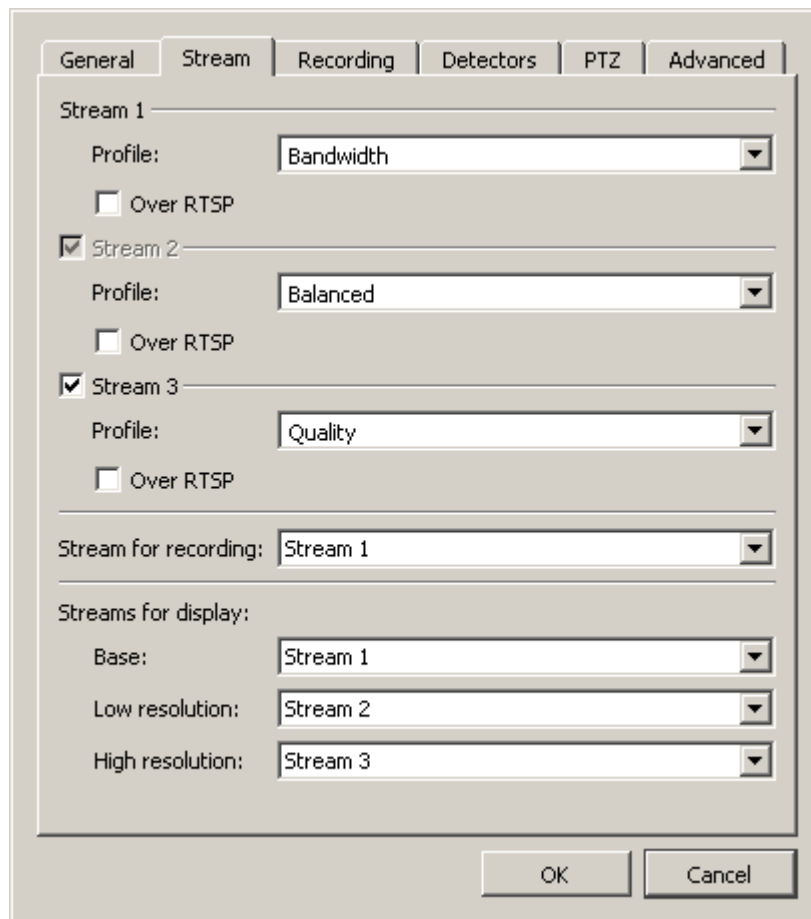


Figure 109. Camera object settings window. Stream Tab

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*. Single stream of such *Camera* will be used both for displaying and recording.

Table 25. Camera object settings. Stream Tab

Parameter	Description
Stream 1	
Profile	From the drop-down list select a predefined camera profile, which settings will be applied to the transmitted video stream.
Over RTSP	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.
Stream 2 (Stream 2 configuration mode and use activation)	
Profile	From the drop-down list select a predefined camera profile, which settings will be applied to the transmitted video stream.
Over RTSP	Select checkbox, if camera operates in a high-load network, network has low capacity, or within network where RTP packets are filtered. Video will be transmitted using the TCP protocol.

Parameter	Description
Stream 3 (Stream 3 configuration mode and use activation). Enabled only if Stream 2 is selected.	
Profile	From the drop-down list select a predefined camera profile, which settings will be applied to the transmitted video stream.
Over RTSP	Select checkbox, if camera operates in a high-load network, network has low capacity, or within network where RTP packets are filtered. Video will be transmitted using the TCP protocol.
Streams	
Stream for recording	Select a stream for recording from the drop-down list.
Streams for display	
Base	Select a base stream from the drop-down list.
Low resolution	Select a low resolution 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 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 *Monitor* 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 *Monitor* 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 *Monitors* 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 Face) 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.

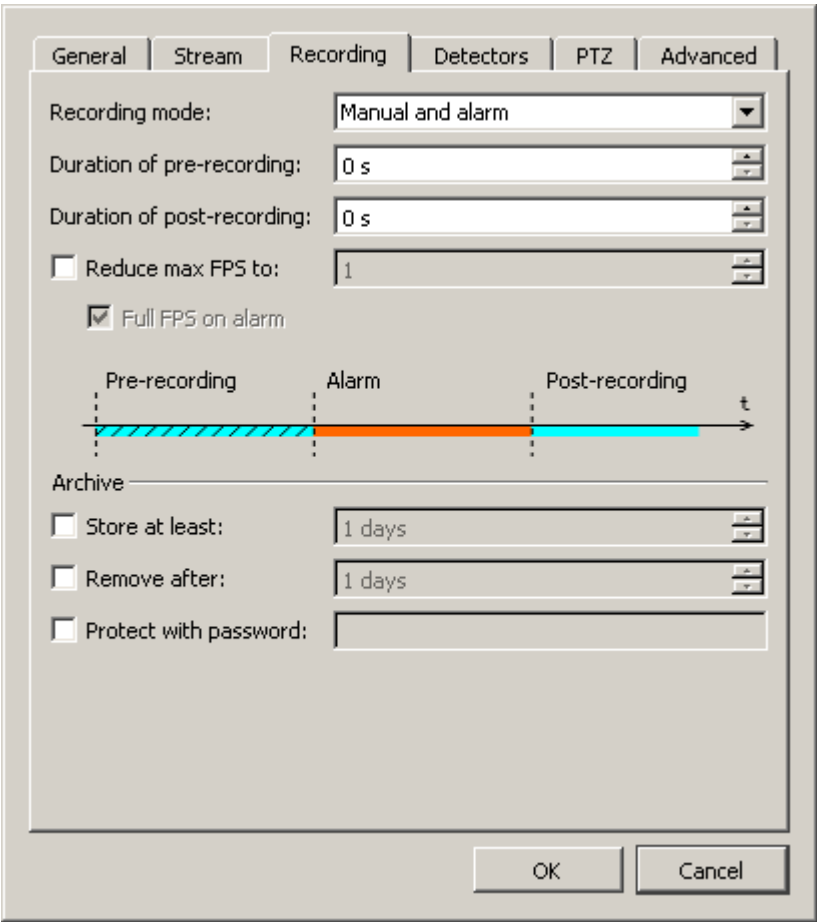


Figure 110. Camera object settings window. Recording Tab

Table 26. Camera object settings. Recording Tab

Parameter	Description
Recording mode	Select the mode from the following:
	Manual – video recording will start either by an operator's command or with the help of the Automation subsystem .
	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. Recommended for working with DVR search panel (see SecurOS User Guide).
	Continuous – video recording will be performed constantly.
	Note. In this mode, recording can be stopped only by changing the <i>Camera</i> settings.
	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>Monitor/Media Client</i> , by program or <i>Macro</i> , from <i>Map</i> etc.).

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 not set or 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 not set or 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	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.
Store at least	Specify a minimum depth of video archive, in days. Note. An hour of an archive creation is accepted as a beginning of a storage period, for example, 15:00 01.07.2015. Checking of that, if archive files should be deleted is performed at system start and, further, at the end of each hour. Archive, retention period of which has not expired, will not be deleted, even if the hard disk is not enough space, the archive recording is suspended until space is released. Range of values: [1; 9999].
Remove after	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].
Protect with password	Enable this option to protect the video archive for this camera with a password (this will apply to newly created video records; current archive will remain untouched). To view password-protected cameras from operator interface, you will need to specify the same password in camera settings within the <i>Monitor</i> object settings (see Monitor). This password will also be requested to view and convert video archives using the Media Export Utility (see ISS Media Export Utility).

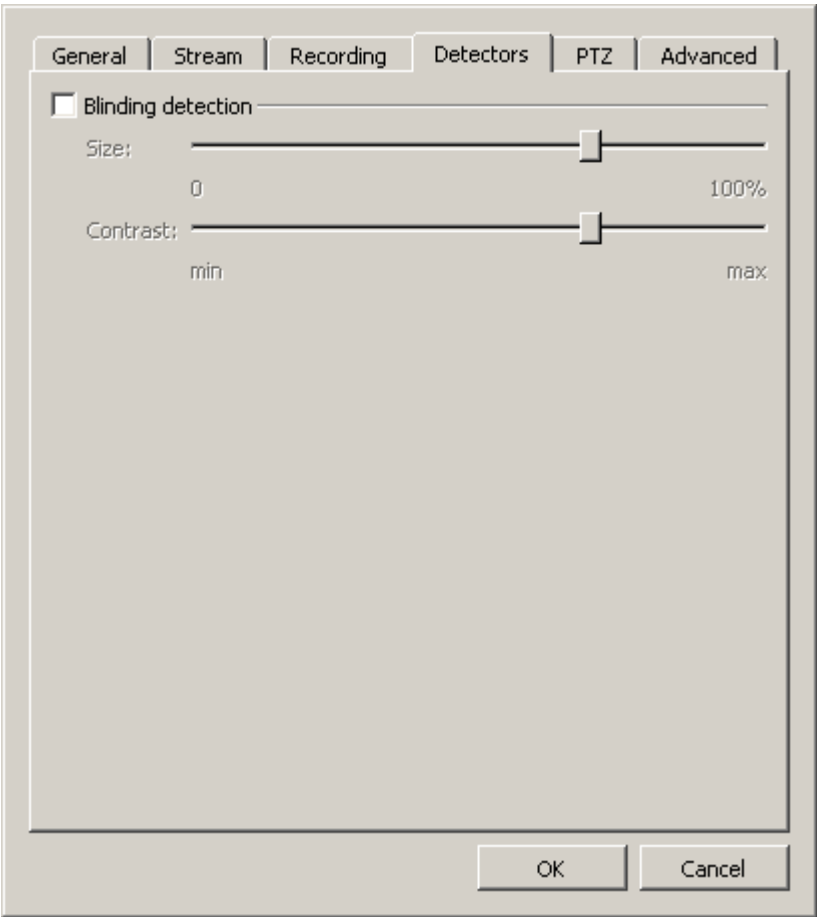


Figure 111. Camera object settings window. Detectors Tab

Table 27. 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.
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.

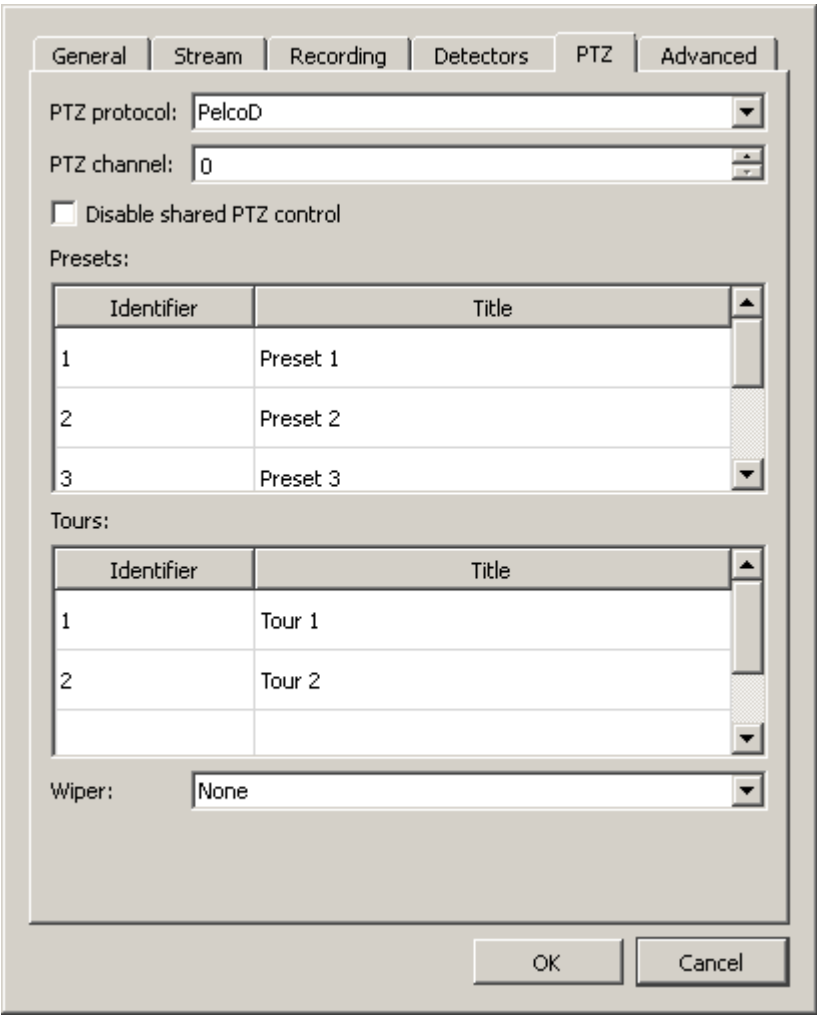


Figure 112. Camera object settings window. PTZ tab

Table 28. 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.
Disable shared PTZ control	Check this box on to activate exclusive telemetry control mode (see Exclusive Telemetry Control).
Wiper	If the <i>Camera</i> is equipped with the <i>Wiper</i> , select the object that can control it. Note. For more details see Configuring System to Work with Wiper .
Presets (table of pre-installed settings)	
Identifier	Type ID of preset specified in the PTZ device which is selected in the <i>Camera</i> object settings to control it.

Parameter	Description
Title	Specify preset title. A list of these presets will be displayed in the operator interface when working with this PTZ device.
Tours (table of tours)	
Identifier	Type ID of tour, preliminary specified in the camera settings with the help of web interface.
Title	Specify tour title. A list of specified tour titles is displayed in the <i>Media Client's</i> tour panel by activation of the given <i>Camera</i> .

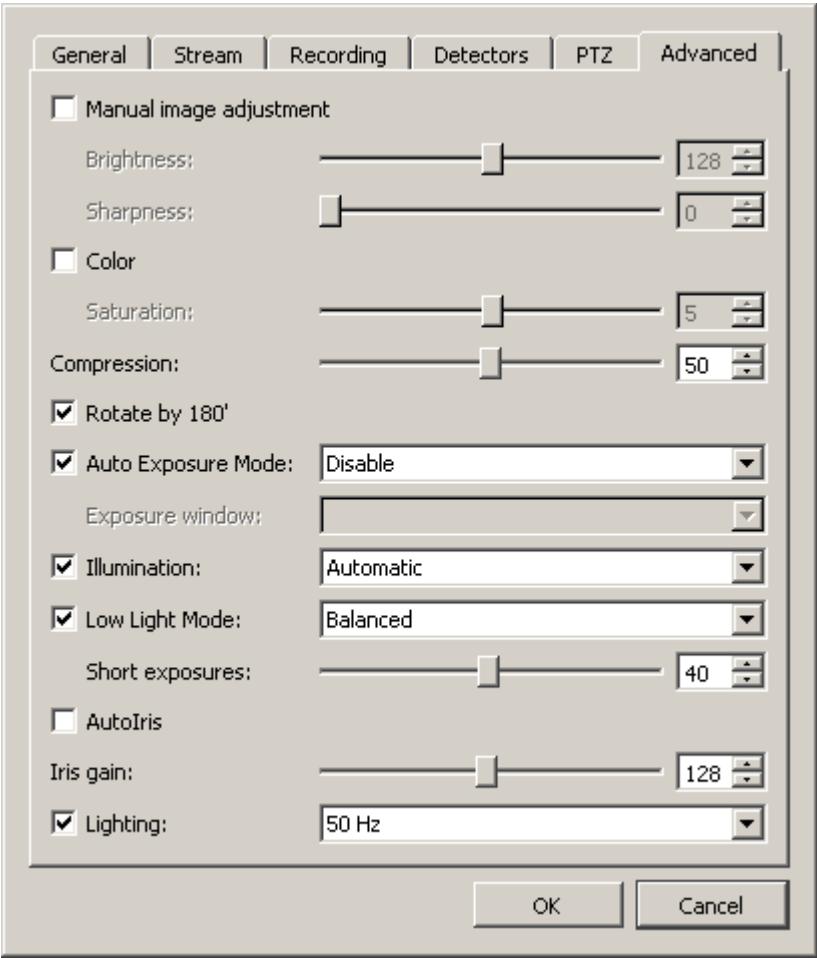


Figure 113. Camera object settings window. Advanced tab

Note. The Arecont AV2155 parameter set is presented in figure 113.

Specify additional parameters depending on the *Camera* model.

Some Axis camera models support broadcasting audio from operator's microphone to camera's built-in speaker. To use this feature select the **Speaker** checkbox in the **Advanced** (see figure 114).

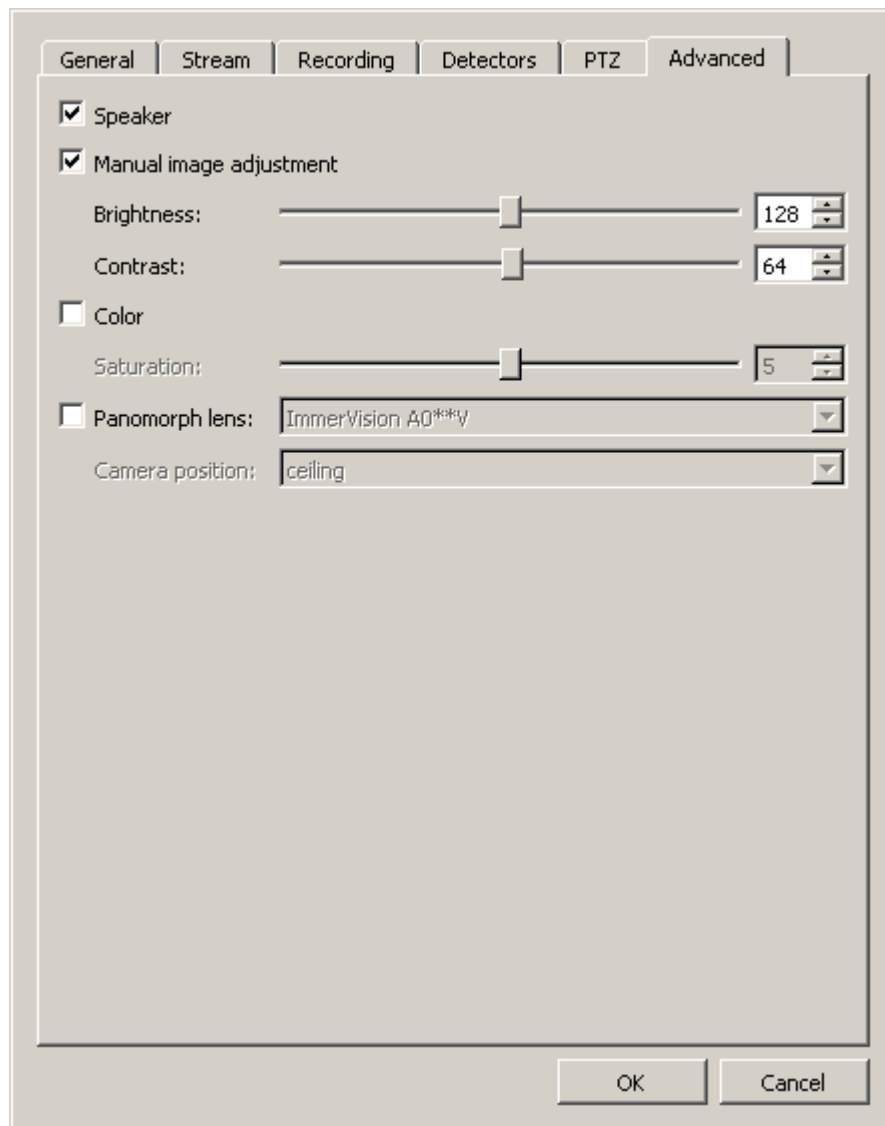


Figure 114. Advanced Tab (for the Axis camera settings example)

7.7.1.3 Defocus detector

This object is designed to specify parameters, used by the *Camera* defocus determination algorithm.

Parent object – [Camera](#).

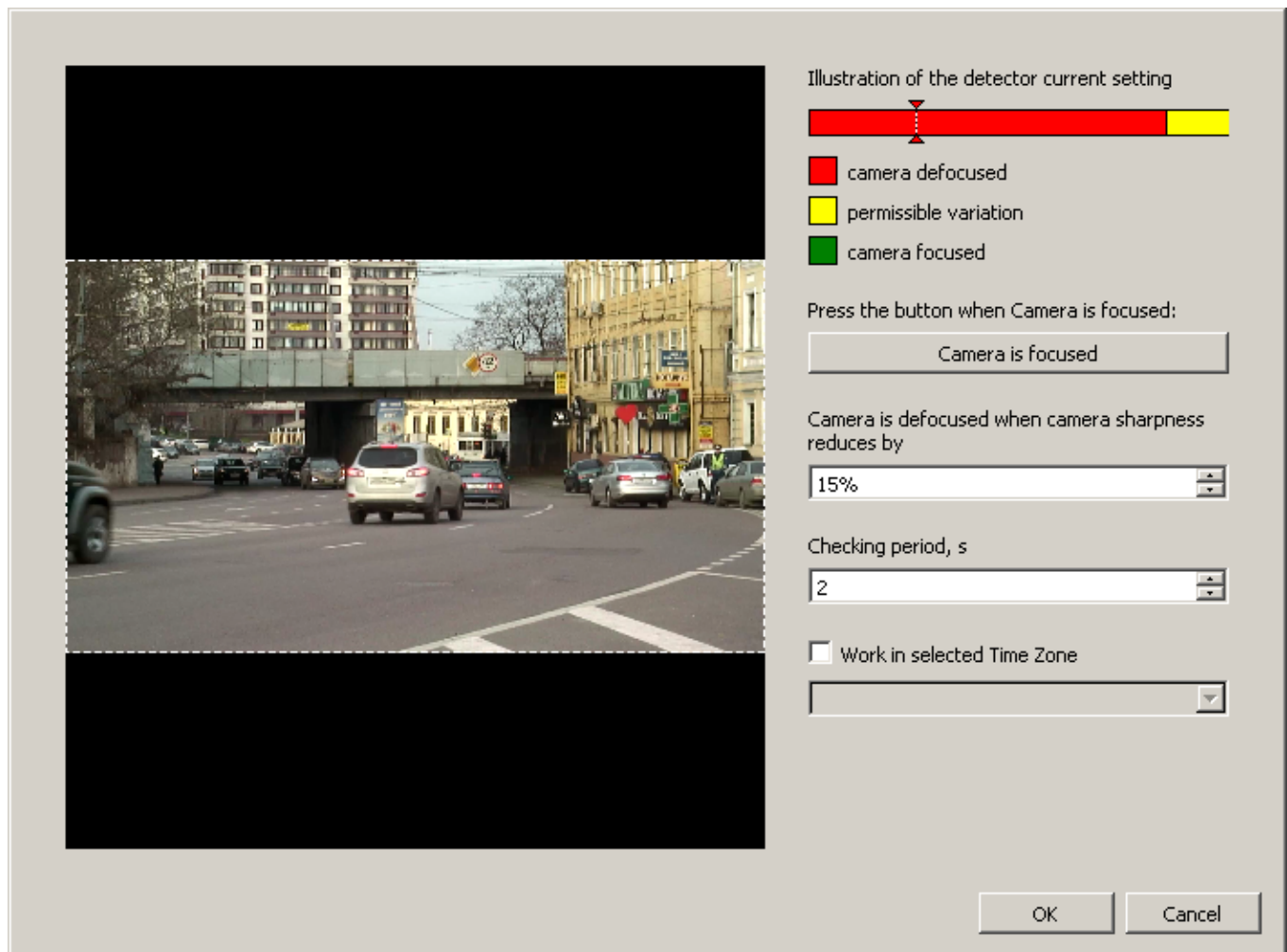


Figure 115. Defocus detector object settings window

Table 29. 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 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].
Work in selected Time Zone	Select option and specify time period to check camera defocus (see Time Zone). If option is not selected, defocus checking is always performed.

Parameter	Description
Buttons	
Camera is focused	When detection parameters are specified, click this button to store reference image.
OK (Cancel)	Save specified values and close the object settings window (Close object settings window without saving changes).

Recommendations for choosing the detection area and configuration of the other detector parameters are shown below (see [Fine Tuning Recommendations](#)).

7.7.1.3.1 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 **Time Zone** 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 [116](#)):

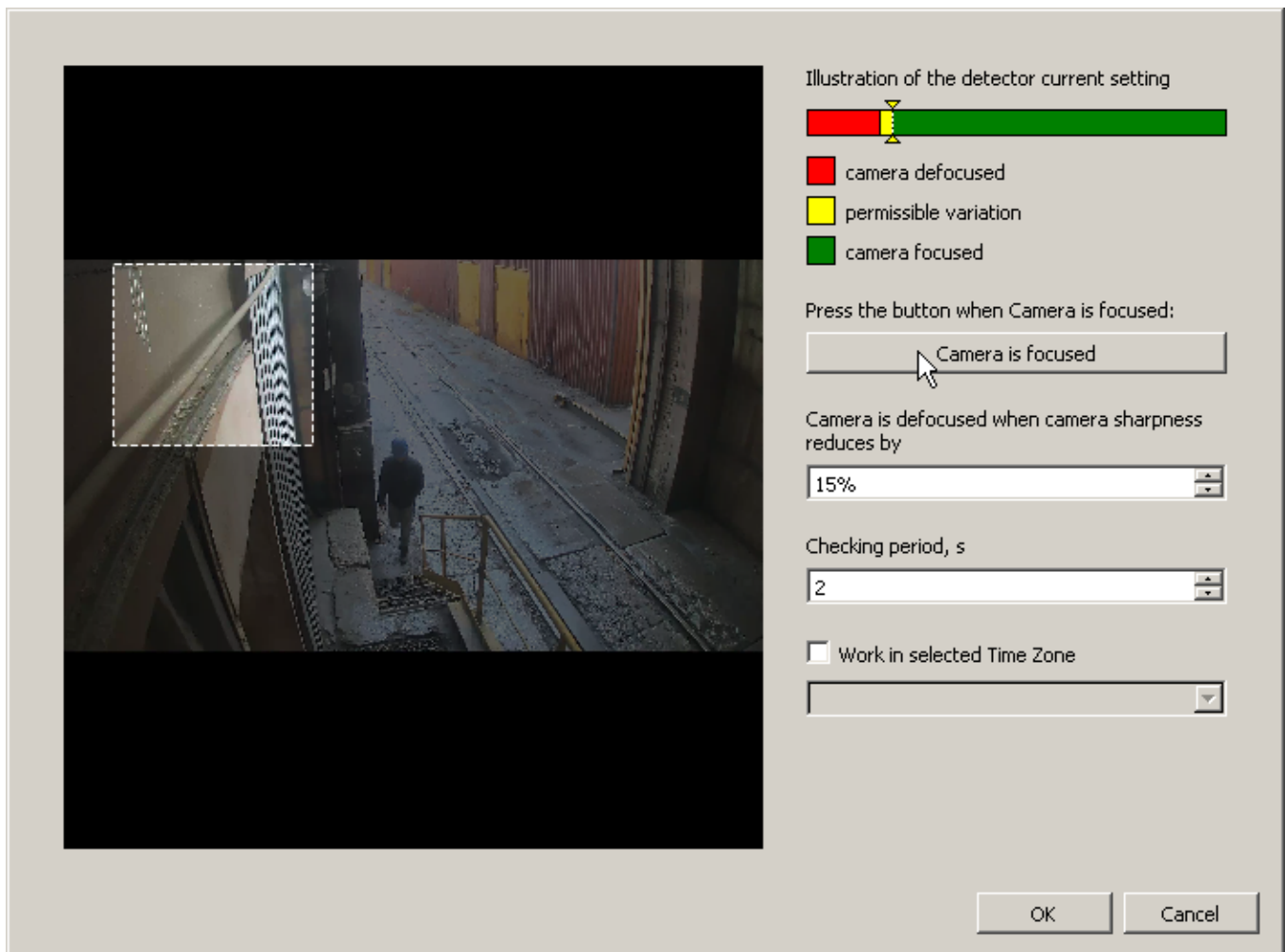


Figure 116. Adjustment of the Defocus Detector

7.7.1.4 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](#).

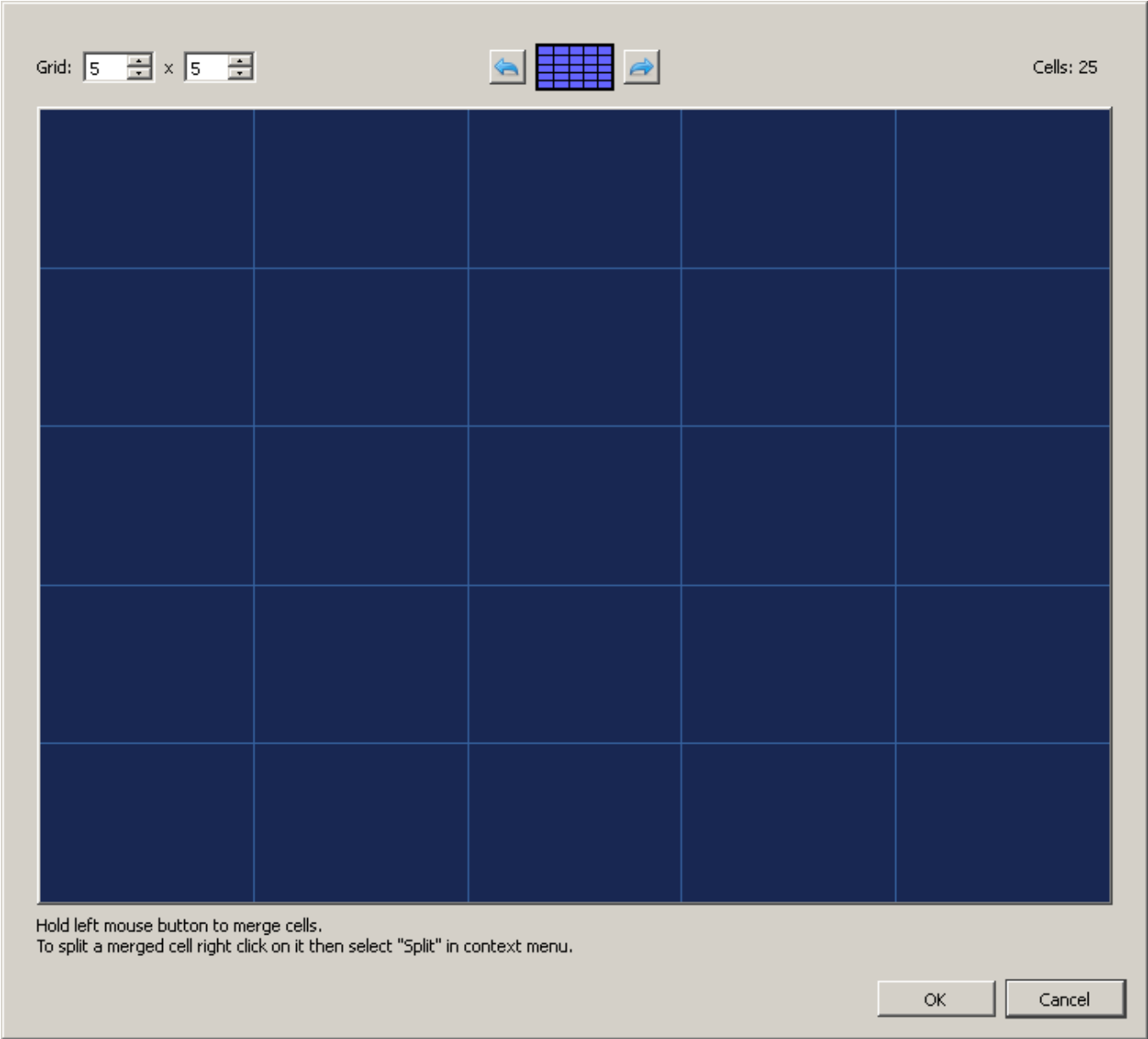


Figure 117. Layout object settings window

Table 30. Layout object settings

Parameter	Description
Grid	A grid defines the basic model of the <i>Media Client</i> 's 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
	View buttons (Previous view, Next view) to look at the intermediate versions of the layout's model. 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.
OK (Cancel)	Saving current layout and closing object settings window (Closing object settings window without saving changes).

7.7.1.5 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**.

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 **Working with Views**).

Setting up *Media Client* to work with *Views* is performed in the **Views** tab (see **Media Client**).

7.7.1.6 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 a threshold for object contrast, relative to the background. 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 a threshold for object size. The top position of the slider means the zone would detect motion of large objects only. The 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.
- **Smart Search** flag must be activated to make it possible to search alarms by selecting/highlighting part of the image.

Note. Several *Zone* objects within the same parent object are combined into the **Motion Detector** logic group in the Object Tree.

Parent object – **Camera**.

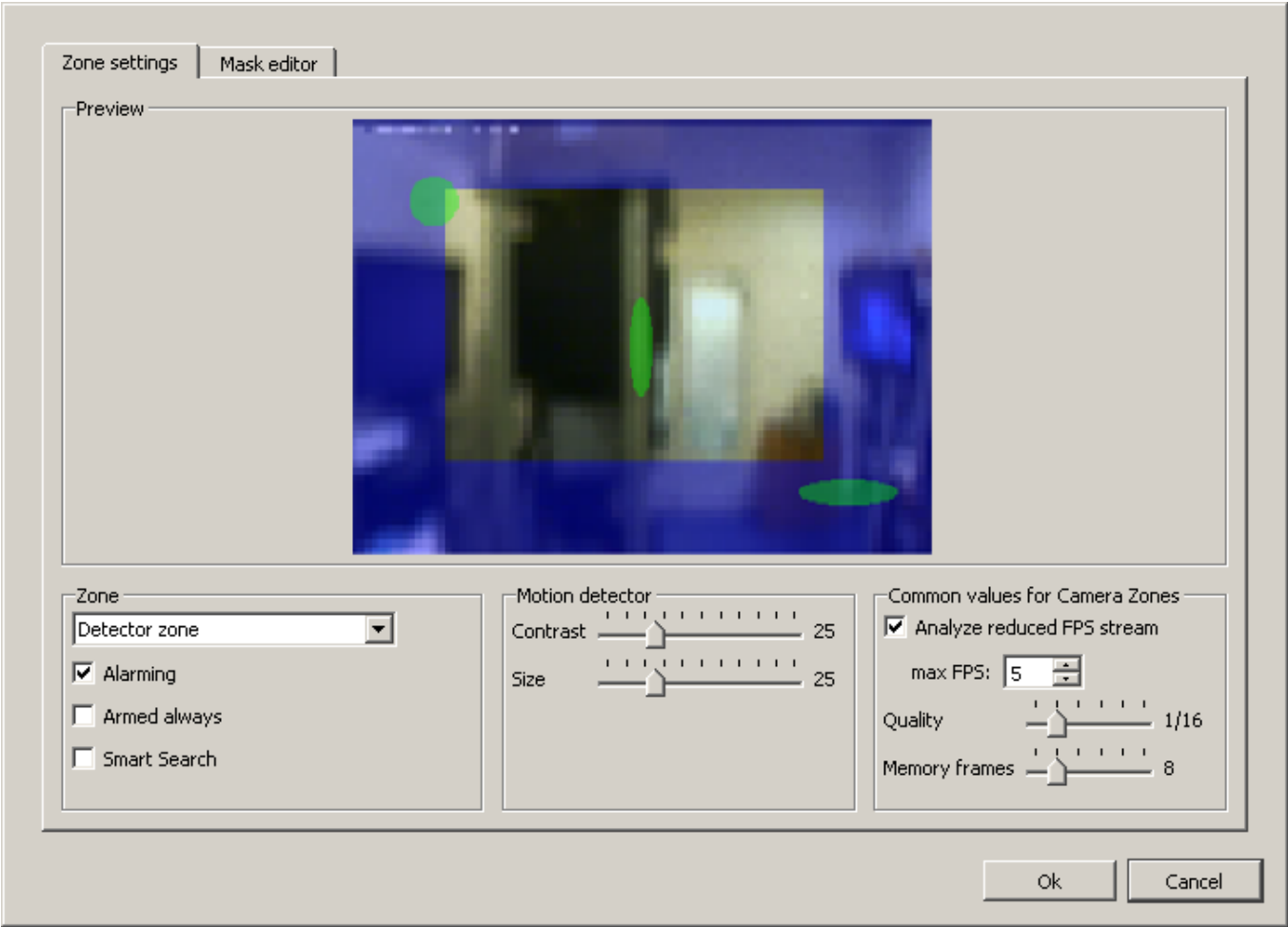


Figure 118. Zone object settings window

Table 31. Zone object settings

Parameter	Description
The Zone settings tab	
Zones	
Zone types (drop-down list)	A <i>Zone</i> can be represented with one of the following types: • 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);

Parameter	Description
	• Generic zone — stores information about zone arrangement. Warning! The Alarming, Armed always, and Smart Search parameters are available for editing only if the Zone type parameter is set to Detector zone.
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 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.
Smart Search	Select this option if you want to enable the DVR Search Panel, see SecurOS User Guide). If the checkbox is selected, alarm data will be recorded to the <code>fsindex</code> database (detection of alarms starts after the camera is armed), which in turn, further allows one to search for specific alarm criteria. The search of alarms becomes accessible in the Monitor DVR-mode. Warning! All records will be registered in the SecurOS database, assuming the default PostgreSQL database is used. In case of other databases, records will not be recorded and searching will be impossible. 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.
Motion detection	
Contrast	Move slider to specify detected object contrast sensitivity. Boundary values: <code>min</code> — even low-contrast objects will be detected. <code>max</code> — only objects with high contrast will be detected.
Size	Move slider to specify detected object size sensitivity. Boundary values: <code>min</code> — even smallest objects will be detected. <code>max</code> — only large objects will be detected.
Common values for Camera Zones	

Parameter	Description
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; 99].
Quality	Specify image quality used when analyzing motion. The term quality stands for the number of pixels per image unit. Possible values from 1/32 to 1 (of initial image). Default value – 1/16.
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 119)	
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.

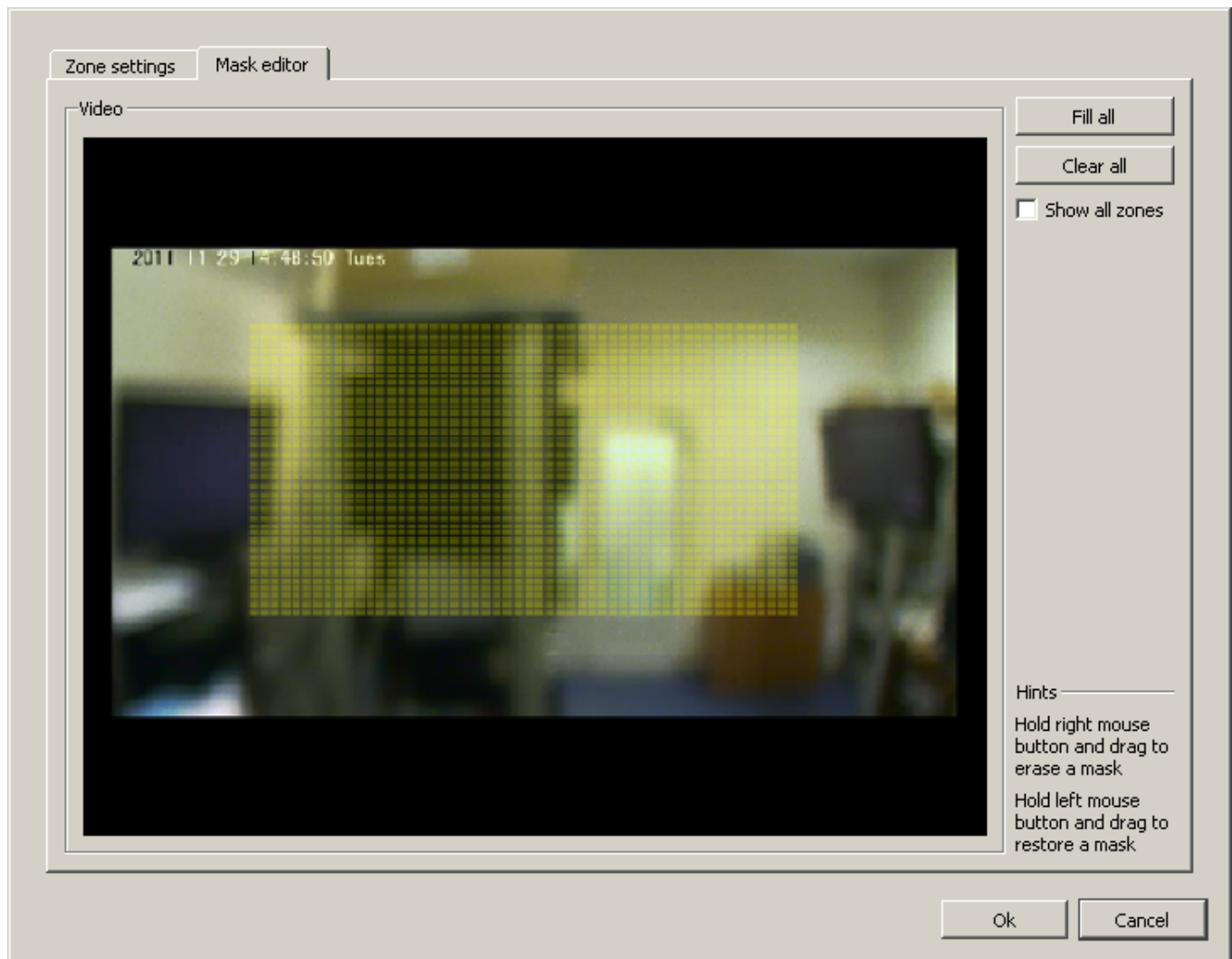


Figure 119. Zone object settings window. Mask editor

For detailed information about motion detection zone control see the [Managing Zones](#) section.

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.

7.7.1.7 Light Detector

This object represents the detector of contrast between inner and outer zones.

Parent object – [Camera](#).

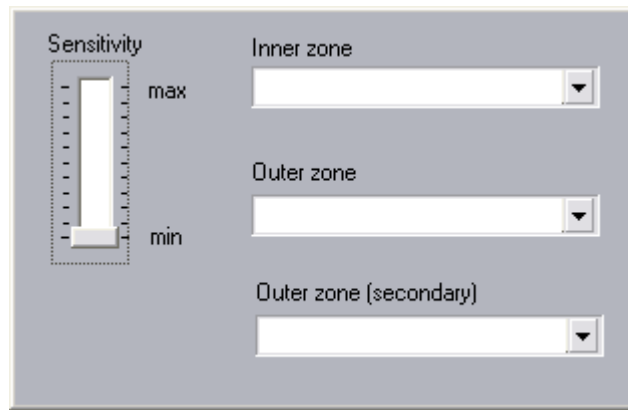


Figure 120. Light Detector object settings window

Table 32. Light Detector object settings

Parameter	Description
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.
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.

7.7.1.8 PTZ Controller

Represents an interface to connect PTZ devices (e. g. RS485 port or serial communication port with RS232 to RS485 converter attached if PTZ device works through the RS232/RS485 interface, or a network PTZ camera), and a specific PTZ protocol.

Parent object — **Computer**.

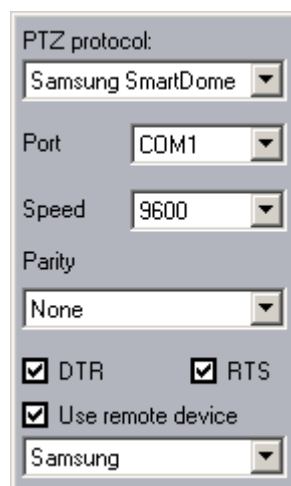


Figure 121. PTZ Controller object settings window

Table 33. PTZ Controller object settings

Parameter	Description
PTZ protocol	Select from the list box the required PTZ protocol to control the PTZ device.
Port	Select the computer's (or IP encoder's) serial communication port that has the RS232 to RS485 converter connected. For PTZ devices integrated with a camera, use default value, as well as for the Speed and Parity fields (see below).
Speed	Select speed of the data transmission (double check with the PTZ device documentation for information on required speed value). The lesser the speed, the more reliable the communication. Default value— 9600.
Parity	Select from the list a method of parity control for data transmission through the serial port (double check with the PTZ device documentation for information on required settings).
DTR, RTS	Enable options corresponding to DTR or/and RTS data flow control. Note. If the PelcoNET 350 device type was selected for the <i>Video Capture Device</i> and DTR option is checked and RTS is not checked, then RS-232 protocol will be used, otherwise RS-485/422 will be used.
Use remote device	Enable this option to work with a PTZ device over the network. Optional: select video hub connected to the device (e. g. VideoHub or LinuxHub) or IP camera with integrated PTZ device (e. g. AXIS or Bosch) from the drop down list box to use it as a proxy to transmit PTZ commands. If a video hub is selected, the port settings above will apply to the hub's serial port (video hubs usually have single serial communication port).

7.7.1.9 PTZ Device

Represents a physical PTZ device connected with a camera through the RS485 interface or integrated with an analog/digital PTZ camera (or dome camera), and a list of its preset positions (presets).

Warning! When connecting an analog camera to a video server, including video hub IP-devices, specify ID of the new object that equals to identifier specified in the video-HUB serial port settings (when connecting through RS232/RS485 interface), or identifier of the unique RS485 interface address of the corresponding physical device or camera. RS485 address is set on device by DIP switches (check the PTZ device documentation for more information). The address should be in the 0 . . . 255 range as single RS485 line can address up to 256 devices.

Notes:

1. Choose name of the object from the **Pan/Tilt/Zoom** list in the camera object settings window corresponding to the camera controlled by this PTZ device (see **Camera**).
2. To control PTZ device through HTML form, it is necessary to indicate an identifier of the corresponding *PTZ Device* object in the **Address** field of the PTZ dialog window (see **SecurOS User Guide**).

Parent object – **PTZ Controller**.

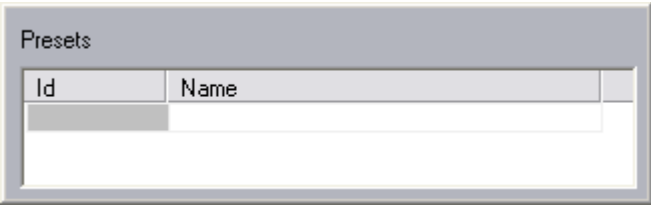


Figure 122. PTZ device object settings window

Table 34. PTZ Device object settings

Parameter	Description
Id	Choose preset identifier. Warning! It must coincide with corresponding preset ID configured in the PTZ device hardware settings (otherwise preset may not work correctly).
Name	Specify a name for the preset. A list of these presets will be displayed in the operator interface when working with this PTZ device.

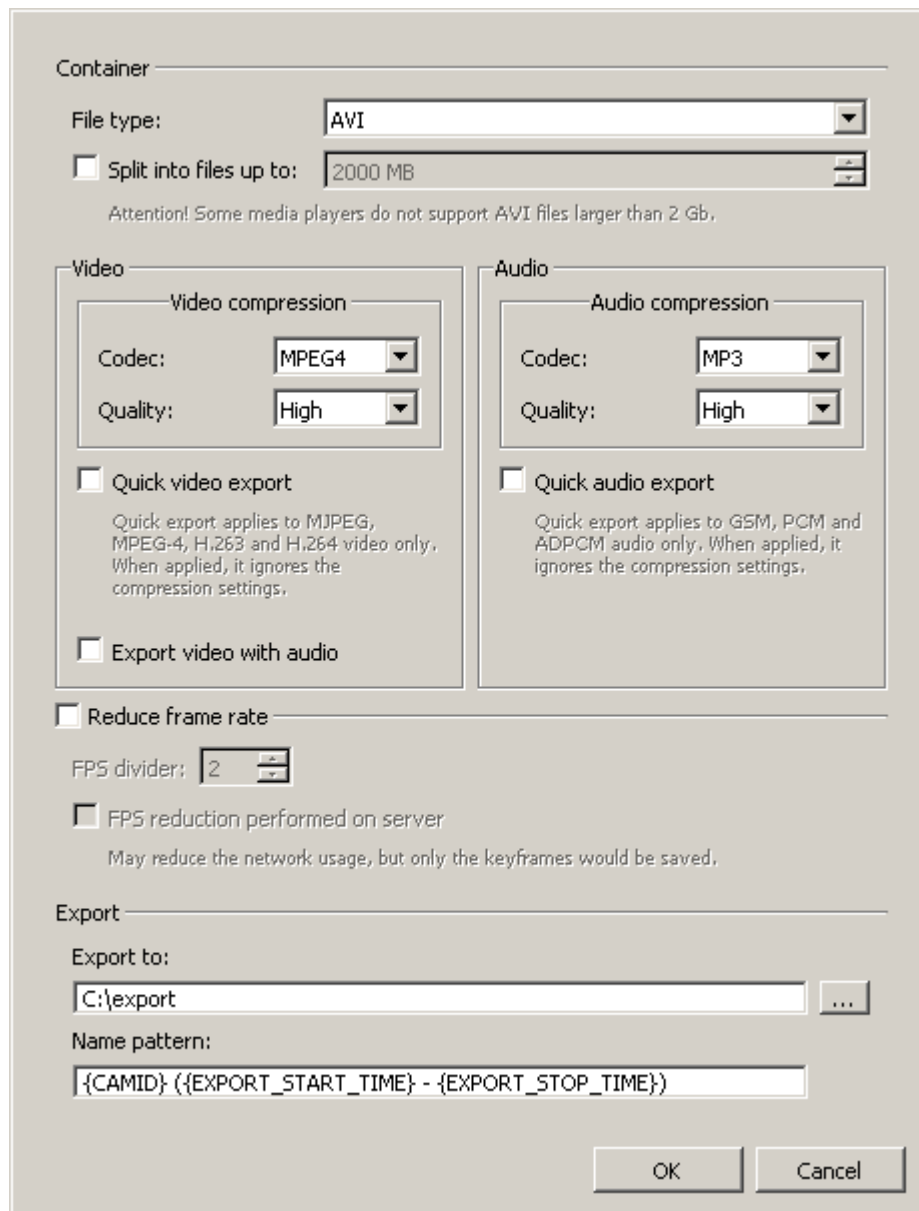
7.7.1.10 Archive Converter

This object is used to get video/audio archives from all the video servers of the system and convert them to ASF, AVI or ISS Native formats.

Warning! 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.

Note. To play **quick converted** video It is recommended to use VLC media player.

Parent object – **Computer**.



The image shows the 'Archive Converter object settings' window. It is divided into several sections:

- Container:**
 - File type:** A dropdown menu set to 'AVI'.
 - Split into files up to:** A text box containing '2000 MB'.
 - A warning note: 'Attention! Some media players do not support AVI files larger than 2 Gb.'
- Video:**
 - Video compression:**
 - Codec:** A dropdown menu set to 'MPEG4'.
 - Quality:** A dropdown menu set to 'High'.
 - ☐ **Quick video export**
Quick export applies to MJPEG, MPEG-4, H.263 and H.264 video only. When applied, it ignores the compression settings.
 - ☐ **Export video with audio**
- Audio:**
 - Audio compression:**
 - Codec:** A dropdown menu set to 'MP3'.
 - Quality:** A dropdown menu set to 'High'.
 - ☐ **Quick audio export**
Quick export applies to GSM, PCM and ADPCM audio only. When applied, it ignores the compression settings.
- ☐ **Reduce frame rate**
 - FPS divider:** A text box containing '2'.
 - ☐ **FPS reduction performed on server**
May reduce the network usage, but only the keyframes would be saved.
- Export:**
 - Export to:** A text box containing 'C:\export' and a browse button (...).
 - Name pattern:** A text box containing '{CAMID} {EXPORT_START_TIME} - {EXPORT_STOP_TIME}'.

At the bottom right are 'OK' and 'Cancel' buttons.

Figure 123. Archive Converter object settings window

Table 35. Archive Converter object settings

Parameter	Description
Container	
File type	Select format of converted file: AVI, ASF or ISS. Default value is - ASF. Note. The ISS format is used to export files encoded with ISS Native codec. If this format is selected, then the frame rate reduction setting is ignored. The converted video can be played back with the help of the ISS Media Export Utility, or with the <i>Archive Player</i> (installed separately).
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.

Parameter	Description
Video (video conversion parameters)	
Codec	Select video codec to convert archive video. Possible values: • MJPEG; • MPEG-4.
Quality	Select the quality of the converted video.
Quick video export	Use original video codec during conversion. Makes it possible to increase conversion rate significantly and to reduce CPU load. Can only be used for H.263, H.264, MJPEG and MPEG-4 formats.
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.
Audio (audio conversion parameters)	
Codec	Select audio codec to convert archive audio. Possible values: • PCM; • WMA (for ASF container); • MP3 (for AVI container).
Quality	Select the quality of the converted video.
Quick audio export	Use original audio codec during conversion. Can only be used for GSM, PCM and ADPCM formats. ADPCM format will be converted to the PCM format.
Reduce frame rate (use frame rate reduction during conversion)	
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. Warning! Using the FPS reduction performed on server parameter allows for the reduction of network load. However, this increases the <i>Video Server's</i> CPU load.
Export (export parameters)	
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
Name pattern	Template for the created file names. Can be formed by any combination of <i>valid characters</i> and <i>macro substitutions</i>. Optional parameter. Default value is {CAMID} ({EXPORT_START_TIME} - {EXPORT_STOP_TIME}) Any characters, that are permitted to be used in the file names by used OS. The following macro substitutions are available (curly brackets are necessary): • {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; • {COMMENT} — export initiator comment, used when the conversion is started from a program or a bookmark is exported; • {CUR_YEAR} — current year in "YYYY" format; • {CUR_MONTH} — current month in "MM" format. Non-significant zero is omitted when displaying in the file name; • {CUR_DAY} — current day in "DD" format. Non-significant zero is omitted when displaying in the file name; • {CUR_HOUR} — current hour in "HH" format. Non-significant zero is omitted when displaying in the file name; • {CUR_MINUTE} — current minute in "MM" format. Non-significant zero is omitted when displaying in the file name; • {CUR_SEC} — current second in "SS" format. Non-significant zero is omitted when displaying in the file name; • {CUR_FRAC} — current millisecond in "SSS" format. Non-significant zero is omitted when displaying in the file name; • {CUR_DATE} — current date in "YYY-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");

Parameter	Description
	• {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.

Warning! Windows Media Player installed on Windows XP does not play video files converted to ASF format with the MJPEG codec.

7.7.1.11 Archiver

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

Object is used to copy video (for specified cameras) from local storage to long-term storage (video in SecurOS format) and to play it back.

Note. To create a long-term archive it is necessary to create the **Archiver Dialog** object. Alternatively, one can use just *Archiver* object with **Macro** to create long-term archive. To play created archives use the **Monitor** or the **ISS Media Export Utility**.

Searching for long-term archive records for playback is performed by a *Camera* object identifier in accordance with the following rules:

1. If an *Archiver* is defined in the *Monitor* object settings, the system searches if the *Camera* is specified in the settings of this *Archiver* object.
2. If the requested *Camera* is not found in the settings of the given *Archiver* object, then further *Camera* searching is performed by ascending *Archiver ID* value for all of the *Archiver* objects existing within the security system.
3. *Camera* searching is stopped when the requested *Camera* is found within the settings of the any *Archiver* existing within system. Then the system will search the long-term archive appropriate for the found *Camera* on the hard drives of the *Computer*, that is the parent object of the found *Archiver*.
4. Further searching is terminated if long-term archive is not found.

Warning! If an object is disabled (see [Disabling Objects](#)), then in order to convert archive records with the help of *Monitor* (see [Export Video Using Monitor](#)) it is necessary to restart SecurOS.

It is recommended to define the required free disk space before archive recording, see [Archive Recording](#) section.

Parent object – [Computer](#).

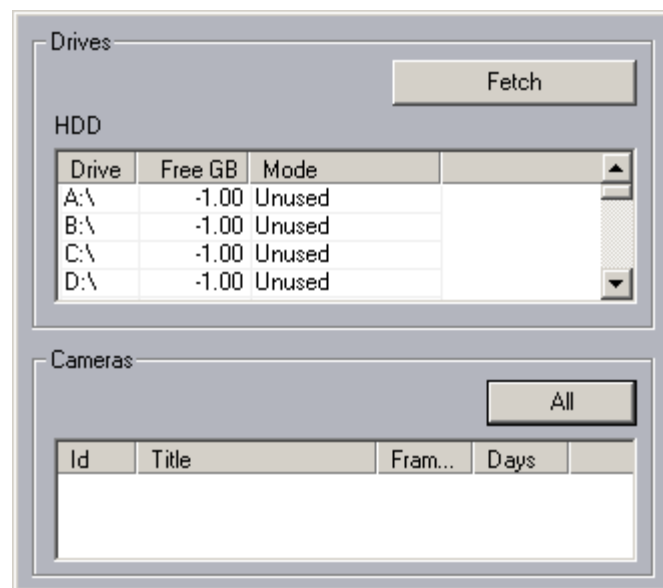


Figure 124. Archiver object settings window

Table 36. Archiver object settings

Parameter	Description
Drives	
Fetch	Click this button to update the HDD table.
HDD	List of available drives (local and mapped drives can be used). Enable or disable reading/writing to one of the drives by selecting the corresponding value from the drop-down list in the Mode row.
Cameras	

Parameter	Description
All	Click this button to populate the Cameras table with all the cameras within the SecurOS security network. To select specific cameras use either the object ID or Title .
Id	Select ID of a <i>Camera</i> object.
Title	Select name of a <i>Camera</i> object. You can use either ID or Title to specify target camera.
Frames per second	Choose the frame rate (in long-term archive) from the list (value from 1 to 30). If specified value is less than operative archive frame rate, then decimation will be done.
Days	Specify the archive depth: the long-term archive of the camera will be stored for the set quantity of days then it will be removed by the system.

7.7.1.12 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/JavaScript 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.

7.7.1.13 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. Transmission is initialized on the external system side by request (see below). 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.

Warning!

- Any stream of the multi-streaming camera can be transmitted.
- Transmission of the synchronized audio is not supported.

Parent object – **Computer**.

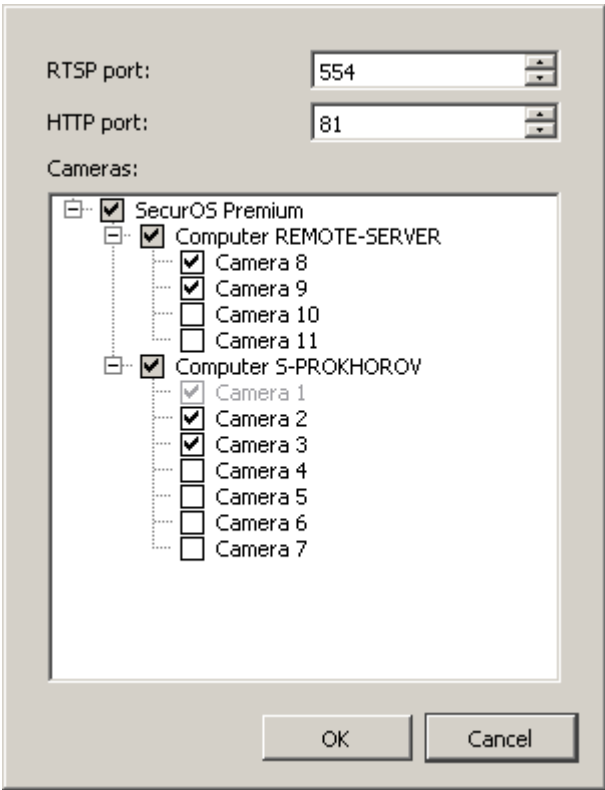


Figure 125. RTSP Server object settings window

Table 37. 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 <code>netstat -aon more</code> query in the command prompt to determine the free port.
Cameras	

Parameter	Description
Object tree	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. Note. Temporarily disabled <i>Cameras</i> (see Disabling Objects) are marked in the Object Tree in gray (see Figure 125, Camera 1). 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.
Buttons	
OK (Cancel)	Save specified values and close object settings window (Close object settings window without saving changes).

After the *RTSP Server* object is created and configured, SecurOS's video can be received by queries of the following format (query string is entered in the Address field of the external application):

Warning! All parameters of the query exclude `stream` are mandatory!

- Query to receive live video:

`rtsp://<IP>:<Port>/live?id=<cam_ID>&stream=<stream_name>`, where:

- <IP> – IP address of the host, where the *RTSP Server* is located;
- <Port> – RTSP port, specified in the *RTSP Server* object settings;
- <cam_ID> – SecurOS's camera ID;
- <stream_name> – type of the transmitted stream, if camera supports multi-streaming (see **Camera**). Possible values:
 - `low` – low resolution stream;
 - `normal` – base stream;
 - `high` – high resolution stream.

- Query to receive archive records:

`rtsp://<IP>:<Port>/archive?id=<cam_ID>&from=<start_date>&to=<end_date>`, where:

- <IP> – IP address of the host, where the *RTSP Server* is located;
- <Port> – RTSP port, specified in the *RTSP Server* object settings;
- <cam_ID> – SecurOS's camera ID;
- <start_date> – archive record fragment start date (in YYYY-MM-DD HH:MM:SS format);
- <end_date> – archive record fragment end date (in YYYY-MM-DD HH:MM:SS format).

Warning! The video stream is transmitted without changes, as it was generated by the camera or recorded to archive (i.e. without transcoding).

Information about whether an archive record exists for the period (with exact start and end dates of the fragments) can be obtained by the query of the following format (query string is entered in the Address field of the web-browser):

`http://<IP>:<Port>/control?`

`method=get_archive_info&id=<cam_ID>&from=<start>&to=<end>`, where:

- <IP> – IP address of the host, where the *RTSP Server* is located;
- <Port> – HTTP port, specified in the *RTSP Server* object settings;
- <cam_ID> – SecurOS's camera ID;
- <start> – start date of the period to search archive in SecurOS (in YYYY-MM-DD HH:MM:SS format);
- <end> – end date of the period to search archive in SecurOS (in YYYY-MM-DD HH:MM:SS format).

Warning! The query is executed only for *Cameras* selected in the *RTSP Server* object settings, excluding disabled *Cameras* (see [Disabling Objects](#)). Otherwise query returns error (see [listing 2](#)).

Listing 2. Archive search query error

```
<result cause="2">
  </params>
  <param name="descr" value="not_found"/>
</params>
</result>
```

If the query is executed correctly and archive records are found within specified period, the following xml-file is generated:

Listing 3. List of the archive record fragments

```
<list>
  <archive-info from="2014-02-17 13:54:06" to="2014-02-17 13:54:11"/>
  <archive-info from="2014-02-17 13:54:46" to="2014-02-17 13:54:53"/>
  <archive-info from="2014-02-17 13:55:10" to="2014-02-17 13:58:16"/>
  <archive-info from="2014-02-17 13:58:32" to="2014-02-17 13:59:18"/>
  . . .
  . . .
  . . .
  <archive-info from="2014-02-17 15:02:34" to="2014-02-17 15:02:57"/>
  <archive-info from="2014-02-17 15:03:24" to="2014-02-17 15:03:31"/>
  <archive-info from="2014-02-17 15:03:58" to="2014-02-17 15:04:15"/>
</list>
```

To get required fragment of the SecurOS archive, execute archive query ([see above](#)) with <start_date> and <end_date> parameters from a string of the xml-file.

If there are no records for the specified period in the SecurOS archive, an empty list is returned:

Listing 4. Empty list

```
<list>
</list>
```

7.7.1.14 EdgeStorage Sync

This object is used to synchronize video archives on the local storage (e.g. SD Cards) of IP *Cameras* with local video archives on *Video Servers*.

Parent object – **Computer**.

This object has no settings to configure.

7.7.2 User Interface Objects

The following are User Interface objects:

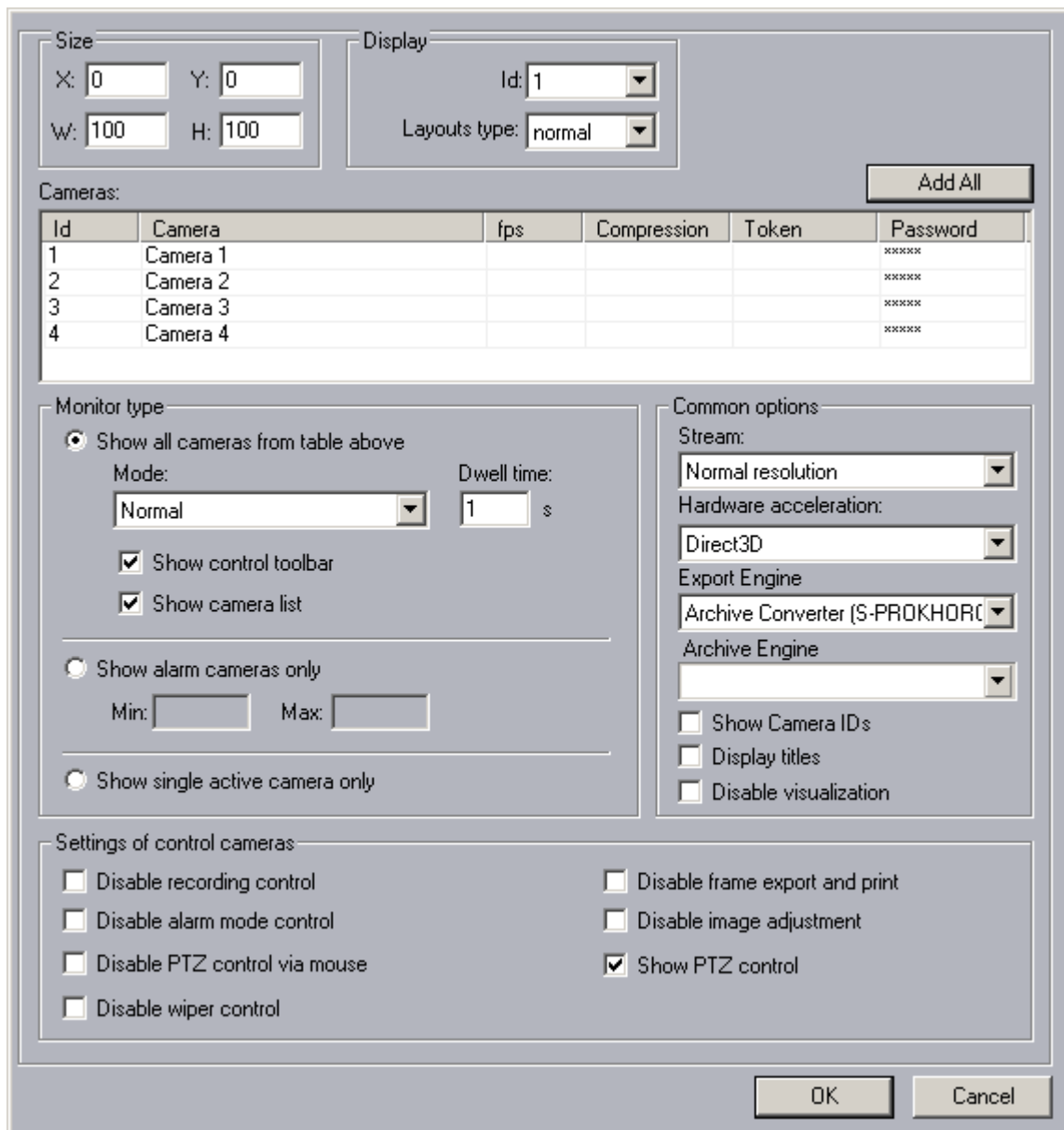
- **Monitor**.
- **Media Client**.
- **Archive Converter Dialog**.
- **Archiver Dialog**.

7.7.2.1 Monitor

This object is used to display video streams from the cameras and to create an operator interface with tools for camera control and video archive operations.

Note. It is not recommended using more than one Monitor object per physical Display. It is not possible to use video card hardware acceleration if using more than one monitor per Display which causes a significant increase in the CPU load.

Parent object – **Desktop**.



The window is titled "Monitor object settings" and contains several sections for configuring a monitor object.

Size: X: 0, Y: 0, W: 100, H: 100.

Display: Id: 1, Layouts type: normal.

Cameras: A table with 6 columns: Id, Camera, fps, Compression, Token, Password.

Id	Camera	fps	Compression	Token	Password
1	Camera 1				xxxxx
2	Camera 2				xxxxx
3	Camera 3				xxxxx
4	Camera 4				xxxxx

Monitor type:

- ☒ Show all cameras from table above
 - Mode: Normal
 - Dwell time: 1 s
 - ☒ Show control toolbar
 - ☒ Show camera list
- ☐ Show alarm cameras only
 - Min: , Max:
- ☐ Show single active camera only

Common options:

- Stream: Normal resolution
- Hardware acceleration: Direct3D
- Export Engine: Archive Converter (S-PROKHORC)
- Archive Engine:
- ☐ Show Camera IDs
- ☐ Display titles
- ☐ Disable visualization

Settings of control cameras:

- ☐ Disable recording control
- ☐ Disable alarm mode control
- ☐ Disable PTZ control via mouse
- ☐ Disable wiper control
- ☐ Disable frame export and print
- ☐ Disable image adjustment
- ☒ Show PTZ control

Buttons: Add All, OK, Cancel.

Figure 126. Monitor object settings window

Table 38. Monitor object settings

Parameter	Description
Display	
Id	Choose ID of physical display this <i>Monitor</i> belongs to.

Parameter	Description
Layouts type	Select desired monitor cell aspect ratio. Possible values: • <code>normal</code> — is recommended to display 4:3 video stream on the display with 4:3 aspect ratio and 16:9 video stream on a wide-screen display; • <code>special</code> — is recommended to display 4:3 video stream on a wide-screen display. Warning! If <code>special</code> type is selected then the frame can be horizontally squeezed when displaying video stream on a 4:3 display. Default value is <code>normal</code>.
Size	
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.
Cameras (table with list of used cameras and their video settings). If Monitor type is set to <code>Show alarm cameras only</code> and <i>Camera</i> is not listed it will use the default video settings and video stream will flow directly from the video server.	
Add all	Click this button to populate the Cameras table with all cameras available within the security network.
Id	Select ID of a <i>Camera</i> object.
Camera	Select name of the <i>Camera</i> object. Like the ID field, the name field can be used to specify the target camera.
fps	Optional: select the maximum frame rate of the video feed delivered to the clients. The frame rate cannot exceed the actual frame rate of the video from the camera. If not specified, original frame rate is used. This setting can be used to reduce system network load.
Compression	Optional: select the compression type of the video that will be transmitted to the clients (if the source and target compression levels differ, video will be recompressed). If not specified, original compression is used.
Token	Optional: specify the token string (unique ID) to activate titles as overlay on video of this camera's cell using SecurOS script commands. If you want to display titles, use <code>cam_N</code> (where <code>N</code> is the ID of the <i>Camera</i> object) or any other string as the token, and use this value as a parameter for script commands of adding or deleting titles. Note. Titles are displayed only when Display titles option is enabled (see below).

Parameter	Description
Password	Optional: if the source camera is password-protected specify the password to be able to watch video from this camera. If a password does not match, you will see a green mask instead of real video in your monitor.
Monitor type	
Mode	Choose monitor mode. Possible values: Normal— default mode. All cameras are in live video mode; operator may enter and leave archive mode of any camera. Operator may enter and leave DVR mode. PTZ control panel is available if the Show PTZ control option is activated (see below); Live only— all cameras are in live mode. Operator is forbidden to enter archive mode. DVR button is hidden; Archive only— all cameras are in archive mode. Operator is forbidden to leave archive mode. Operator may enter and leave DVR mode. PTZ control panel is hidden; DVR only— all cameras are in archive mode. Operator is forbidden to leave archive mode. Monitor is in DVR mode. DVR button is hidden. PTZ control panel is hidden; LPR— the same as DVR only but only one active camera is shown, Search DVR panel is hidden; Map (2x vertical)— mode for wide screen live video viewing; no more than two active cameras can be shown; control panels and camera blocks are hidden.
Show all cameras from table above	Select this option to display a fixed list of cameras specified in the Cameras table on the monitor (this mode is enabled by default).
Dwell time	Specify a delay in seconds between automatic switching/scrolling of named layouts or cameras on a monitor. Default value is 3. See SecurOS User Guide for more information on this feature.
Show control toolbar	Check this option for the monitor to display control toolbar (toolbar options include switching between layouts, cameras, list cameras by pages manually or automatically, view alarm log for target cameras, etc.).
Show camera list	Check this option to show camera block in user interface (on the given monitor).
Show alarm cameras only	Check this option to automatically display on this monitor a set of cameras that are currently in alarm state for the current <i>Computer</i> object. Cameras that are not alarmed (no motion detected for them) will never be displayed using this option. Set the values in the Min and Max fields (see below) to limit the minimum and maximum number of simultaneously displayed alarm cameras.

Parameter	Description
Min, Max	Optional: Specify the minimum (1...16) and maximum (1...16) number of alarm cameras displayed. Numbers will be rounded up to a higher value of either 1, 4, 9 or 16 in accordance with a layout selected for the monitor. If there will be more than Max alarm cameras at the same time, only the most recent cameras will be displayed.
Show single active camera only	Check this option to automatically display on this monitor only one currently active camera from another monitor or selected on a map in the same <i>Desktop</i>. If another monitor does not exist or a camera on the map is not selected then nothing will be displayed on this monitor. The table of cameras is used to define or override video settings for some cameras to display. If the camera is not in the list, its default video settings will be used. Notes: 1. It is recommended to create such an active monitor to make it easier to work with another monitor containing a large amount of cameras or for working with a map. 2. If using a map and an <i>active</i> monitor on the same desktop, an operator can easily see video from any camera on a map by simply selecting it on this map.
Common options	
Stream	Select stream to display. Warning! Selected stream type will be displayed in all cells of the <i>Monitor</i>. Note. For the cameras that do not support multi-streaming, Stream represents all three types simultaneously. Therefore, regardless of the type selected, it will appear the same. For the additional information see Multi-streaming and Camera.
Hardware Acceleration	Select hardware acceleration type for displaying video. Possible values: No — software rendering is used; Warning! Software rendering consumes a lot of CPU resources; use hardware acceleration whenever possible. Overlay and Direct3D — differences between these types are typically insignificant. Try to experiment with both types and see which mode is supported by your video card, gives better picture quality and, possibly, uses less CPU. Warning! If it is necessary to display titles on a user monitor, make sure that the current video card supports hardware acceleration and set the appropriate value.

Parameter	Description
Export Engine	Select <i>Archive Converter</i> object used to export video (see Archive Converter). Warning! It is not possible to export a video sequence if this parameter is empty!
Archive Engine	Select <i>Archiver</i> object used to copy video to long-term storage (see Archiver). When entering a Monitor's archive mode, (see SecurOS User Guide for more information) the Long-term mode option will become accessible. Note. The monitor will play archived video from cameras that are defined in the <i>Archiver</i> object settings.
Show camera IDs	Check this option to display internal camera IDs along with names. Used primarily for script debugging purposes.
Display titles	Enable or disable displaying of titles for all cameras on the monitor. For displaying titles use script commands. If you disable this option, titles will not be shown on all cameras, regardless of Token option value (see above).
Disable visualization	Disable the mouse pointed camera cell zoom.
Settings of control cameras	
Disable recording control	Check this option to disable recording control using Monitor (see SecurOS User Guide).
Disable alarm mode control	Check this option to disable camera's alarm mode control using Monitor (see SecurOS User Guide).
Disable PTZ control via mouse	Check this option to disable PTZ control by mouse using Monitor (see SecurOS User Guide).
Disable wiper control	Check this option to disable wiper control using Monitor (see SecurOS User Guide).
Disable frame export and print	Check this option to disable frame export and printing using Monitor (see SecurOS User Guide).
Disable image adjustment	Check this option to disable image adjustment for the camera cell using Monitor. Digital zoom, Grid and Contrast filter options will be disabled (see SecurOS User Guide).
Show PTZ control	Check this option to show the PTZ control panel (see SecurOS User Guide). The panel is active only for active PTZ cameras displaying video in live mode. Otherwise the PTZ control panel will not be active.

Warning! To correctly display all interface elements in the Monitor DVR mode, it is recommended to set the physical display resolution to no less than 1280x1024 and the **W** and **H** Monitor object parameters to no less than 80.

7.7.2.2 Media Client

This object represents an updated version of the operator GUI which allows a user to work with the system *Cameras* and *Microphones*. The previous GUI is represented by the *Monitor* object. As compared with the *Monitor*, which allows operating with one video stream only, the *Media Client* provides the system with the ability to process each stream generated by a multi-streaming camera in real-time (see **Multi-streaming**). Besides supporting some features of the *Monitor*, the *Media Client* allows to assign a type of stream to display depending on the camera cell size (see figure 127 and Table 40).

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).

As opposed to the **Monitor**, the *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**.

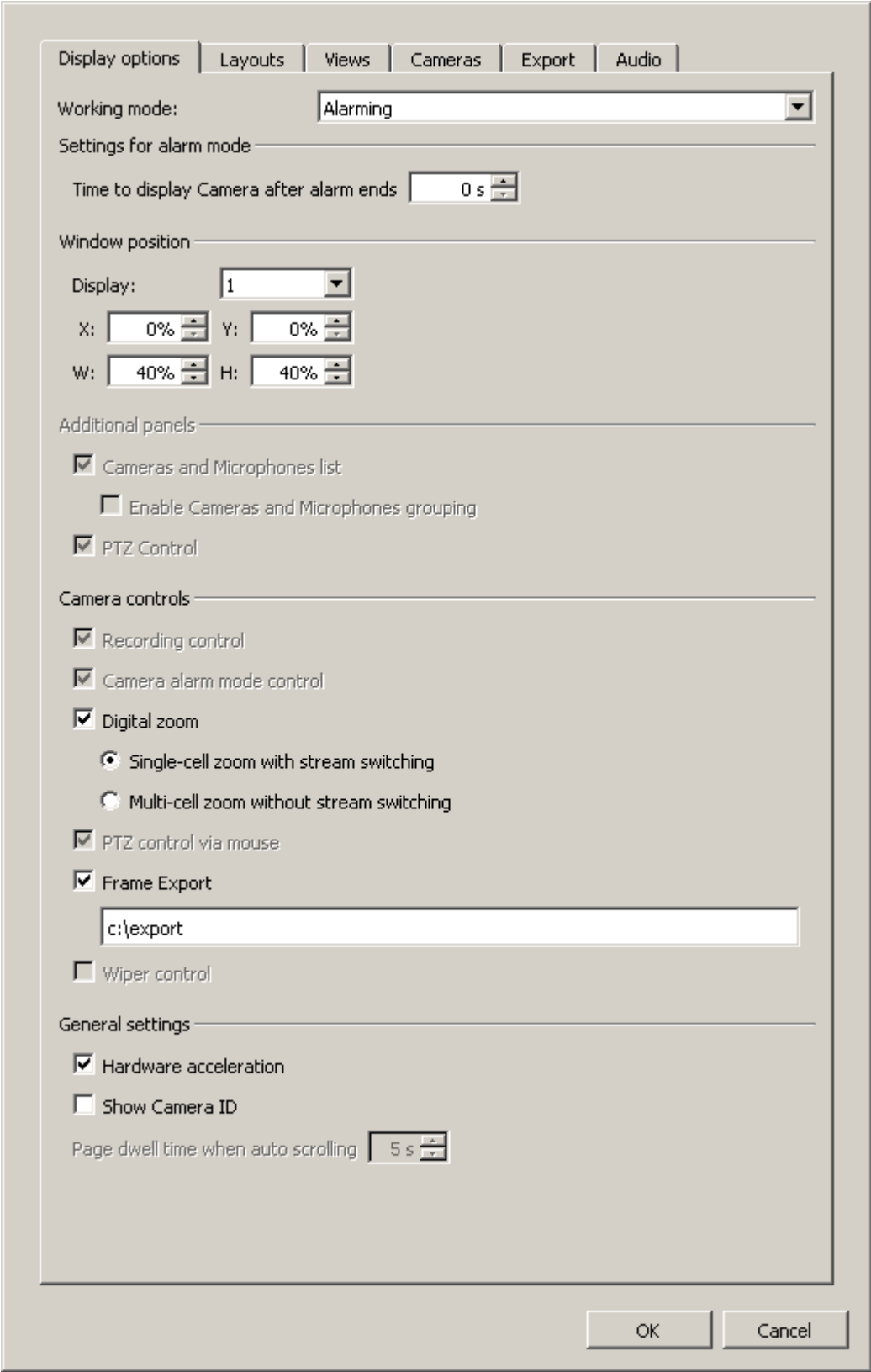


Figure 127. Media Client object settings window. Display options Tab

Table 39. Media Client object settings. Display options Tab

Parameter	Description
Working mode (select <i>Media Client</i> working mode)	

Parameter	Description
Normal	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. This mode is specified by default.
Live only	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).
Alarming	In this mode only alarmed cameras (i.e. where motion is detected) are displayed. 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's</i> controls are not available. <i>Zoom</i> and <i>Export frame</i> buttons are available in the camera cell. 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 Time to display camera after alarm ends parameter (see below).
Active	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.
View only	In this mode, the standard <i>Media Client's</i> controls are not available to the operator. 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. 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. 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: • layout switching; • moving <i>Camera</i> to the specified cell; • switching between live/archive modes; • archive control commands.
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).

Parameter	Description
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 Title (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 title 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 Title , do not belong to any level and are united under the <i>Ungrouped</i> 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.
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.

Parameter	Description
Single-cell zoom with stream switching	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. It is recommended to use this feature if cameras support multi-streaming and are configured to be operated in such mode. Option is enabled if Digital zoom parameter is selected and is the default value.
Multi-cell zoom without stream switching	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. Option is available if the Digital zoom parameter is selected.
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 <i>Media Client</i> . By default it is selected. If this option is selected, then a frame will be saved into the specified directory.
Wiper control	Select this checkbox to control <i>Wiper</i> from the camera cell.
General settings	
Hardware acceleration	Select checkbox to use Direct3D for displaying video. If the checkbox is not selected, then software rendering is used.
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 Title> format. By default is not selected.
Page dwell time when auto scrolling	Video page dwell time in auto scrolling mode (in seconds).

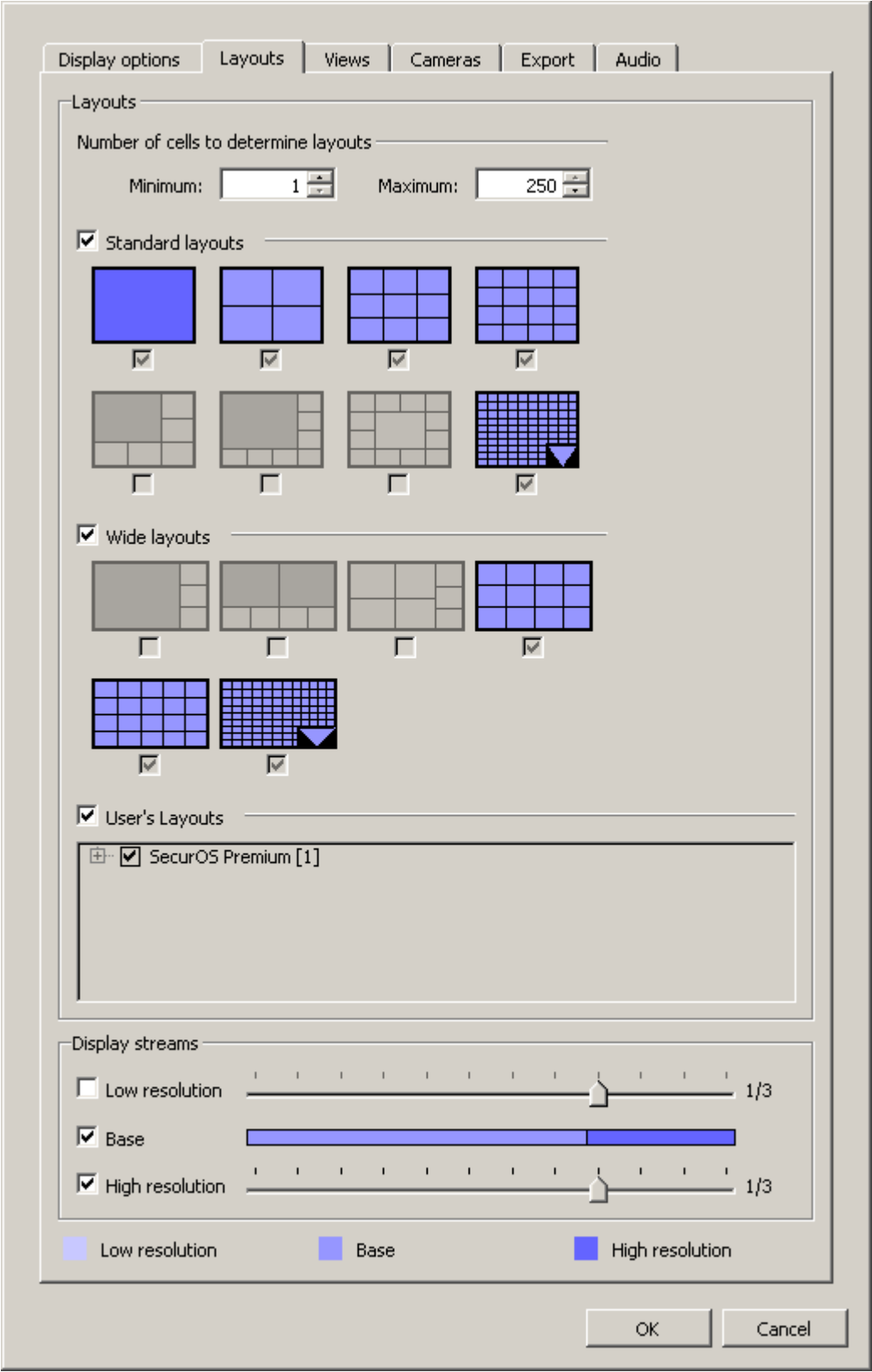


Figure 128. Media Client object settings window. Layouts Tab

Table 40. Media Client object settings. Layouts Tab

Parameter	Description
Number of cells to determine layouts	

Parameter	Description
Minimum/Maximum	Warning! Parameters are displayed only when Alarming mode is selected. 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. 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. 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.
Layouts (to select/deactivate all layouts of the group select/deactivate appropriate checkbox on the left of the group name)	
Standard layouts	Select checkbox of the appropriate standard layouts, which will be enabled to the operator in the layout panel of the <i>Media Client</i>. Warning! 1*1 layout is mandatory. It is selected by default and cannot be disabled.
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	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 128). 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.

For example, as it is illustrated in Figure 128, 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.

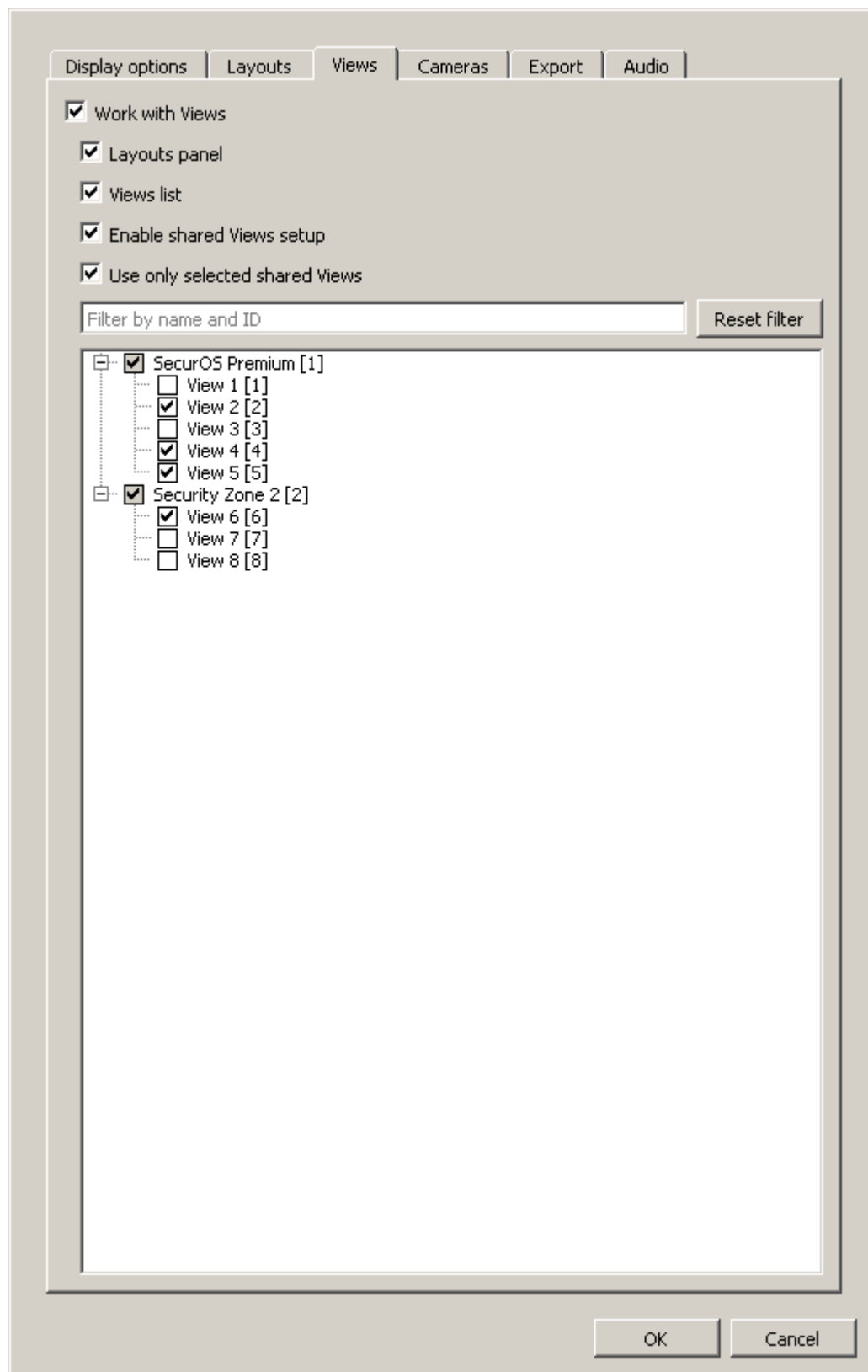


Figure 129. Media Client object settings window. Views Tab

Table 41. Media Client object settings. Views Tab

Parameter	Description
Work with Views	Select this checkbox to work with <i>Views</i>. By default is not selected. Note. Listed below parameters are available only if this checkbox is selected. Operations with <i>Views</i> are described in Working with Views section.
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	Select checkbox to activate manual control mode of the <i>Views list</i> for the given <i>Media Client</i>. 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. Note. Listed below parameters are available only if this checkbox is 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	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>. 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. Note. By default objects in the tree are sorted ascending by name and ID.

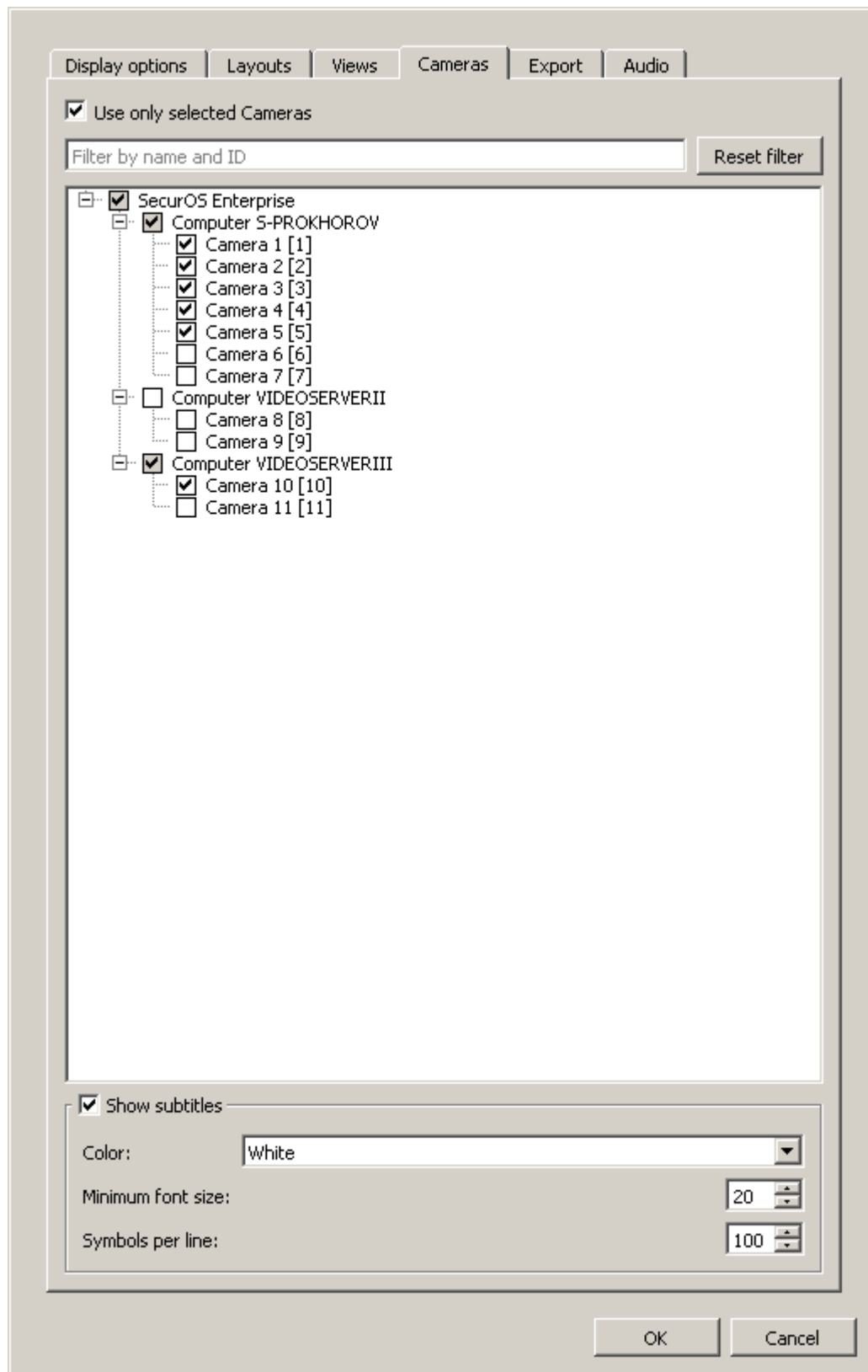


Figure 130. Media Client object settings window. Cameras Tab

Table 42. Media Client object settings. Cameras Tab

Parameter	Description
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	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. To add a camera to the <i>Media Client's Camera list</i> select appropriate checkbox to the left of the object. 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.
Show subtitles (displaying mode and parameters of the subtitles to be added to the image externally, for example, by using a <code>ADD_SUBTITLES</code> command (see SecurOS Programming Guide). Warning! If subtitle parameters are specified in the <code>ADD_SUBTITLES</code> command, the following values are ignored.	
Color	Choose a subtitles color.
Minimum font size	Specify minimal subtitles font size.
Symbols per line	Specify subtitle string length. If subtitle string exceeds frame horizontal size, it wraps to the next line.

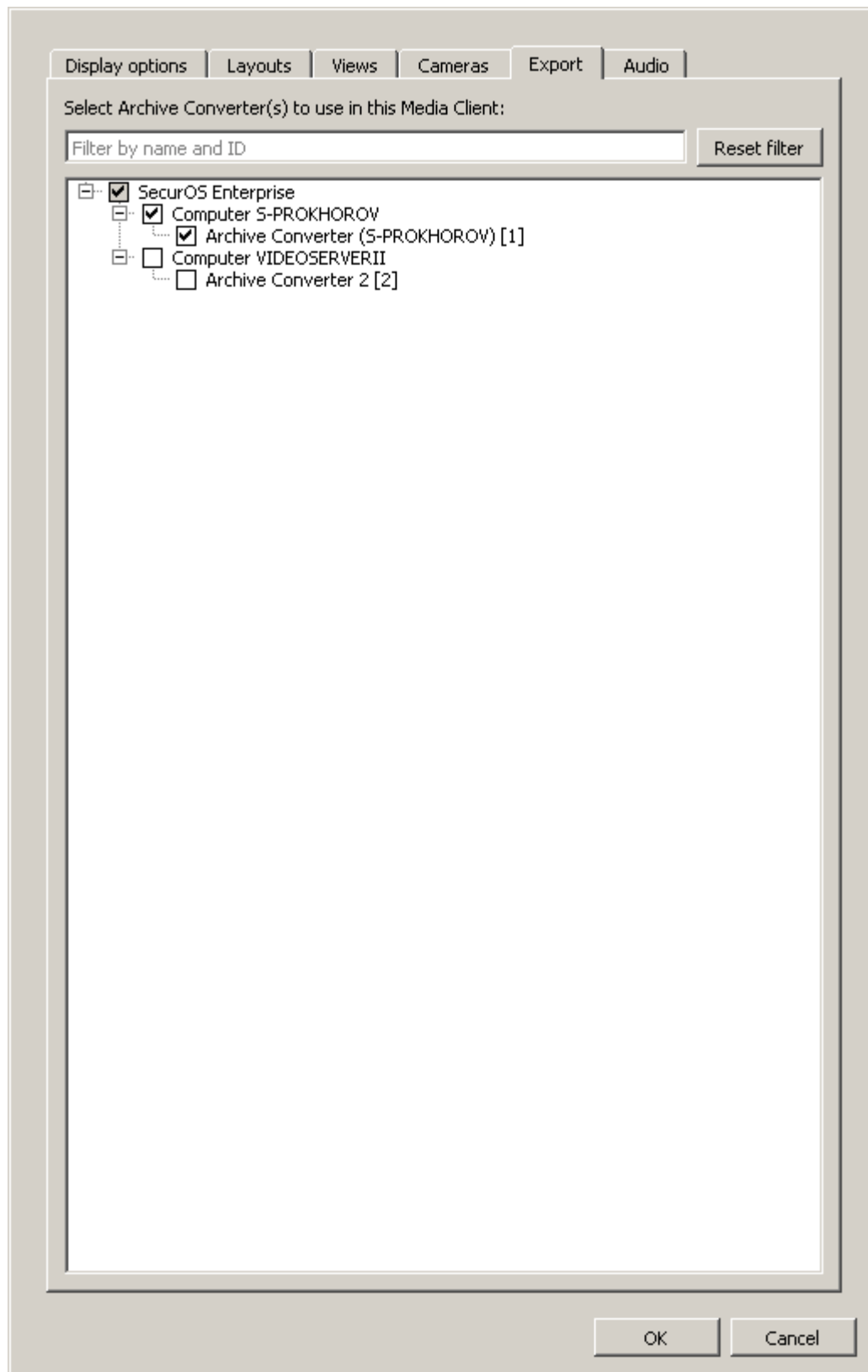


Figure 131. Media Client object settings window. Export Tab

Table 43. Media Client object settings. Export Tab

Parameter	Description
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	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>Archive Converter</i> children objects are displayed. 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.

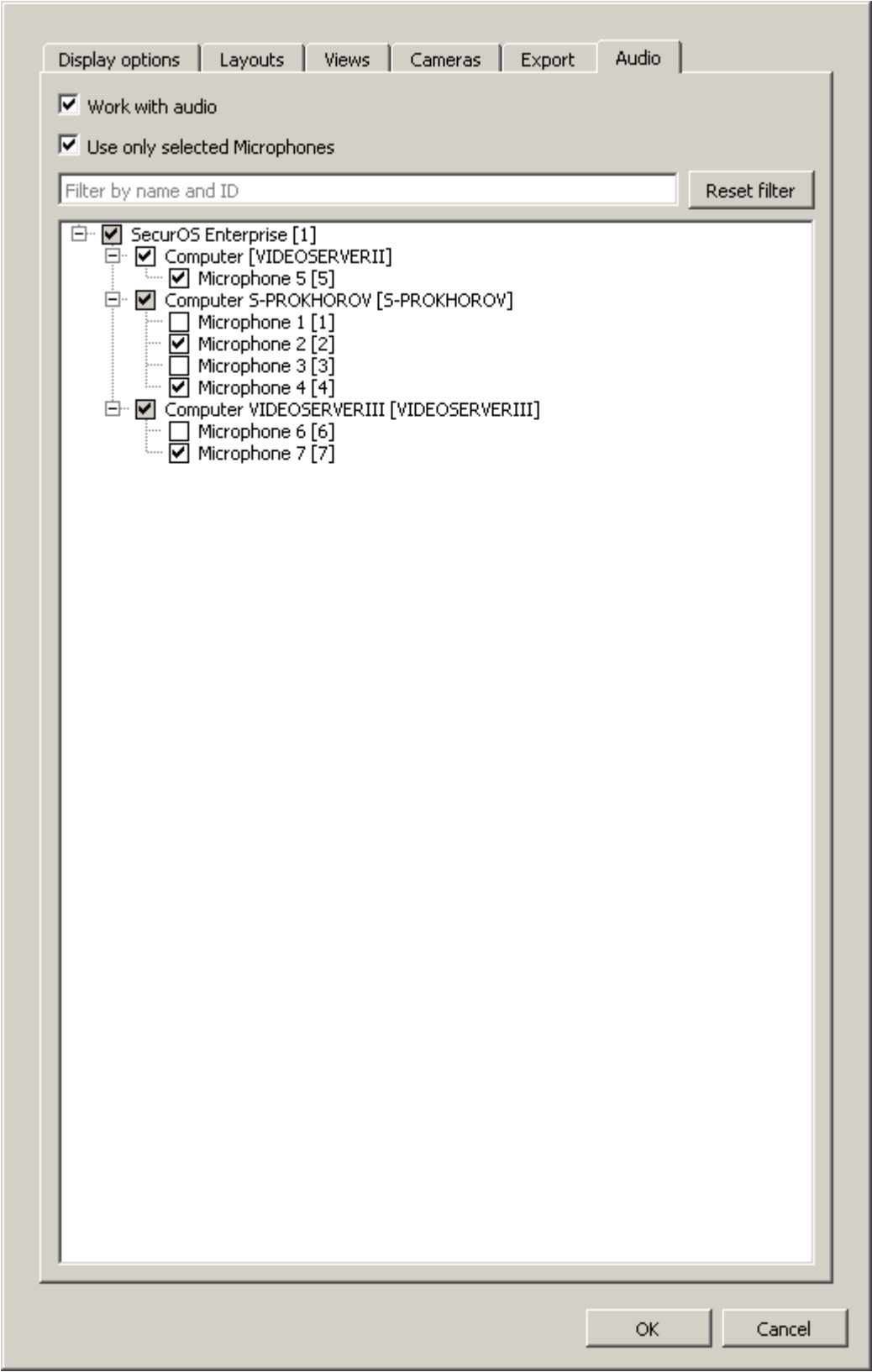


Figure 132. Media Client object settings window. Audio Tab

Table 44. Media Client object settings. Audio Tab

Parameter	Description
Work with audio	Select checkbox to listen to the live or archived audio.

Parameter	Description
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: 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.

7.7.2.2.1 Working with Views

View is a separate object of the *Media Client* that consists of the following components:

1. *Layout* — specifies *View's* geometry, i.e. quantity, mutual arrangement and size of the camera cells. *Layout* of the *View* is selected from the list of available system *Layouts* or User's *Layouts* (see [Layout](#)).
2. *Cameras* — arbitrary number of the SecurOS's *Cameras* allocated in the cells of the selected *Layout*. *Cameras* are placed in the *Layout* cells in the required order that is fixed for the *View* life cycle, but can be changed by editing.
3. *Microphones* — arbitrary number of independent SecurOS's *Microphones*, placed in the *Microphone Panel*. *Microphones* are placed in the panel in the required order that is fixed for the *View* life cycle, but can be changed by editing.

Note. No component is mandatory. For example, a *View* can contain only *Microphones*.

There are the following types of *Views*:

1. *Shared* — single-page *View* that can contain any *Camera* and *Microphone* objects created within SecurOS. *View* of given type is created by system administrator or operator. Operator can work with *Shared* views if this possibility is specified by system settings;
2. *All objects* — separate multi-page *View* that consists of all *Cameras* and *Microphones* selected to work with given *Media Client*. This *View* is created automatically and is available to any operator on any *Media Client*.

Media Client provides the following tools to control *Views* (see Figure 133):

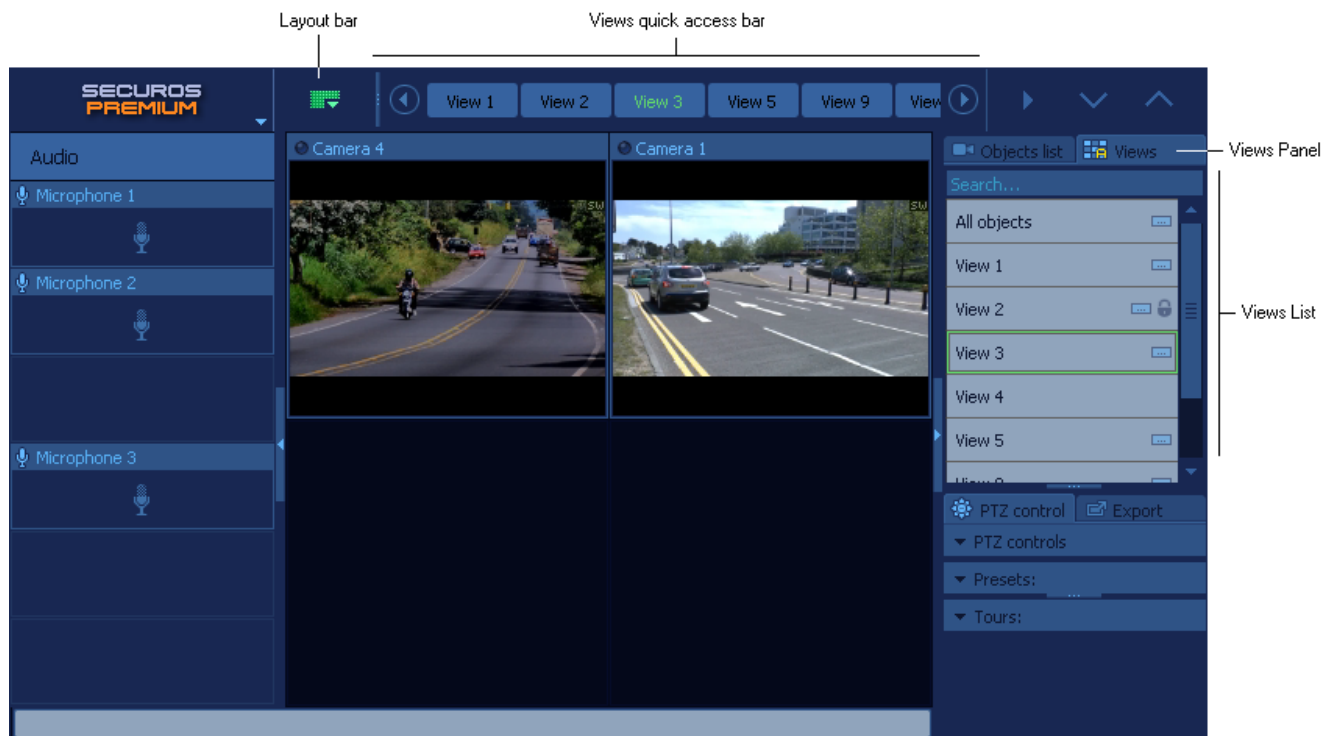


Figure 133. Media Client's View Control Tools

- *Layout bar* — (is collapsed in Figure 133) contains all *Layouts* that can be used when working with *Views*;
- *Views quick access bar* — is intended for quick switching between *Views*. Is populated with *Views* selected by administrator. To scroll panel ribbon the  and  buttons or mouse wheel are used. Currently displayed *View* is selected in the panel in green.

Note. To scroll panel ribbon place mouse cursor over it.

- *Views Panel* — contains *Views List* and *View* search field. Searching is performed by part of the *View*'s name or ID and is case insensitive;
- *Views List* — contains all *Views* available for operator to work with given *Media Client*.

Views state indicators are additionally displayed in the *Views List*:

-  — given *View* is placed on the *Views quick access bar*;
-  — given *Views* contains blocked object. When editing such a *View* it cannot be saved with current name.

Views List is displayed both in normal and edit modes. In normal mode in *Views List* are displayed only those *Views* that contain some objects. In edit mode list is supplemented with those *Views* that contain no objects. Such *Views* are highlighted gray background — .

In edit mode the *View edit bar* is displayed in the *Media Client* (see Figure 134).



Figure 134. View edit bar

This bar contains the following buttons:



— create new *View*;



— rename *View*;



— delete *View*;



— discard changes;



— save *View*;



— save *View* as.

To create *View* do the following:

1. To switch to the *Views* edit mode click the  in upper left corner of the *Media Client* (see Figure 135) and select the **Enter Views Setup** command.

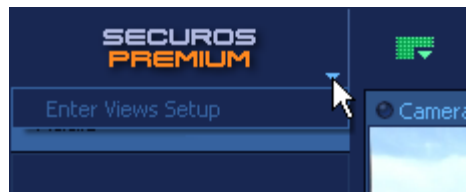


Figure 135. Switching to Views edit mode



2. Click the  button. System will display the *View* create window (see Figure 136).

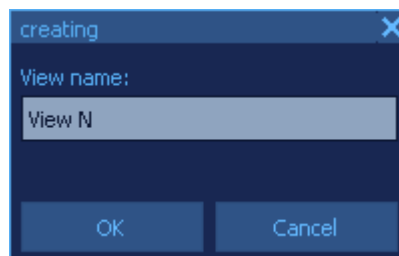


Figure 136. View create window

3. Specify a name of new *View* in the **View Name** field. Click the **OK** button to save the changes. New *View* will be created in the SecurOS *Object tree*.
4. To populate created *View* with *Cameras* and *Microphones* perform the *View* edit operation.

New empty *View* can also be created in SecurOS *Object tree* (see [Working with Objects](#)).

To create *View* on the base of existing *View* do the following:

1. Enter the edit mode.
2. In the *Views List* select a *View* that must be edited and click it. Selected *View* will be displayed on the *Media Client's Working area*.
3. Perform the **Edit View** operation (see below).



4. To save new created *View* click the button.

To edit *View* do the following:

1. Enter the edit mode.
2. In the *Views List* select a *View* that must be edited and click it. Selected *View* will be displayed on the *Media Client's Working area*.
3. Select required *Layout* in the *Layout panel* and click it to use.
4. To place *Camera* in the *View* click required *Camera* in the *Object List* and, holding the button pressed, drag it to the required cell of the *Layout*.
5. To place *Microphone* in the *View* click required *Microphone* in the *Object List* and, holding the button pressed, drag it to the required position of the of the *Microphone Panel*.
6. To change current *Camera* position click required *Camera* and holding mouse button pressed move it to the required cell of the *Layout*.
7. To change current *Microphone* position on the *Microphone Panel* click required *Microphone* and, holding the button pressed, drag it to the required position on the *Panel*.
8. To delete *Camera* or *Microphone* from the *View* click required object and, holding the button pressed, drag the object from the *View* to the *Object List*.



9. Click the button to save the changes.
10. To exit edit mode click the button (see Figure 135) again and select the **Exit Views Setup** command. If there are unsaved changes system will display an informational message (see Figure 137).

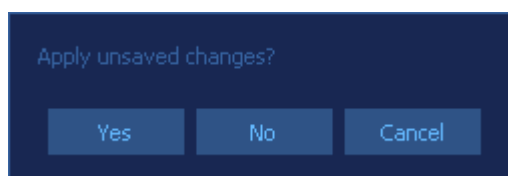


Figure 137. Informational message about unsaved changes

To save changes click the **Yes** button, to discard changes click the **No** button.

Note. Changes of the shared *View* performed and saved on any *Media Client* are automatically applied to all *Media Clients* that use given *View*.



To **rename View** select required *View* in the edit mode, click the button, then in the **Saving as** window specify a new name. One can also rename a *View* in the SecurOS *Object tree* (see **Working with Objects**).



To **delete View** select required *View* in the *Views* edit mode, then click the button. *View* can also be deleted in the SecurOS *Object tree* (see **Working with Objects**).

To add *View* to the *Views quick access bar* click required *View* in the *Views List* and, holding the button pressed, drag it to the *Views quick access bar* (see Figure 138).



Figure 138. Adding View to the Quick Access Bar

Note. Current position of the *View* in the *Views quick access bar* will be marked with white vertical stroke.

To delete *View* from the *Views quick access bar* click required *View* in the *Views List* and, holding the button pressed, drag it to the right part of the *Media Client* (see Figure 139).

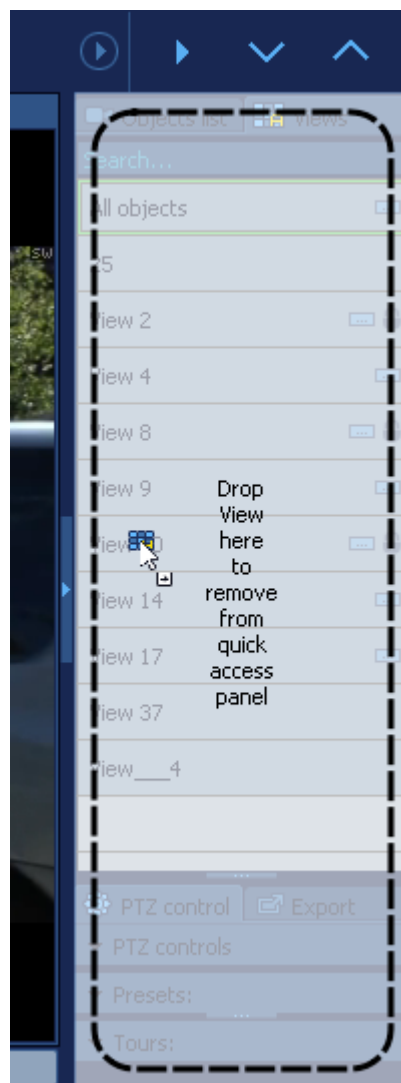


Figure 139. Deleting View from the Quick Access Bar

To setup *Views quick access bar* with the help of context menu do the following:

- 1. Right click the *View* button on the bar or empty area of the bar.
- 2. System will display context menu. List of available commands will depend on selected option (see step 1) and current state of the bar. For example, if there are several *Views* placed in bar and context menu is called for *View* button, it will contain full set of available commands (see Figure 140).



Figure 140. Views Quick Access Bar Context Menu

- 3. To select required command click it.

Note. If context menu is called for *View* context menu commands are applied to the currently selected *View*. For example, when executing the **Hide right** command (see Figure 140) all *Views* on the right of current *View* 8 will be deleted from the bar.

7.7.2.3 Archive Converter Dialog

This is an interface object used to manage the remote server's video conversions to AVI and ASF format as well as to get information about the conversion statuses (see [SecurOS User Guide](#)).

Parent object – [Desktop](#).

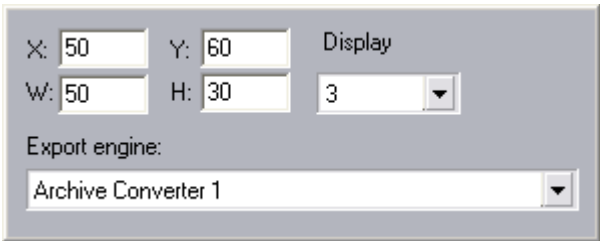


Figure 141. Archive Converter Dialog object settings window

Table 45. Archive Converter Dialog 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	Select ID of the physical display this object belongs to.
Export engine	Choose previously created <i>Archive Converter</i> object from the list.

7.7.2.4 Archiver Dialog

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

This object is used to manage the video archiving done by the Archiver object. This object is also responsible for getting information (logs) about the archiving statuses.

Parent object – Desktop.

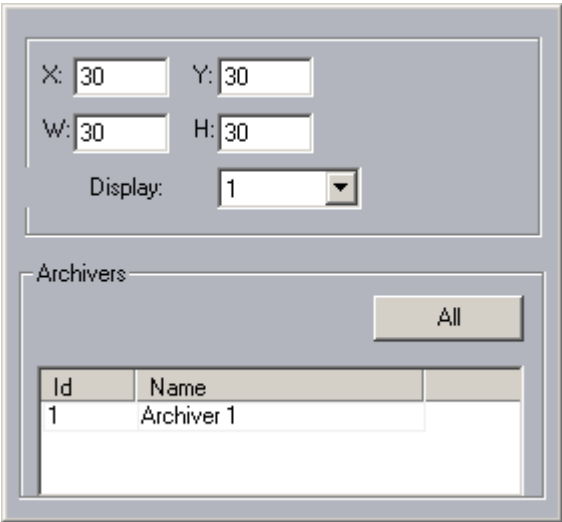


Figure 142. Archiver Dialog object settings window

Table 46. Archiver Dialog 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	Select ID of the physical display this object belongs to.
Archivers (list of Archiver objects).	
All	Click this button to populate the table with all accessible Archiver objects within the SecurOS security network.
Id	Select the ID of an Archiver object.
Name	Select the name of an Archiver object.

7.8 Configuration Examples

This section includes examples of how to setup typical configurations.

7.8.1 Standalone Configuration

Original objective: a single computer with one TVISS-4MX1 (single-chip) video capture card and two CCTV cameras connected to it. Computer should be used not only to capture and record video, but to monitor cameras also.

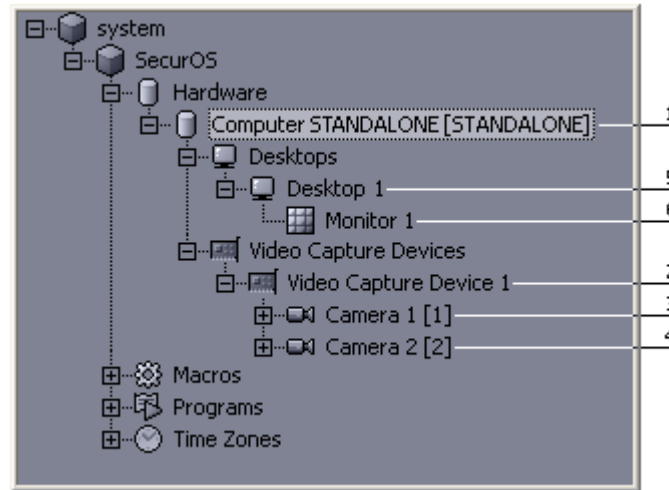


Figure 143. Object tree for standalone configuration

Solution: (see figure 143):

1. Open *Computer* object settings window (see [Editing Object's Settings](#) section) and for at least one hard drive in the **Archive** table (for example, for C:\) set **Video** parameter to Read/Write and **Computer's role** parameter to Video Server.
2. Create *Video Capture Device* object (see [Creating Objects](#)).
3. Create *Camera* object with the following parameter:
 - **Channel number** – set the actual number of the labeled BNC connector the first camera is attached to.
4. Create second *Camera* object with the following parameter:
 - **Channel number** – set the actual number of the labeled BNC connector the second camera is attached to.
5. Create *Desktop* object.
6. Create *Monitor* object. In its settings window click the **All** button to assign all cameras to this monitor and set the following parameters:
 - **X** – 0.
 - **Y** – 0.
 - **W** – 100.
 - **H** – 100.
7. Exit administration mode.

Now you will see a full-screen monitor with live video from two cameras.

7.8.2 Video Server + Operator Workstation

Original objective: a video server with one TVISS-16MX4 (2 chips) video capture card and two CCTV cameras connected to it; each camera uses its own chip for better performance. One separate operator workstation to monitor cameras (see figure 144).

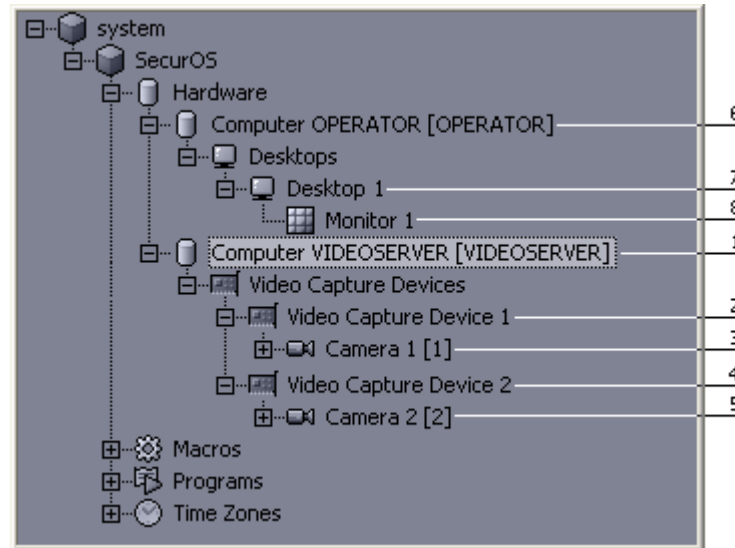


Figure 144. Object tree for server-workstation configuration

Solution: (see figure 144):

1. Open *Computer* object settings window (see [Editing Object's Settings](#) section) and for at least one hard drive in the **Archive** table (for example, for C:\) set **Video** parameter to Read/Write and **Computer's role** parameter to Video Server.
2. Create *Video Capture Device* object (see [Creating Objects](#)).
3. Create *Camera* object with the following parameter:
 - **Channel number** – set the actual number of the labeled BNC connector the first camera is attached to.
4. Create second *Video Capture Device* object with the parameter:
 - **PCI channel** – 01 (unique PCI channel number).
5. Create second *Camera* object with the following parameter:
 - **Channel number** – set the actual number of the labeled BNC connector the second camera is attached to.
6. Create *Computer* object with identifier (ID) equal to NetBIOS name of computer to be used as a workstation, and set the following parameter:
 - **IP address** – IP address or DNS/WINS name of the computer within the local TCP/IP network;
 - **Computer's role** – set to Operator workstation value.
7. Create *Desktop* object.
8. Create *Monitor* object. In its settings window click **All** button to assign all cameras to this monitor and set the following parameters:
 - **X** – 0.
 - **Y** – 0.
 - **W** – 100.
 - **H** – 100.

9. Launch the SecurOS client on the operator workstation and specify the video server IP address (or DNS/WINS name) when prompted.

When client has started, you will see on its display a full-screen monitor with live video from two server-side cameras.

7.8.3 Setting Up Camera

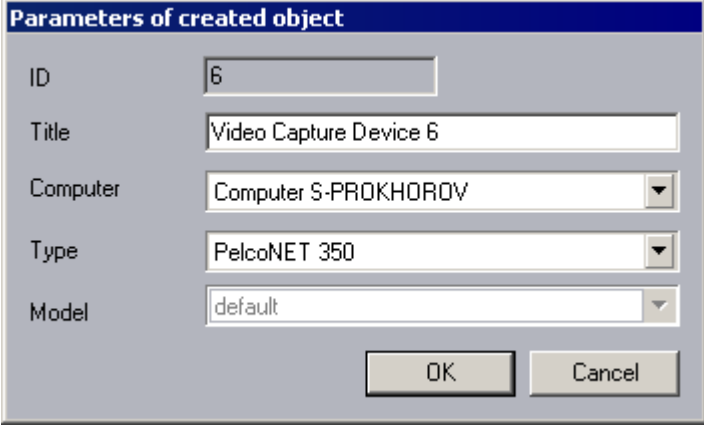
Setting up a camera includes the following operations:

1. **Adding Video Capture Device.**
2. **Adding Camera to System.**
3. **Adding Camera to Monitor.**
4. **Adding User Rights.**
5. **Setting up telemetry.**

7.8.3.1 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 a *Video Capture Device* child object.
4. In the **Parameters of created object** window (see figure 145) set the required values.

A screenshot of a dialog box titled "Parameters of created object". It contains five input fields: "ID" with the value "6", "Title" with "Video Capture Device 6", "Computer" with a dropdown menu showing "Computer S-PROKHOROV", "Type" with a dropdown menu showing "PelcoNET 350", and "Model" with a dropdown menu showing "default". At the bottom right are "OK" and "Cancel" buttons.

Parameters of created object	
ID	6
Title	Video Capture Device 6
Computer	Computer S-PROKHOROV
Type	PelcoNET 350
Model	default

Figure 145. Parameters of created object

5. In the object properties window (see figure 146) set the required values.

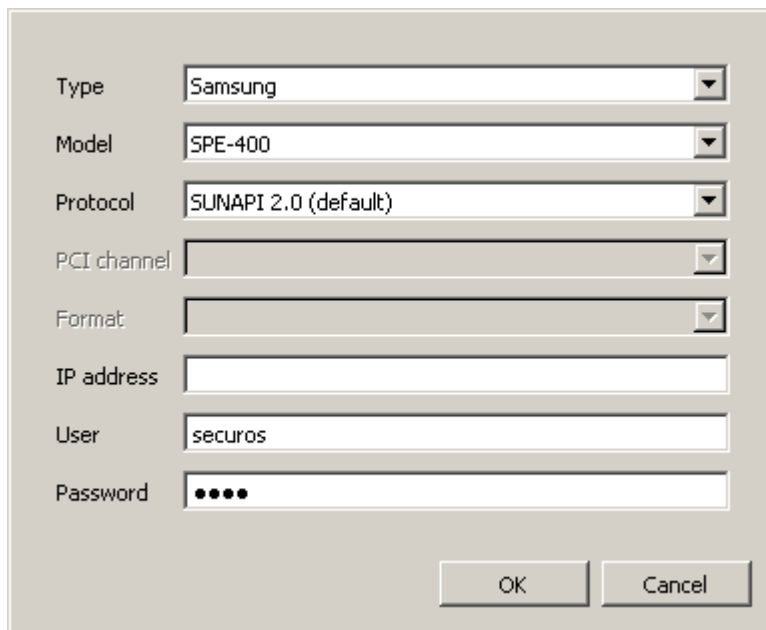


Figure 146. The Video Capture Device object properties window

6. Apply new settings.

7.8.3.2 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 (see figure 147) set the required values.



Figure 147. Parameters of created object

5. In the object properties window (see figure 148) 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.

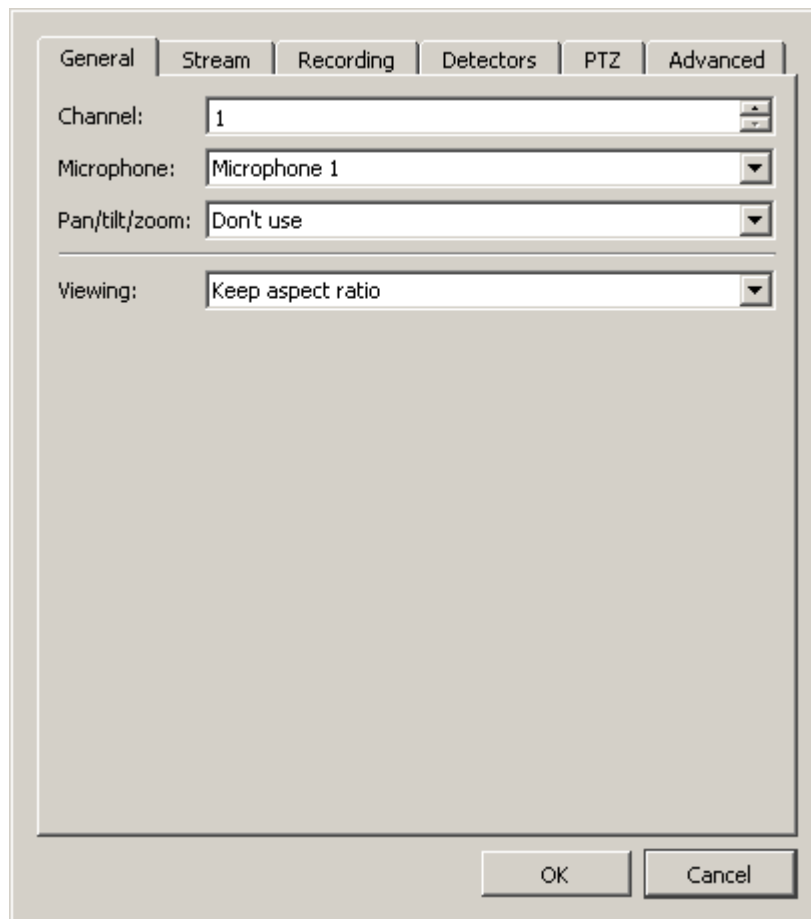


Figure 148. The Camera object properties window

6. Apply new settings.

7.8.3.3 Adding Camera to Monitor

To display video from the added camera in the *Monitor* cell do the following:

1. Enter the Administration Mode.
2. In the *Object Tree* select the *Monitor* on which it is necessary to add the *Camera* (**Security Zone → Hardware group → Computer → Desktops group → Desktop → Monitor**).
3. Open the *Monitor* object settings window.
4. Add a line in the list of displayed cameras (click the mouse on the last line and press the ↓ key on your keyboard). In the **Camera** list select the necessary *Camera* (see figure 149). If needed set the *Camera* parameters.

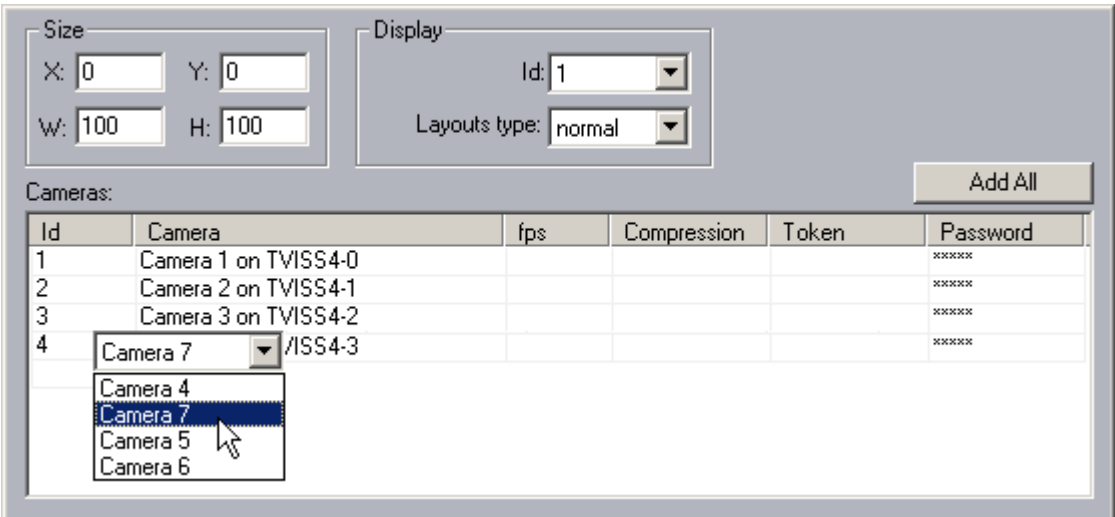


Figure 149. Monitor object settings window

5. Apply new settings.

7.8.3.4 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 the current *User Rights* for which it is necessary to grant access to control the created *Camera*.
- 3. In the User Rights settings window (see figure 150) select the *Camera* object you need, and set the required access level (using the icon on the left side of the object name).

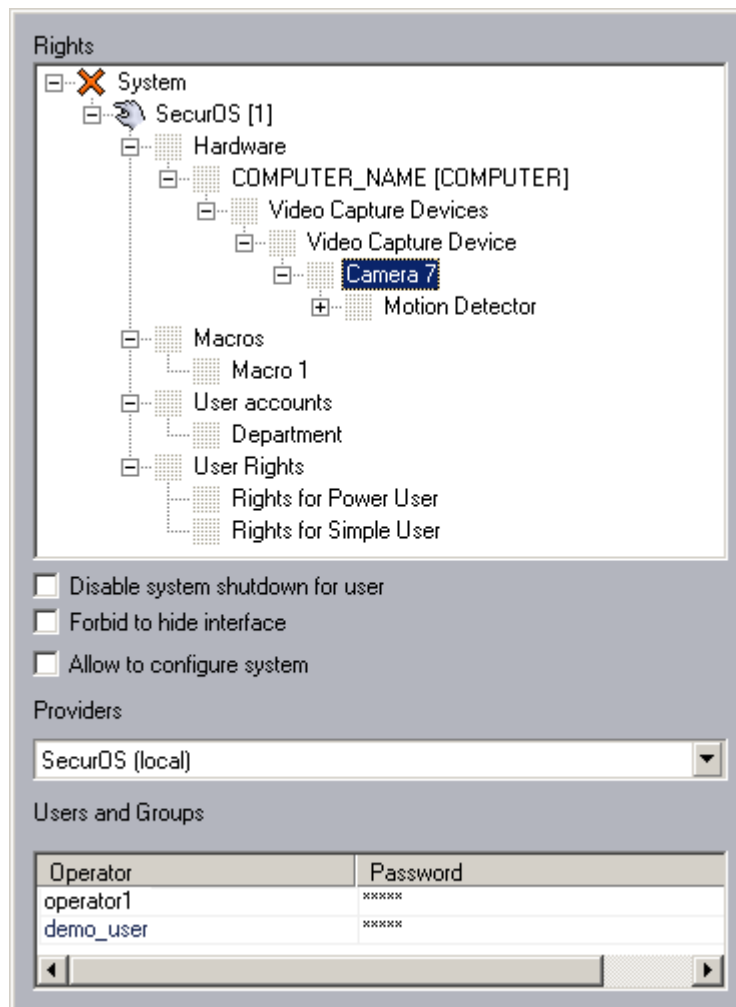


Figure 150. The User Rights object properties window

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

4. Apply new settings.

7.8.3.5 Setting up telemetry

Depending on the camera and video encoder type supporting PTZ Devices, the PTZ configuration procedures in SecurOS can be different. For most IP PTZ cameras, it is not required to create any additional PTZ Controller and PTZ Device objects. Although, for most analog PTZ cameras additional objects will need to be created.

After PTZ Device configuration, at the activation of a cell of any camera placed on the *Monitor*, the **Pan/Tilt/Zoom** button will be displayed.

When activating the controlled camera on the operator *Monitor* the *PTZ Device Control Panel* will be activated.

7.8.3.5.1 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. 151) from the **Pan/tilt/zoom** drop-down menu select the *Use* option.

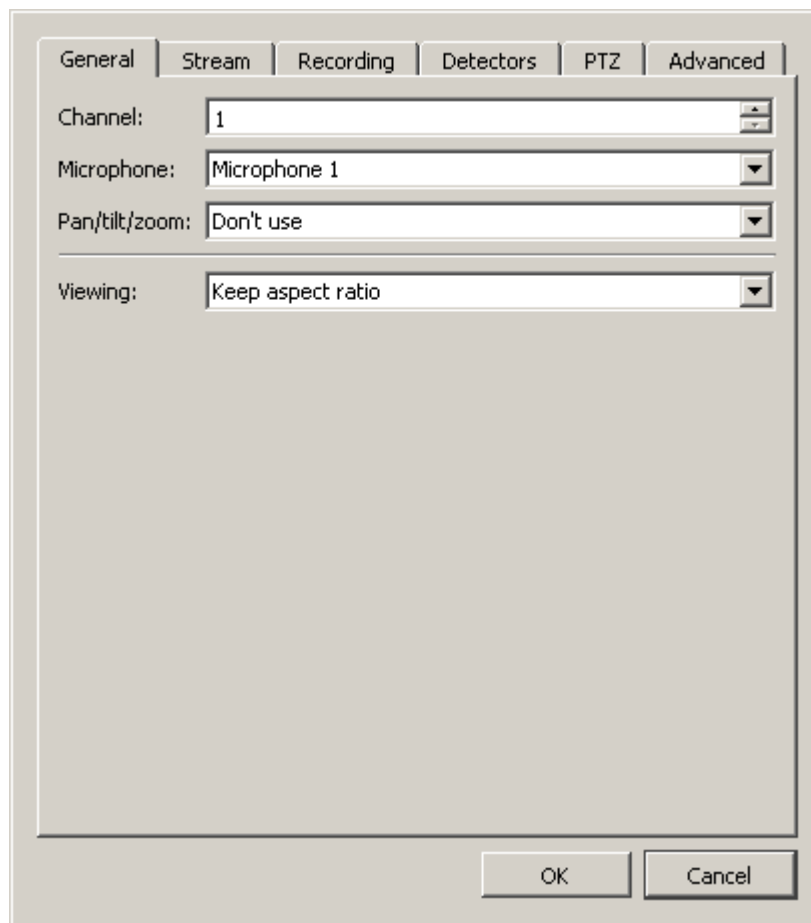


Figure 151. General tab of Camera object settings window

Note. Control of IP cameras that do not have native telemetry, can be carried out using an external PTZ controller (See Section [Setting up telemetry with PTZ Controller Creation](#)).

4. In the **PTZ** tab (see fig. 152) configure the necessary parameters.

General Stream Recording Detectors **PTZ** Advanced

PTZ protocol: PelcoD

PTZ channel: 0

☐ Disable shared PTZ control

Presets:

Identifier	Title
1	Preset 1
2	Preset 2
3	Preset 3

Tours:

Identifier	Title
1	Tour 1
2	Tour 2

Wiper: None

OK Cancel

Figure 152. PTZ tab of Camera object settings window

5. To disable shared PTZ control mode used by default, check the **Disable shared PTZ control** box (see **Exclusive Telemetry Control** section).
6. Apply new settings.

7.8.3.5.1.1 Exclusive Telemetry Control

Exclusive control mode assumes that the camera is operated in a specific mode which allows an operator to capture PTZ controls of this camera exclusively. Controlled camera can be in the object tree of any *Server* or *Operator Workstation* of the SecurOS network.

Warning! Only cameras equipped with a native PTZ device (i.e. cameras, that do not require a separate *PTZ controller* object) can be operated in exclusive control mode.

When the system is running in the exclusive control mode it:

- disables possibility to control telemetry of the given camera from all other *Servers* and *Operator Workstations* of the security network;
- resumes shared control mode if there are no commands initiated during 5 second timeout since the last command was sent from given *Computer*.

It is assumed that exclusive control mode session starts at the moment when any telemetry control command is being transmitted: turn in any direction, start/stop tour, focusing and scaling commands initiated with the help of the *Camera* control elements (not a system).

If telemetry control is captured by any user, then the system will ignore all other telemetry commands initiated by the monitor, joystick, *Macros* or *VB/JScript programs*, even if they were executed by the user who captured the controls (i.e. were sent from the same *Computer* of the security network).

When working in the exclusive control mode, the PTZ control panel of the *Monitor* and PTZ control button in the *Camera* cell are disabled for all users except for the user who captured the control.

When working in shared PTZ control mode, then:

- commands initiated by *Macros* or *VB/JScript programs* are executed;
- PTZ control is not blocked.

Telemetry control mode is configured in the *Camera* object settings window. By default PTZ device is in shared control mode. To activate exclusive control mode check the **Disable shared PTZ control** box in the **PTZ** tab (see figure 153).

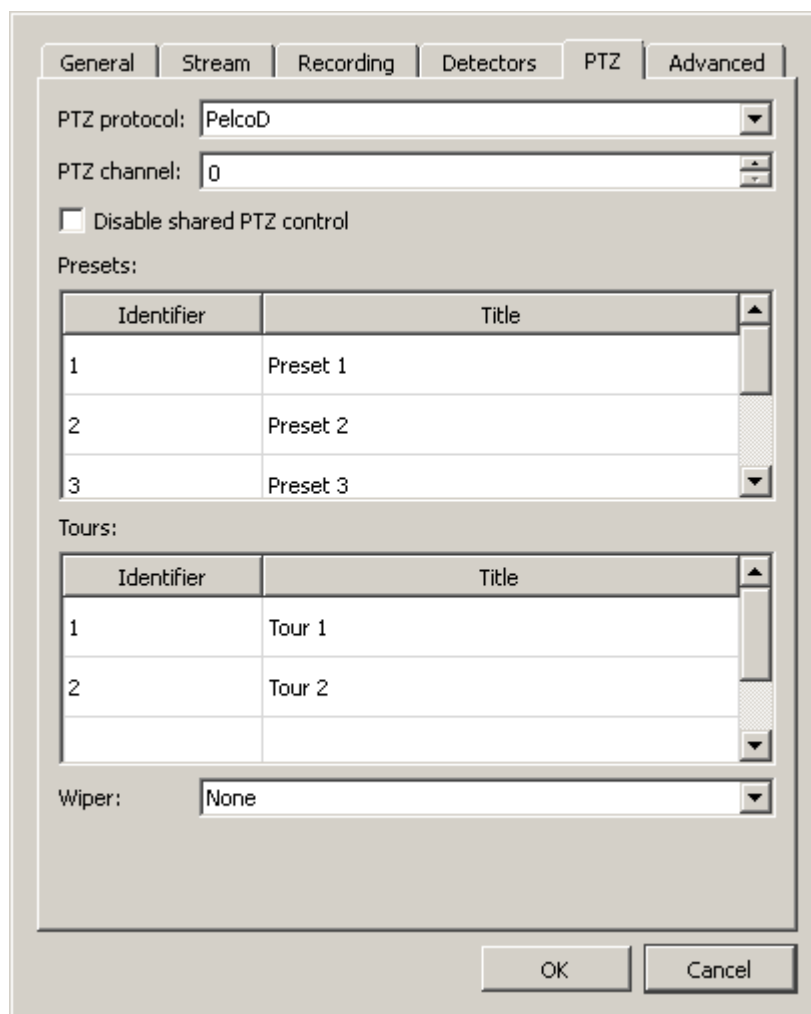


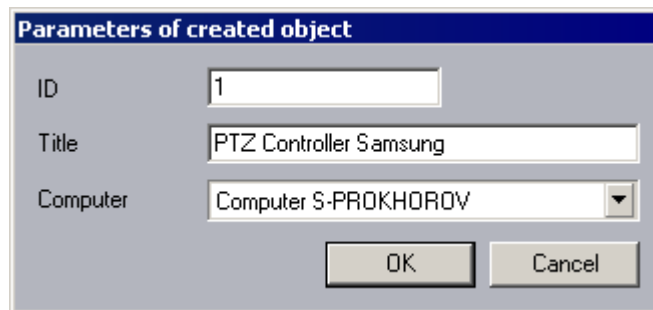
Figure 153. Camera object settings window. PTZ tab

7.8.3.5.2 Setting up telemetry with PTZ Controller Creation

Note. This method is used to configure PTZ control for all types of analog cameras and for IP cameras not equipped with a PTZ device.

To configure telemetry for such types of cameras do the following:

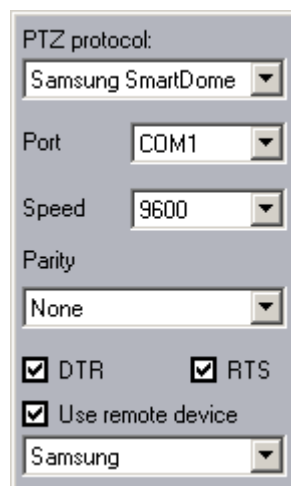
1. Enter the Administration Mode.
2. In the SecurOS *Object Tree*, under the selected *Computer*, create a *Video Capture Device* child object with a child *Camera* object.
3. Create for the current *Computer* object a *PTZ Controller* child object.
4. In the **Parameters of created object** window (see figure 154) set the required values.



The 'Parameters of created object' window shows the following fields: ID (1), Title (PTZ Controller Samsung), and Computer (Computer S-PROKHOROV). The OK and Cancel buttons are at the bottom right.

Figure 154. Parameters of created object

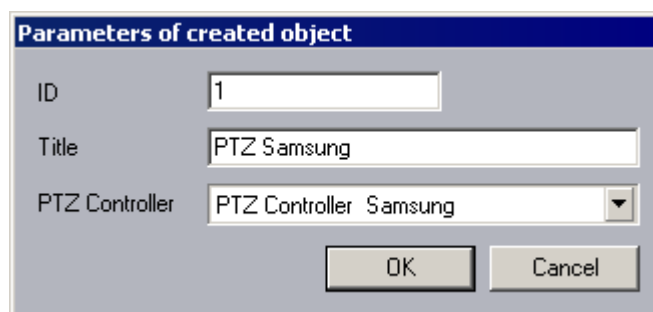
5. In the **PTZ Controller object settings** window (see figure 155) from the drop-down list select the required **PTZ protocol**; choose the **Use remote device** checkbox; from the drop-down list select the video capture device associated with the camera that will be controlled by the PTZ device.



The 'PTZ controller object settings' window shows the following settings: PTZ protocol (Samsung SmartDome), Port (COM1), Speed (9600), Parity (None), DTR (checked), RTS (checked), Use remote device (checked), and a video capture device dropdown (Samsung).

Figure 155. PTZ controller object settings window

6. In the *Object Tree* select the previously created *PTZ Controller* object, and create a *PTZ Device* child object for it.
7. In the **Parameters of created object** window (see figure 156) set the required values.



The 'Parameters of created object' window shows the following fields: ID (1), Title (PTZ Samsung), and PTZ Controller (PTZ Controller Samsung). The OK and Cancel buttons are at the bottom right.

Figure 156. Parameters of created object

8. In the PTZ Device object properties window (see figure 157), if needed, set the preliminary setting of

the PTZ device allowing quickly to move the camera in one of the given fixed positions. Detailed description of the procedure of setting up presets is described in the [PTZ Device](#) section.

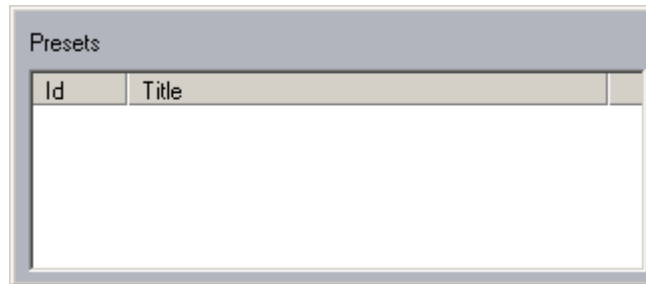


Figure 157. PTZ device object settings window

9. Apply new settings.
10. In the *Object Tree* select the *Camera* object (see [Setting Up Camera](#) section), for which it is necessary to configure PTZ Device, and enter the parameters editing mode.
11. In the **General** tab of the Camera object settings window (see fig. 158), select the previously created PTZ Device object from the **Pan/Tilt/Zoom** parameter drop-down menu.

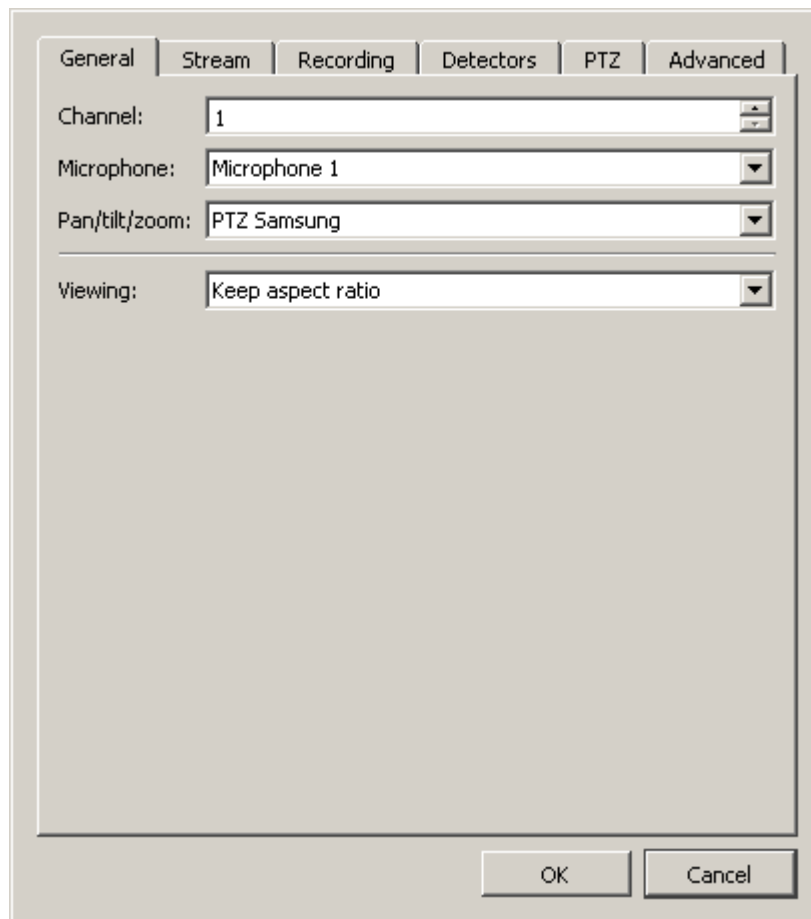


Figure 158. General tab of Camera object settings window

12. In the **PTZ** tab (see fig. 159) configure the parameters.

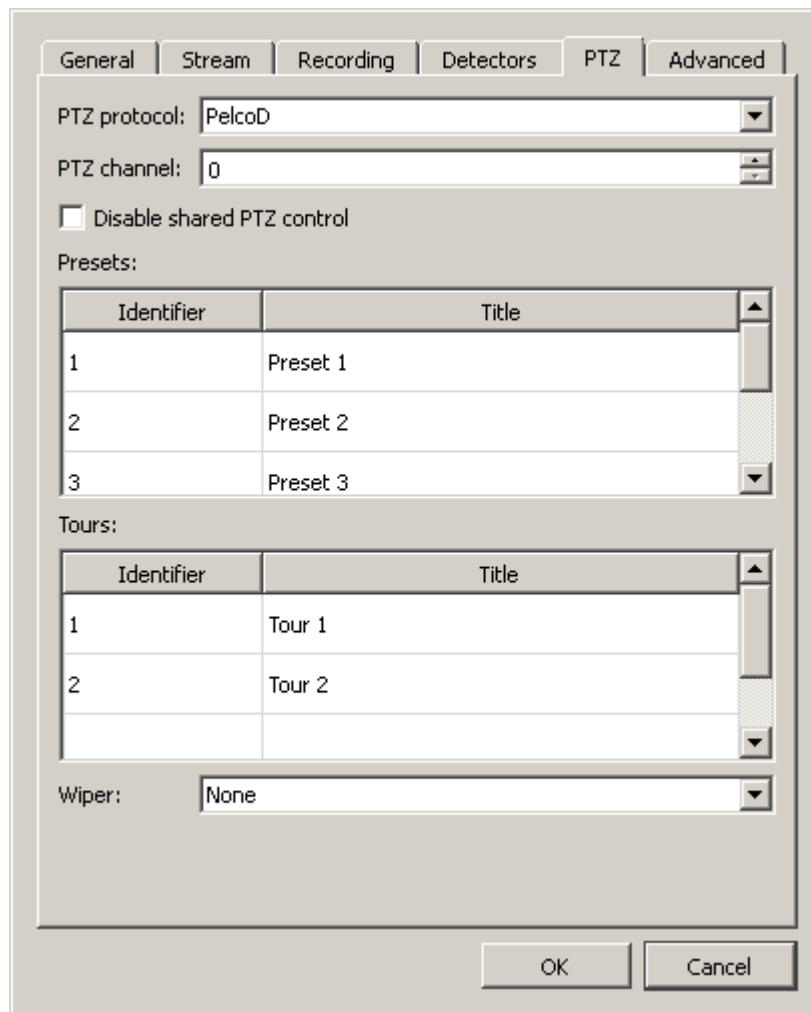


Figure 159. PTZ tab of Camera object settings window

13. Apply new settings.

7.8.4 Joystick Configuration

To use a joystick for PTZ video monitor control (see [SecurOS 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 *Monitor*'s cell (see **Monitor**), 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.

It's impossible to control synchronized recording with the help of the *Audio Player* interface object. Microphones associated to the *Camera* are displayed in the *Audio Player*'s list of available microphones in `<Microphone Name> [Microphone ID]:Camera[Camera ID]` format.

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 *Audio Player* system object is typically used.

Microphones, that can provide separate recording (i. e. that are not linked to the *Camera* object) are displayed in *Audio Player*'s list of the available microphones in the <Microphone Name> [Microphone ID] format.

8.2 Object Reference

The audio subsystem involves the following classes of objects:

- **System Objects.**
- **User Interface Objects.**

8.2.1 System Objects

The following are the system objects:

- **Audio Capture Device.**
- **Microphone.**

8.2.1.1 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;
 - sound circuits of the TVISS video capture cards;
 - microphones connected to the computer's audio inputs.
- *SoundMixer* module.

Additional Information

The *SoundMixer* module is intended for combining multiple input signals of different audio sources into a single combined output signal. Recording and further playing back of the combined signal is done with the help of the *Audio Player* interface object (see **Audio Player** section).

Parent object — **Computer.**

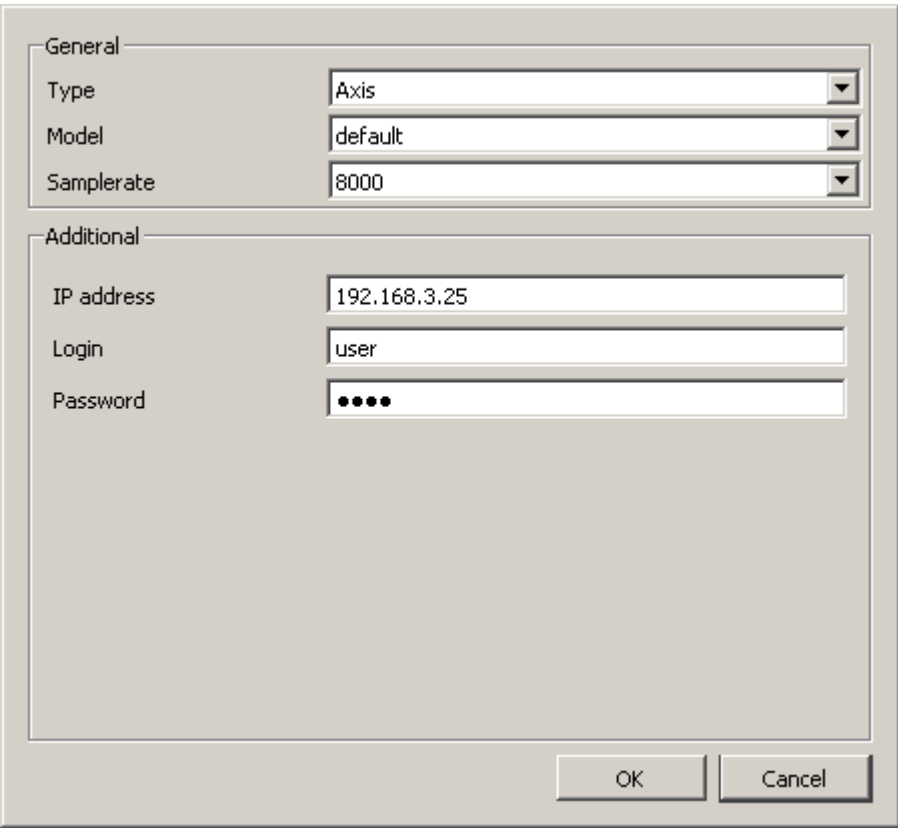


Figure 160. Audio Capture Device object settings window

Table 47. Audio Capture Device object settings

Parameter	Description
General (type independent general parameters of sound source)	
Type	Select audio source type. Mandatory parameter. Default value – "not set".
Model	Select audio source model. Mandatory parameter. Default value – "default".
Samplerate	Select audio source frequency (Hz). Mandatory parameter. Default value – min from list of available, for selected device Type . Note. The higher the samplerate the better the audio record quality, but more disk space will be required.
Additional (type dependent additional parameters of sound source)	
For IP-device	Set the following parameters (see figure 160): • IP address – IP-address of sound source in the SecurOS network. Default value is "000.000.000.000"; • 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).

Parameter	Description
For Sound Card or Sound Circuits of the TVISS Video Capture Cards	Set the following parameters (see figure 161): • PCI channel – PCI channel number to connect device. Mandatory parameter. Range of values: [1; 32]. 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>. Note. In case of some microphones are connected to the audio card only one of them can be used.
For SoundMixer module	Create a list of microphones selecting them from the available microphones in the system (see figure 162): • ID – <i>Microphone</i> object identifier; • Microphone – <i>Microphone</i> object name. Note. The list of available <i>Microphones</i> is populated with ones existing in the system already (excluding the <i>Microphones</i> which are child objects to the <i>Audio Capture Device</i> object being currently configured). At the same time the Samplerate parameter of the <i>Audio Capture Device</i> parent for such <i>Microphones</i> must be equal to 8000.

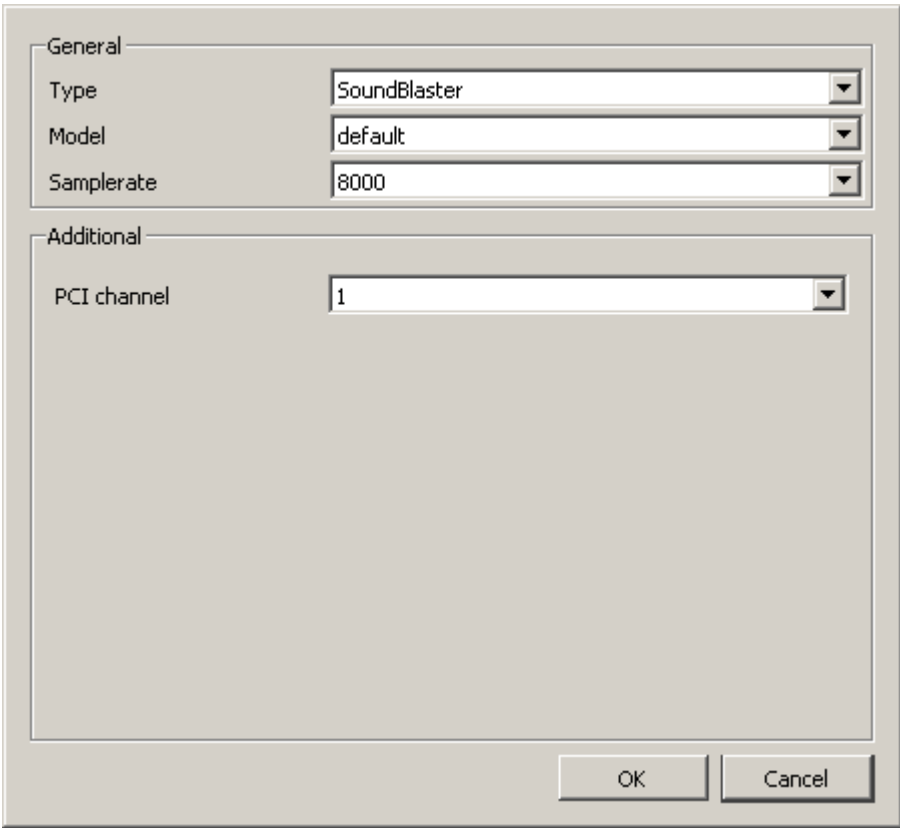


Figure 161. Sound Card or Video Capture Device Settings Window

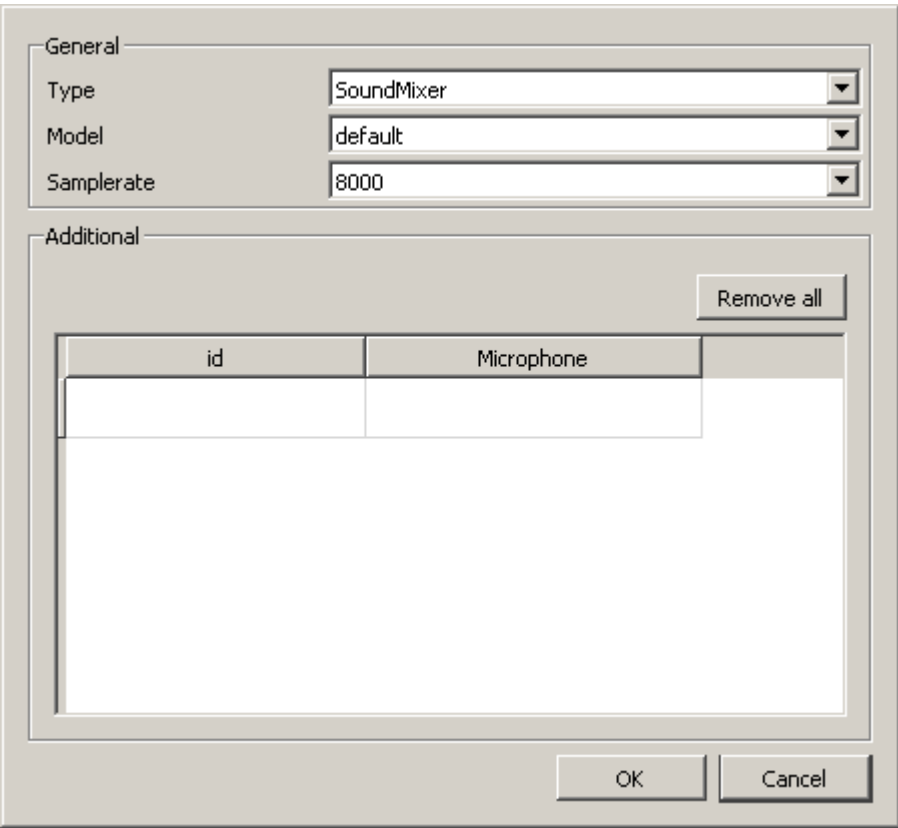


Figure 162. SoundMixer Module Settings Window

8.2.1.2 Microphone

This object represents a single mono audio channel. To record stereo signal, use two *Microphone* objects created under the same *Audio Capture Device* object and using two different channels (**Left** and **Right**).

Parent object – **Audio Capture Device**.

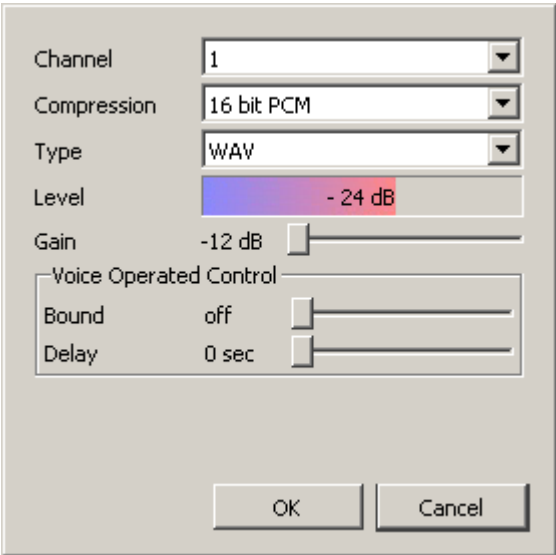


Figure 163. Microphone object settings window

Table 48. Microphone object settings

Parameter	Description
Channel	Select a channel from the list of available channels of the parent Audio Capture Device object. The same input channel can be shared between any number of <i>Microphone</i> objects. This is useful for recording audio in several formats or to several locations simultaneously.
Compression	Choose an audio compression codec. Possible values: • 16 Bit PCM— no compression, best sound quality, stream rate is 128 Kbps at 8 KHz sampling rate; • IMA ADPCM— average compression quality, good sound quality, stream rate is 32 Kbps at 8 KHz; • GSM 6.10— best compression, average sound quality (this codec is intended primarily to compress speech), stream rate is 13 Kbps at 8 KHz sample rate. Note. GSM 6.10 value is available if Samplerate parameter in the <i>Audio Capture Device</i> settings is set to 8000.
Type	Reserved for future use. Possible value— WAV.
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.
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).	
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.

8.2.2 User Interface Objects

The following are the user interface objects of the audio subsystem:

- [Audio Player](#).

8.2.2.1 Audio Player

This is an interface object used to listen to live and recorded audio from microphones (see [SecurOS User Guide](#)).

Warning! Due to system restrictions it is not allowed to create more than one *Audio Player* child object for each *Desktop* object in the SecurOS object tree.

Parent object – [Desktop](#).

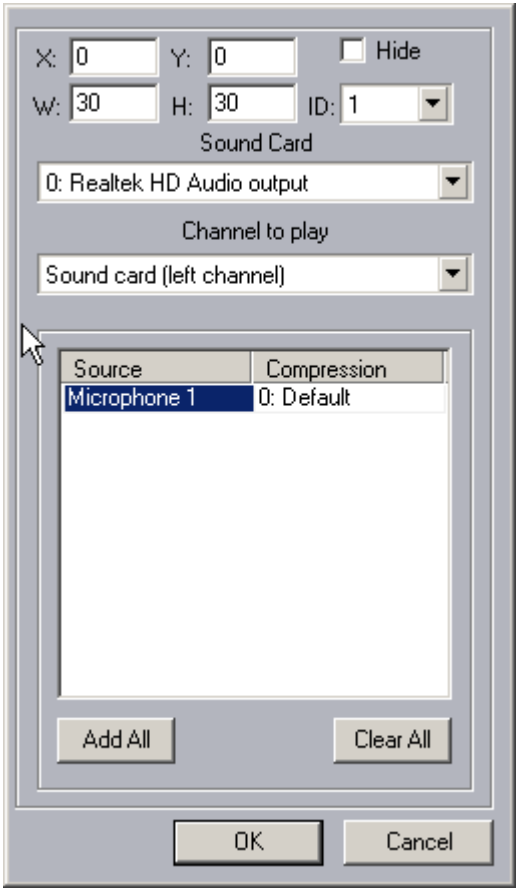


Figure 164. Audio Player object settings window

Table 49. Audio Player 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 displays' horizontal and vertical size.
Hide	Check this box to hide the <i>Audio Player</i> window when activating the parent <i>Desktop</i> . By default this box is not checked. When hide mode is enabled it is impossible to work with available <i>Microphones</i> (i.e. microphones not linked to cameras).
ID	Identifier of the physical monitor, where <i>Audio Player</i> window should be displayed. Possible values: [1 ; 16]. Default value is 1.
Sound Card	Select from the list an audio output line to the play audio files.

Parameter	Description
Channel to play	Select from the list the target channel to play audio from. You can select either mono or stereo output (stereo means pseudo-stereo: it just plays the same mono sound on both channels).
Table of audio sources (a list of registered audio sources that should be available from this audio player)	
Source	Select one or more <i>Microphone</i> object(s) from the list.
Compression	<i>Optional:</i> select the compression with which audio will be delivered from the server to the client. If the compression differs from that on the server, audio will be re-compressed on the fly. Since re-compression increases CPU load, use this parameter with caution. This option should be used if you want to store audio archive with the best possible quality (16 Bit PCM compression), but want to listen to audio compressed with either IMA ADPCM or GSM 6.10 compression, thus reducing network load at the cost of some audio quality loss. If you do not select the compression or set it to Default, live audio will be transmitted with best quality (16 Bit PCM) and archived audio will be transmitted in the original format it was saved in.
Add all	Click this button to populate the table with all the microphones within the SecurOS network.
Clear all	Click this button to clear the entire table.
OK	Save the changes and close the object settings window.
Cancel	Close object settings window without saving changes.

8.3 Example of System Configuration for Synchronized Audio/Video Recording and Playback

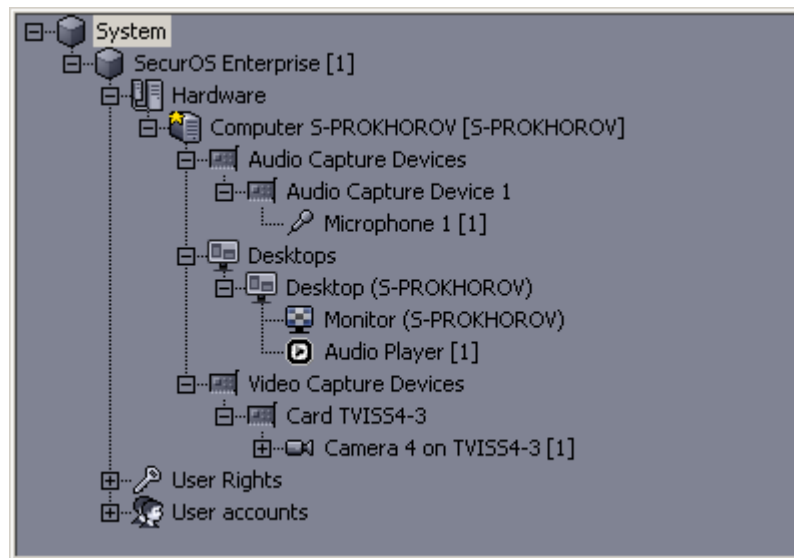


Figure 165. Object Tree for Workstation Configured for Synchronized Audio/Video Recording

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 (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. Create a *Audio Player* child object (see [Audio Player](#)) under the *Desktop* object created in the previous step. In its *Source* list, select the *Microphone* previously selected in the *Camera* object settings (see step 3).
6. If necessary create a *Monitor* object on the same *Desktop* and place the *Camera* (with linked *Microphone*) on it.

Warning! To watch live video and audio, the *Audio Player* object (with *Microphone*) and *Monitor* (with appropriate *Camera* to which this *Microphone* is linked to) object must be placed on the same *Desktop*.

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. General purpose I/O devices are connected to TVISS-4IO boards or to supported IP devices (see [SecurOS Installation Guide](#)).

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).

Note. Several *Sensor* objects within the same parent object are combined into the **Sensors** logic group in the object tree.

Parent object – **Video Capture Device.**

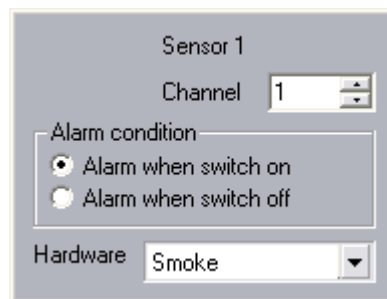


Figure 166. Sensor object settings window

Table 50. Sensor object settings

Parameter	Description
Channel	Select channel number the sensor is connected to (see SecurOS Installation Guide for more information on channel numbering).

Parameter	Description
Alarm condition	Select the type of alarm condition. Possible values: - 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 map, not its behavior).

9.1.2 Relay

This object represents a electrically operated switch (e. g. relay) that controls any device.

Note. Several Relay objects within the same parent object are combined into the **Relays** logic group in the object tree.

Parent object – **Video Capture Device**.

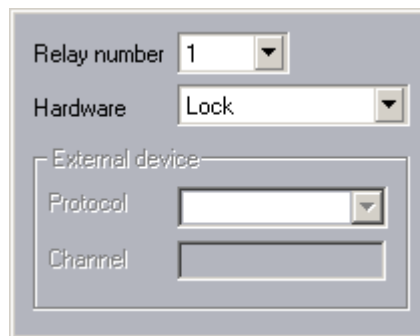


Figure 167. Relay object settings window

Table 51. 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

This object is designed to control user interface objects (for example, *Monitor*), cameras (like *PTZ devices*) and their modes, to execute operations with layouts, record operations, etc. The list of supported commands depends on the object's program realization in SecurOS.

Several *CCTV Keyboard or joystick* objects within the same parent object are combined into the **CCTV Keyboards** logical group.

Parent object – **Computer**.

SecurOS supports the following types of keyboards:

- **Bosch Intuikey**;
- **Panasonic WV-CU950**;
- **Pelco KBD300A**.

Device type is selected in the object settings window.

Warning!

1. CCTV Keyboards listed above are not USB devices.
2. CCTV joysticks supporting USB-interface are connected to the system directly, without an *CCTV Keyboard or joystick* object creation.
3. Please view `DevicesIntegrationList` for additionally supported USB joysticks.

9.1.3.1 Bosch Intuikey

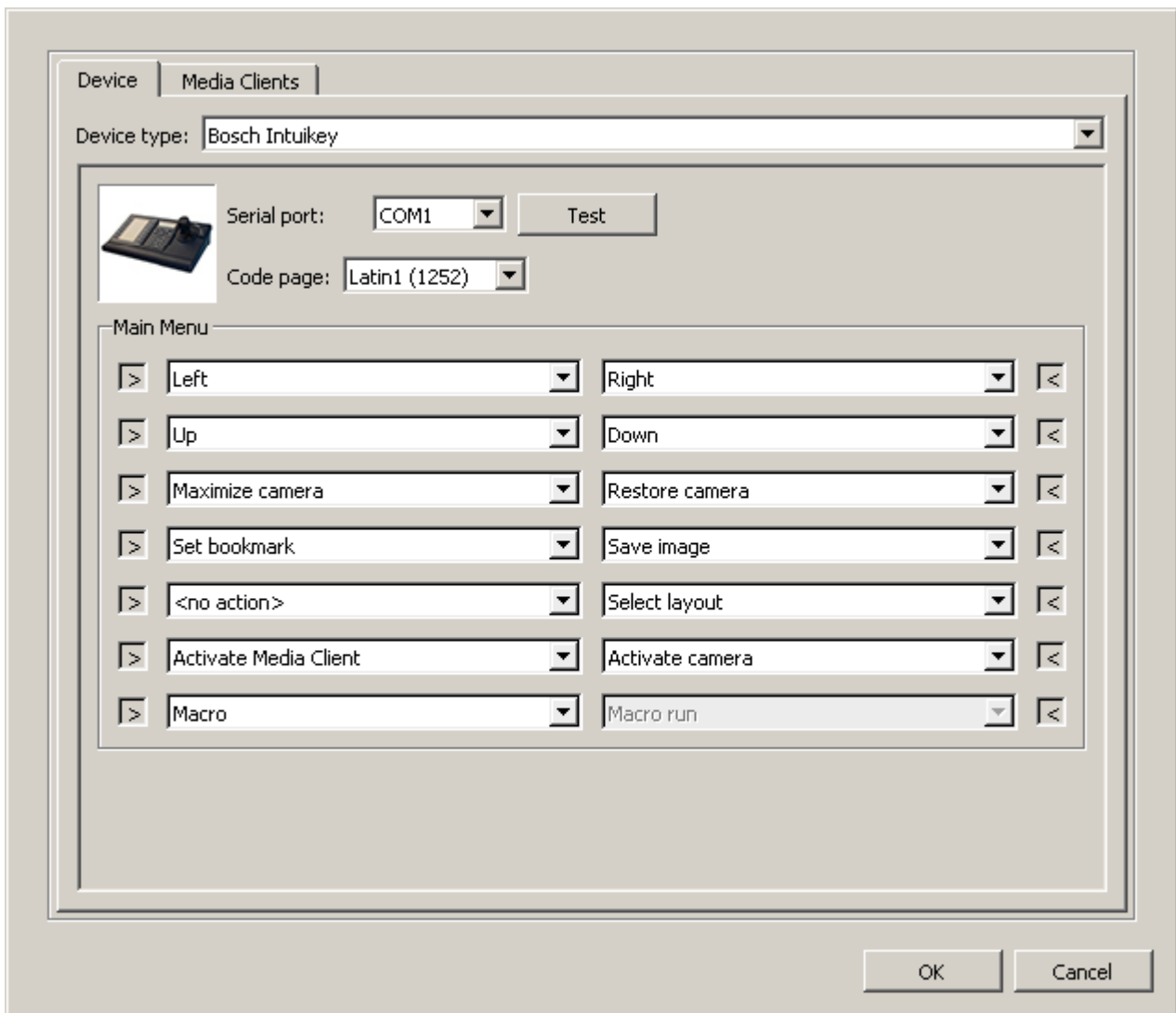


Figure 168. Bosch Intuikey object settings window

Table 52. Bosch Intuikey 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.
Code page	Code page specifying program interface language.
Main Menu	Programmable buttons and assigned actions. List is populated with SecurOS commands that are supported by the device.
OK (Cancel)	Press to save specified values and close object settings window (close object settings window without saving changes).

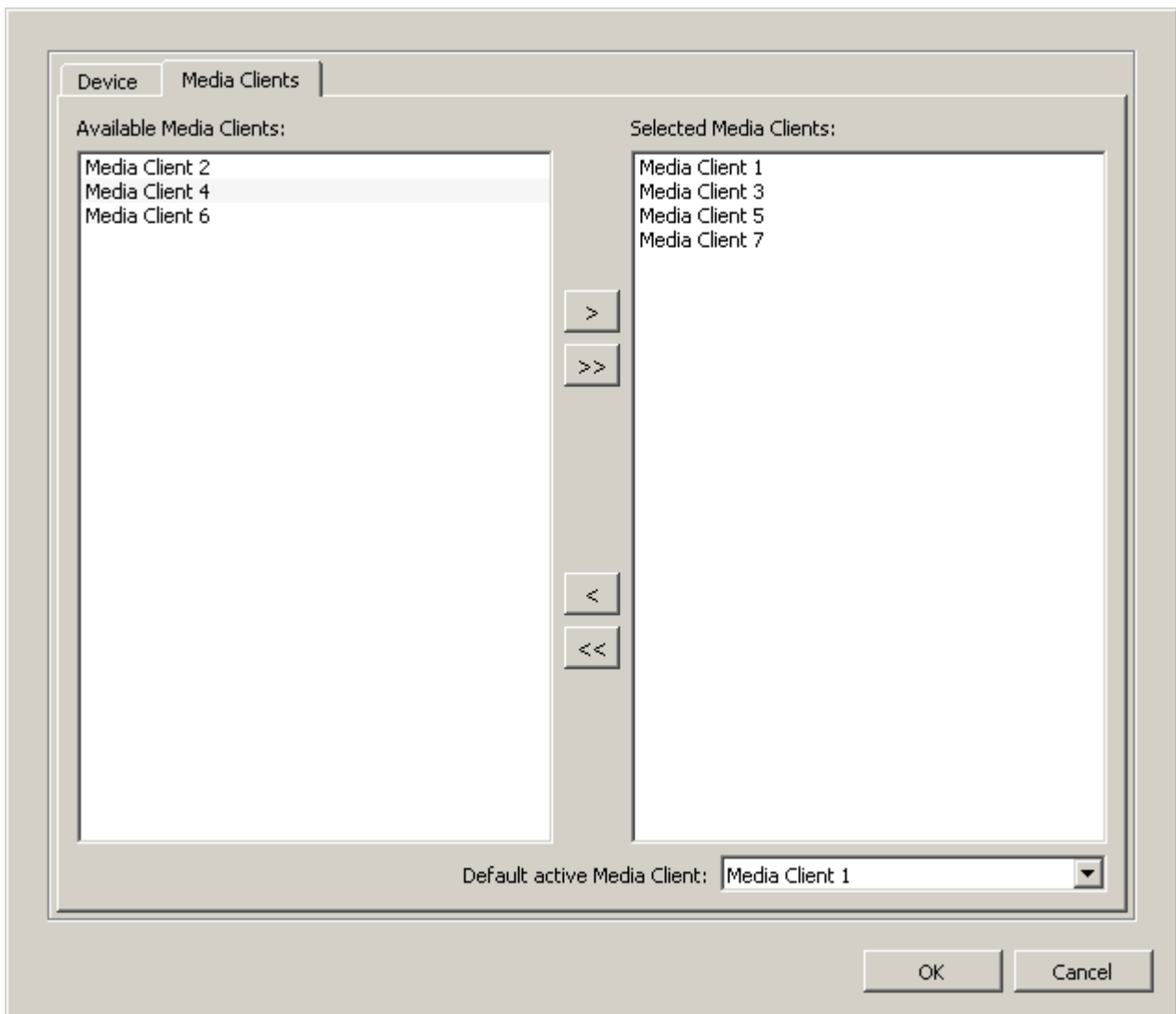


Figure 169. Device settings window. Media Clients tab

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 53. Media Clients tab

Parameter	Description
Available Media Clients	List of all <i>Media Clients</i> objects existing in the system exclude Selected Media Clients (i.e. all system <i>Media Clients</i> that can be controlled with the CCTV keyboard, but this option is not specified in the <i>CCTV Keyboard</i> or <i>joystick</i> object settings).
Selected Media Clients	List of the <i>Media Clients</i> that can be controlled with the given <i>CCTV Keyboard</i> or <i>joystick</i> object.

Parameter	Description
Default active Media Clients	<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. Note. In order to change controlled <i>Media Client</i> when working with the system simply enter it's ID (see User Manual for the appropriate <i>CCTV keyboard</i>).

9.1.3.2 Panasonic WV-CU950

Device | Media Clients

Device type: Panasonic WV-CU950

 IP address: 192.168.0.210

Functional buttons

F1	Start record	Shift-F1	Macro run
F2	Activate camera	Shift-F2	Stop record
F3	Play stored tour	Shift-F3	Stop stored tour
F4	Set bookmark	Shift-F4	Restore camera

Joystick buttons

A	<no action>	B	<no action>
---	-------------	---	-------------

Ok Cancel

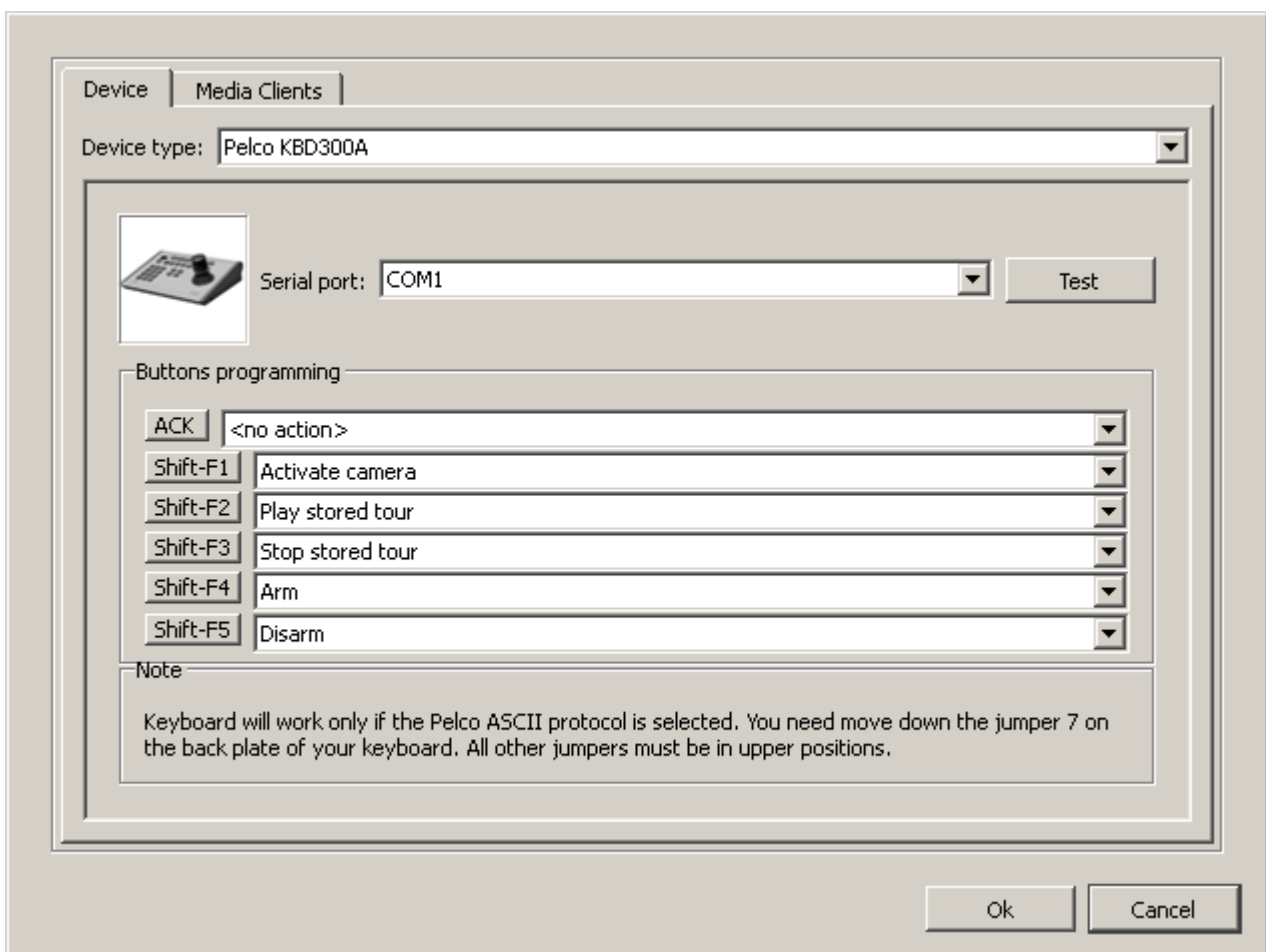
Figure 170. Panasonic WV-CU950 object settings window

Table 54. Panasonic WV-CU950 object settings

Parameter	Description
IP address	IP address of the device.
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.
OK (Cancel)	Press to save specified values and close object settings window (close object settings window without saving changes).

Media Clients tab and its actions are described in the [Bosch IntuiKey](#) section.

9.1.3.3 Pelco KBD300A

**Figure 171.** Pelco KBD300A object settings window**Table 55.** KBD300A object settings

Parameter	Description
Serial port	Serial port to connect device.

Parameter	Description
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 device.
OK (Cancel)	Press to save specified values and close object settings window (close object settings window without saving changes).

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;
- *Camera* — object settings define the *Relay* object, that is used to control the *Wiper* for the given camera;
- *Monitor* — object settings define the button display mode in the *Camera* cell.

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 window click the **Pan/Tilt/Zoom** button, then select the created *Relay* in the **Wiper** box of the PTZ device settings window;
5. Add created *Camera* to the *Monitor*. *Wiper* control button () will be displayed in the *Camera* cell by default. To hide the button select the **Disable wiper control** check box in the *Monitor* object settings window.

Note. The wiper control button displaying mode also depends on the set of access rights assigned to the user.

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:

- [E-mail Message Service](#).
- [E-mail Message](#).
- [Short Message Service](#).
- [Short Message](#).
- [Audible Notification Service](#).

10.1.1 E-mail Message Service

This object represents an SMTP service which will be used to send E-mail notifications.

Parent object – [Computer](#).

Figure 172. E-mail Message Service object settings window

Table 56. 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).

Parameter	Description
Port	Specify SMTP server port. Default value is 25.
SMTP Server 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.
Login, Password	Specify login and password for SMTP authentication.
Secure connection	
Use secure connection	Select this checkbox to enable connection via encrypted channel using the selected protocol.
Protocol	Choose the connection protocol. Possible values: Auto— default value, protocol selection depends on server setup (possible protocols: SSL 3.0, TLS 1.0). SSL— use the SSL 3.0 protocol.

10.1.2 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 173. E-mail Message object settings window

Table 57. 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.

Parameter	Description
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.
Attachment	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 Open 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.

10.1.3 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**.



Figure 174. Short Message Service object settings window

Table 58. Short Message Service object settings

Parameter	Description
Device	Select device from the list. Click Refresh button to rescan serial ports for available devices and update the list. The following phones models are compatible: Sony Ericsson (1018, J105i, K810, K790i, Z610i), Nokia (N76, N86, C5, 6120, 6300, 6555, 6700, 5130, 5310, 3500), Motorola C650, Samsung D900.

10.1.4 Short Message

This object represents an individual SMS message.

Parent object – **Short Message Service**.



Figure 175. Short Message object settings window

Table 59. 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. You can enter up to 255 symbols. Use ASCII (latin) characters only!

10.1.5 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 Object Types Database Editor**). All audio files should be placed in the `\wav` subdirectory of the SecurOS program folder.

Parent object – **Computer**.



Figure 176. Audible Notification Service object settings window

Table 60. Audible Notification Service object settings

Parameter	Description
Sound card	Select an audio output line to play the audio files through.
Channel	Select output sound channels (Left, Right, or Left+Right). Use NONE value to temporarily disable audible notifications.
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.

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 Working Principles

This section contains general information about what the automation subsystem objects are intended for.

11.1.1 Time Zones

Time zones are used to set the schedule for user access control to the security objects and zones, and to schedule system reactions to events triggered by the system.

The time zone sets the time interval when the events triggered by the program are handled by the system. When some event which is programmed to execute an alarm or any other programmed reaction happens within the limits of the time zone assigned for this program, the program behaves as it was defined. If the event falls out of this time zone, the system will show no reaction.

Example. If you select time interval from 08:00 to 22:00 and specify Monday and Wednesday as the days of week for a time zone, the event handling rules will be applied from 08:00 to 22:00 on Mondays and Wednesdays starting from the date you set as a start date, and within the number of days you specified.

Note. If no time zones are defined, you can select only Always or Never options or any reaction triggered by the program to be shown by the system.

11.1.2 Macros

Macros are used to define the links between the events and system actions. Every system object has its own set of events, and you can use visual tools to select the system reactions for them. These definitions are stored as a special system object called *Macro*.

11.1.3 Scripting

SecurOS provides the scripting language that can be used to describe and program complex scenarios. In these scenarios, you can define the system behavior for some specific cases or just set the system reactions to the events triggered by SecurOS objects. You can use scripting tools for any physical or virtual system object, for example, camera, desktop or reader.

Writing scripts is described in the [SecurOS Programming Guide](#).

11.1.4 Integration with 3rd Party Systems

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 objects (see [IIDK Manual](#)).

11.2 Object Reference

Automation subsystem includes the following objects:

- **Time Zone.**
- **Macro.**
- **Program.**
- **VB/JScript program.**
- **IIDK Interface.**
- **HTTP Event Gate.**

11.2.1 Time Zone

This object represents a time schedule and is used to define activity time for macros and programs. For each time zone specify time intervals, days of week, single dates and periods at which certain actions of macros and scripts will be executed. Time zone rules will be active for the specified days.

Note. Several *Time Zone* objects within the same parent object are combined into the **Time Zones** logic group in the object tree.

Parent object – **Security Zone**.

Days of week		Time intervals	
☒ Mon	☐ Tue	From	To
☒ Wed	☐ Thu	12:00	18:30
☒ Fri	☐ Sat	10:00	19:00
☐ Sun			
☐ Holidays			

Date: 2/ 2/2001 Period: [dropdown] days

Figure 177. Time Zone object settings window

Table 61. Time Zone object settings

Parameter	Description
Time intervals	Fill in the table of time intervals within a day (From , To). Last minute of the interval is included into the interval. Time should be specified in the HH:MM format. The number of time intervals is not limited. Time intervals may overlap, but this is generally not recommended. For each interval, dates or periods of execution are chosen (see below).
Days of week	Select days of week on which specified time intervals are active (logical AND operation is used between days and time intervals with a day). Note that by default none of the days are selected and the time zone is not active.
Holidays	Check this option to make the selected time interval of the <i>Time zone</i> active on dates defined as "holidays" within the <i>Security Zone</i> object settings (see Security Zone). If Days of week or Date, Period are not set then selected time interval will be active only on Holidays . If they are selected, rules of Time Zone will be active both on Holidays and the schedule defined within the time zone (Days of week or Date, Period).
Date, Period	Enable Date field and select start date to make the time zone correspond not to days of the week, but to single repeating days with period of any length. Specify period in Period field (in days). This means that time zone will be active every single N-th day starting from the specified date. Note. To make more complex time schedules like two active days followed by two inactive, you should create several <i>Time Zone</i> objects and specify the same period but shifted start dates.

11.2.2 Macro

Used to define SecurOS system behavior by catching specific system events and generating custom reactions for those events.

Note. Several *Macro* objects within the same parent object are combined into the **Macros** logic group in the object tree.

Parent object – [Security Zone](#).

The figure shows a 'Macro object settings' window. It contains two main sections: 'Event' and 'Actions'.

Event Section: At the top right, there are two checkboxes: 'Local' and 'Hidden'. Below them is a table with the following data:

Type	Id	Title	Event
Camera	1	Camera 4 on TVISS4-3	Alarm

Actions Section: Below the 'Event' section is a table with the following data:

Type	Id	Title	Action	Parameters
Camera	1	Camera 4 on TVISS4-3	Start record	

Figure 178. Macro object settings window

Table 62. 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.
Hidden	Select 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 video server, administrator workstations or operator workstations 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 omit ID to refer to any objects of the specified type within the security network.
Title	<i>Information field:</i> title 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. Omit this field to refer to any events of this 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.

Parameter	Description
Id	Choose object ID. You can omit ID to refer to any objects of the specified type within the security network.
Title	<i>Information field:</i> title 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.
Parameters	Parameters of the selected action. Parameters are set as a string, maximum length – 255 symbols. The string format is similar to the program parameter one, see VB/JScript program .

11.2.3 Program

Warning! This object is deprecated. Use the **VB/JScript program** object to create automation scripts.

Used to define programs (scripts) to help automate and customize SecurOS.

Note. Several *Program* objects within the same parent object are combined into the **Programs** logic group in the Object Tree.

Parent object – **Security Zone**.

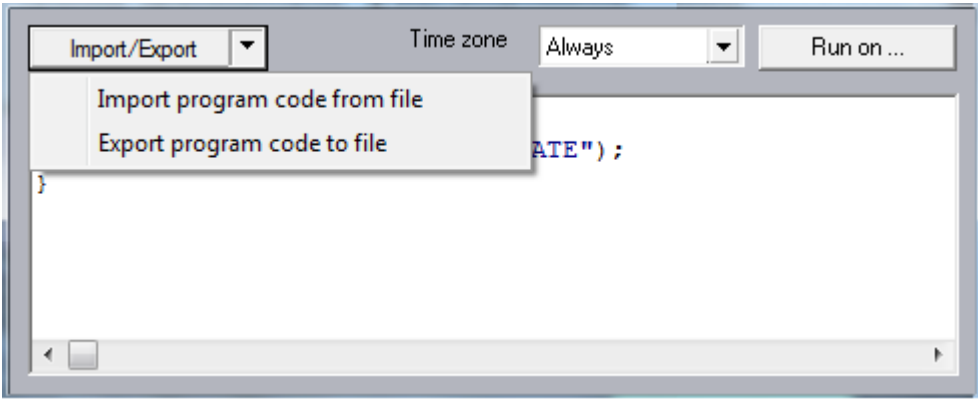


Figure 179. Program object settings window

Table 63. Program object settings

Parameter	Description
Time Zone	Select <i>Time Zone</i> (see Time Zone section) object from the list to specify the time period(s) when this script is active (if selected time zone is inactive the script does not operate). <i>Never</i> (never operate) or <i>Always</i> (always operate) also can be selected as the time zone value.
Run on	Click this button to open a dialog, where you can setup, on what particular computers of the parent Security Zone this script will run on. By default, the script is executed simultaneously on all servers of the security zone.

Parameter	Description
Import/Export	Click the button and choose the required action from the drop-down list: Import program code from file — to load code from file; Export program code to file — to save code copy to file. File name format is <program_id>.nis.
Script text area	Fill in the text area with the script body itself. Warning! Script size should not exceed 4 MB.

The text of a removed program can be restored. To restore the program do the following:

1. Export program code to a file before deleting the *Program* object.
2. Import program code from file into a new Program object.

Warning! **Time Zone** and **Run on** parameter values of the deleted object are not saved and cannot be restored!

11.2.4 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](#)).

Parent object — *VB/JScript programs*.

Note. Parent to the *VB/JScript programs* is the **Computer** object.

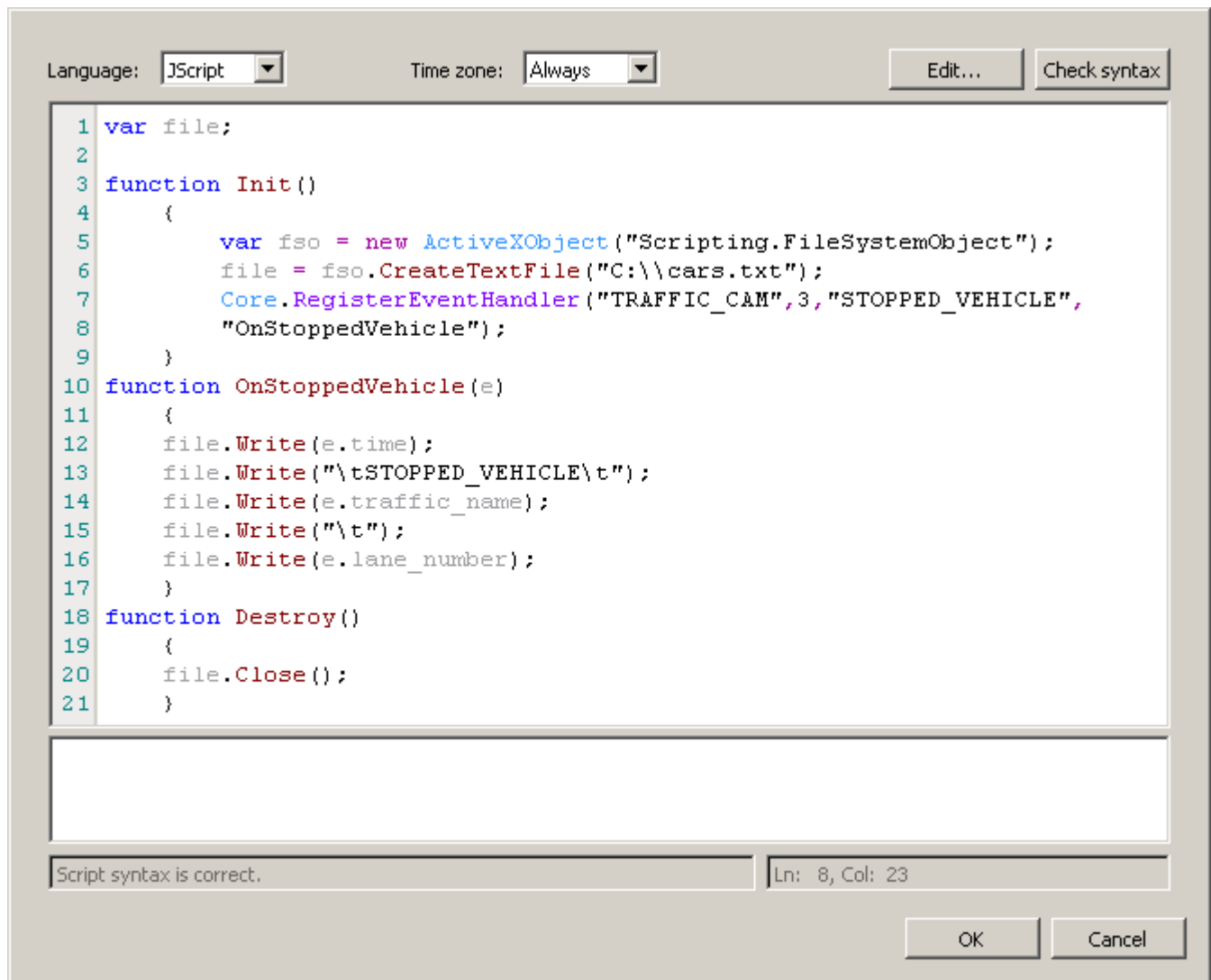


Figure 180. VB/JavaScript program object settings window

To create and configure a *VB/JavaScript program* object do the following:

1. Enter the Administration Mode.
2. In the SecurOS Object Tree select or create the *VB/JavaScript programs* object, for which create a *VB/JavaScript 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 64. VB/JavaScript program object settings

Parameter	Description
Language	Select the required programming language of the current script from the drop-down list. Possible values: • VBScript; • JScript.

Parameter	Description
Time zone	Select time zone (see Time Zone section) object from the list to specify the time period(s) when this script is active (if selected time zone is inactive the script does not operate). Time zone rules are configured in corresponding <i>Time Zone</i> object settings. Possible values: • Always — script functions anytime; • Never — script never functions; • a list of accessible <i>Time Zones</i> — script functions within chosen time zone.
Buttons	
Edit	Click this button to call an external VB/JScript editor. 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. 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.

11.2.5 IIDK Interface

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

This is a service for external connection to SecurOS via the IIDK protocol. Create this object on one or more computers that will act as IIDK servers (see **IIDK Manual** for more information).

Parent object — **Computer**.

Object has no settings to alter.

11.2.6 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**.

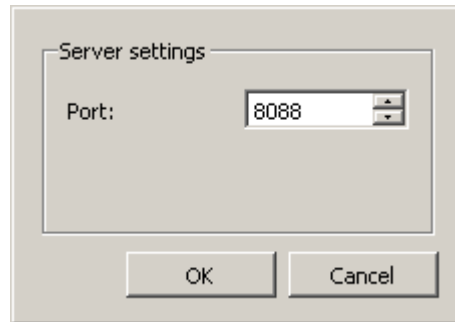


Figure 181. HTTP Event Gate object settings window

Table 65. 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.

Request syntax

`http://<video_server_IP_address>:<port>/event?<param1_name>=<param1_value>[&<param2_name>=<param2_value>[& . . . ]]`, where:

- `http://<video_server_IP_address>:<port>/event?` – URL to send a request;
 - `<video_server_IP_address>` – IP address of the SecurOS *Video Server*, where the *HTTP Event Gate* object is created;
 - `<port>` – port number of the SecurOS HTTP server, specified in the object settings;
- `<param1_name>`, `<param2_name>`, . . . – name of the parameters, which will be transmitted to the SecurOS.
- `<param1_value>`, `<param2_value>`, . . . – value of the parameters, which will be transmitted to the SecurOS.

For example, to transmit to SecurOS a license plate and coordinates of the vehicle, one should send the following request:

`http://172.16.1.41:8080/event?plate=135&latitude=57.6565&longitude=37.8787,`

or the following request to transmit a persons' name:

`http://172.16.1.41:8080/event?name=Alex`

Checking Request Correctness

To check if request is correct, send it via web browser. If the following request was sent:

`http://172.16.1.41:8080/event?plate=135&latitude=57.6565&longitude=37.8787,`

the server will return the following string in the browser window:

```
Event(HTTP_EVENT_PROXY|1|RECEIVED|_body<>,_method<GET>,_path</event>,_peer_address<::1>,_latitude<57.6565>,_longitude<37.8787>,_plate<135>) has been sent to SecurOS, where:
```

- `latitude<57.6565>,_longitude<37.8787>,_plate<135>` — parameters transmitted in the request;
- The following are SecurOS service parameters generated by the system automatically:
 - `_body<>` — text body of the POST request;
 - `_method<GET>` — HTTP method used to transmit the request. Possible values: GET or POST.
 - `_path</event>` — request path (see [Custom HTTP Requests](#)).
 - `_peer_address<::1>` — IP address of the request sender. If a request is sent from the computer, where *HTTP Event Gate* is deployed, this parameter has the value of `::1`.

SecurOS Events

If a request is correct, then a response of the HTTP server is returned in the web browser.

Thus, if the following request was sent:

`http://172.16.1.41:8080/event?plate=135&latitude=57.6565&longitude=37.8787,`

then the following event will be generated within SecurOS:

```
Event : HTTP_EVENT_PROXY 1 RECEIVED _body<>,_plate<135>,_method<GET>,_latitude<57.6565>,_path</event>,_peer_address<::1>,_longitude<37.8787>,_slave_id<S-PROKHOROV.1>,_owner<S-PROKHOROV>,_date<19-12-14>,_time<12:11:39.340>,_core_global<1>
```

Custom HTTP Requests

Besides standard HTTP requests *HTTP Event Gate* supports custom requests. The rules of the custom request processing are specified in a *VB/JavaScript program* (see [SecurOS Programming Guide](#)).

To work with custom queries within SecurOS it is necessary to do the following:

1. Specify a list of the allowed requests using a **HTTP Request Filter**.
2. Specify an individual **HTTP Request Handler** for each request, that implements the following functions:
 - preparing data for the incoming unfiltered requests (for example, data in XML format);
 - sending a response to the request with prepared data.

Configuring HTTP Request Filter

HTTP request filter is defined in the `paths.txt` file, that is stored in the `\Modules\http_event_proxy` folder of the SecurOS install directory. One line of the file corresponds to one request. If a URL of the request has a constant part and another part may vary, then you also can merge them with the help of the `*` character. For example, see listing 5.

Listing 5. Using wild card in the request filter

```
/*if requests are the following:*/

/config/user1?par1=val1&par2=val2
/config/user2?par1=val1&par2=val2
...
/config/user16?par1=val1&par2=val2

/*create the following rule in paths.txt: to merge URLs*/

/config/user*
```

Listing 6 represents a simple request filter.

Listing 6. Request filter example

```
/*If the paths.txt contains the following strings:

/get-analytics
/get-detectors
/get-state/*

/*then the allowed URLs are the following:

http://ip:port/get-analytics?par1=val1&par2=val2
http://ip:port/get-detectors
http://ip:port/get-state/linecross_detector
http://ip:port/get-state/abandoned_detector?from=26-01-14%2011:12:13
&to=26-01-14%2012:13:14
/*etc.

/*and not allowed URLs are the following:

http://ip:port/get-analytics/plates
http://ip:port/command

/*etc.*/
```

Creating HTTP Request Handler

To process custom requests the following events and commands are supported by the *HTTP Event Gate* object:

Table 66. HTTP_EVENT_PROXY Events

Event identifier: PENDING_REQUEST
Description: Incoming custom request
Parameters:

_id	Request identifier. Is used to respond to a request.
_path	Substring of the URL between :port and ?. For example, if request string is http://ip:port/path/is?param1=value1, then the /path/is substring will be the parameter value.
_method	HTTP request method. Possible values: GET/POST/DELETE.
_peer_address	IP address of the sender.
custom parameters	Custom parameters are defined by the query contents (see Request syntax).
Event identifier: RECEIVED	
Description: Incoming custom request	
Parameters:	
_path	Substring of the URL between :port and ?. For example, if request string is http://ip:port/path/is?param1=value1, then the /path/is substring will be the parameter value.
_method	HTTP request method. Possible values: GET/POST/DELETE.
_peer_address	IP address of the sender.
custom parameters	Custom parameters are defined by the query contents (see Request syntax).

Table 67. HTTP_EVENT_PROXY Commands

Command identifier: RESPONSE	
Description: Send a respond for the received request PENDING_REQUEST.	
Parameters:	
_id	Request identifier received within the PENDING_REQUEST. Required parameter.
_body	Request text body (for example, data in XML format).
_content_type	Type of the data transmitted within _body parameter. Default value is application/xml. Example of possible values: • text/plain; charset=utf-8, • application/json; charset=utf-8 etc.

Listing 7 represents a request handler.

Listing 7. Request handler

```
/*paths.txt contains the following rules:
* /get-analytics
* /get-detectors
```

```

    * /get-config/*
*/

/* SecurOS receives the following requests:
 * http://ip:port/get-analytics
 * http://ip:port/get-detectors?area=outdoor
 * http://ip:port/get-config/abandoned?area=indoor
 */

//Declare custom events handler function
function Init(){
    Core.RegisterEventHandler("HTTP_EVENT_PROXY","1","PENDING_REQUEST",
                             "fRequestHandler");
}

//Request handler
function fRequestHandler(e){
    switch(e._path){
        case "/get-analytics": fGetAnalytics(e, e._id); break;
        case "/get-detectors": fGetAnalytics(e, e._id); break;
        default:
            if( e._path.match(/get-config/ ) fGetConfig(e, e._path, e._id);
            break;
    }
}

//Response example
function fGetAnalytics(e, request_id){
    ...
    var text= "<xml><param>value</param></xml>";
    Core.DoReact("HTTP_EVENT_PROXY","1","RESPONSE","_id",request_id,
                 "_body", text);
}

function fGetAnalytics(e, id){ ... }

function fGetConfig(e, path, id){ ... }

```

Streaming via HTTP Event Gate

HTTP Event Gate provides processing of the stream data, that is transmitted into SecurOS. Any text data (for example, XML) can be transmitted. External application is sending HTTP POST request; the data is transmitted in the request body.

Example of the XML data transmission into SecurOS is shown below.

Listing 8. JScript program example to transmit XML data

```

function Init(){
    Core.RegisterEventHandler("MACRO","1.1","RUN","fSend");
    Core.RegisterEventHandler("HTTP_EVENT_PROXY","1","RECEIVED","fPrint");
}

function fSend(e){
    var HTTP = new ActiveXObject("Msxml2.ServerXMLHTTP.3.0");
    var url = "http://127.0.0.1:9050/event?id=777";
    var XML = "<root><node1>value1</node1><node2>value2</node2></root>";
    HTTP.open("POST",url,false);

```

```

HTTP.send(XML);
var response = HTTP.responseXML;
}

function fPrint(e) {
    Script.Echo(e._body);
}

```

11.3 Setting up Macros and Scripts

This section describes specifics of configuring and using the macros and programs.

11.3.1 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. Enter the Administration Mode.
2. In the SecurOS *Object Tree* create a *Macro* which is a child object of the *Security Zone* object.
3. In the **Parameters of created object** window set the required values.
4. In the object properties window (see figure 182) create the macro command description.

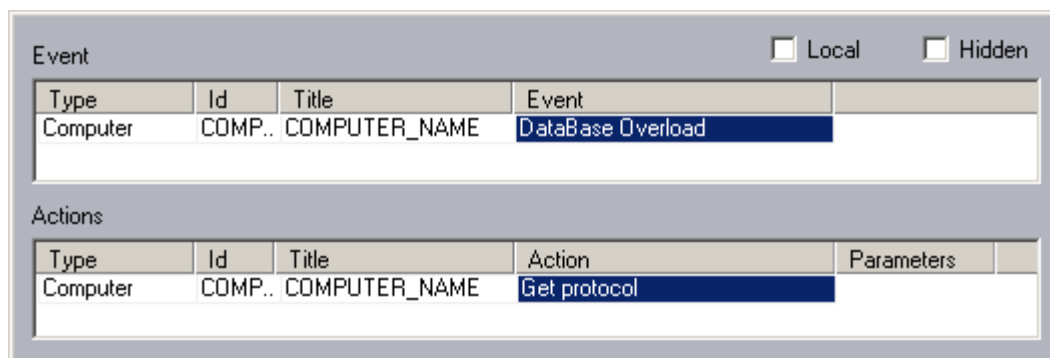


Figure 182. The object settings window

5. Apply new settings.

Buttons to execute the created *Macros* are displayed on the system Control Panel (see figure 183).

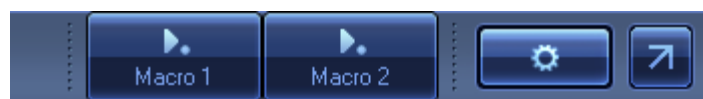


Figure 183. Control panel. Available Macros

11.3.2 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. Enter the Administration Mode.
2. In the SecurOS Object Tree select the *Computer* object, for which create a *VB/JScript programs* child object.
3. In the **Parameters of created object** window set the required values.
4. In the SecurOS Object Tree create a *VB/JScript program* object, child to created *VB/JScript programs* object.
5. In the **Parameters of created object** window set the required values.
6. In the *VB/JScript program* object properties window, type in the program code.
7. Check code syntax, correct found errors.
8. Apply new settings.

12 Light Integration

This section describes light integration of SecurOS with the external FAAC (Fire Alarm/Access Control) and radiation monitoring systems.

12.1 General Description

SecurOS allows to integrate some FAAC (Fire Alarm/Access Control) or radiation monitoring systems – **Bolid**, **FortNet** and **Yantar**. 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, FortNet or Yantar 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).

The program interface with the external system is provided by the SecurOS internal executor, that corresponds to Bolid, FortNet or Yantar 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 [Setting Up Integration](#)).

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.

12.2 Setting Up Integration

To configure integration do the following:

1. In the SecurOS object tree create the *Integration point* object (child of the [Computer](#) object):

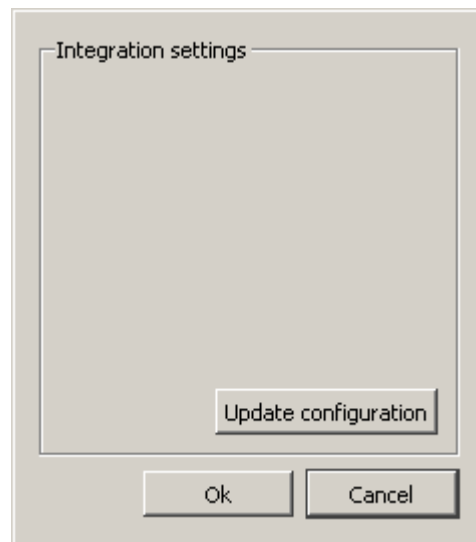


Figure 184. Integration point object settings window

2. Click the **Update configuration** button. The internal integration module receives data from the external system and builds the integration object tree (see [SecurOS Integrations](#)).
3. To complete configuration click **OK**.

12.3 SecurOS Integrations

SecurOS software distributive contains the dynamic link libraries that provide integration with the following external systems:

- **Bolid**;
- **FortNet**;
- **Yantar**.

The parent object for all integration types is **Computer**.

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;
- Yantar – Amber System - 5.2.3.

12.3.1 Bolid

Bolid integration object is used to provide integration with the FAAC (Fire Alarm/ Access Control) Bolid system:

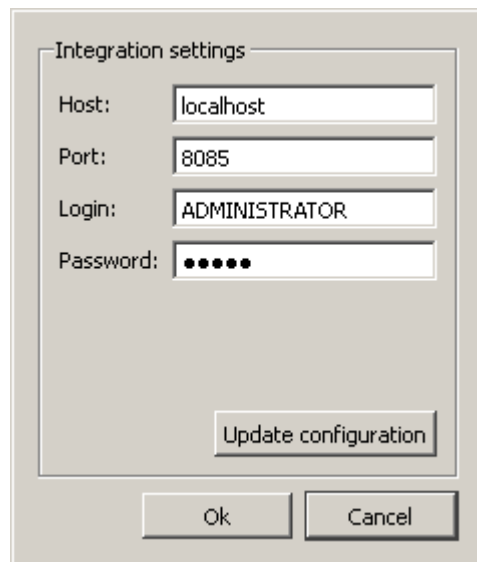


Figure 185. Bolid integration object settings window

Table 68. 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/JavaScript Programs* and *Map* object control commands. *Map* or *Event Viewer* objects are used to monitor object states.

12.3.2 FortNet

FortNet integration object is used to provide integration with the AC (Access Control) FortNet system:

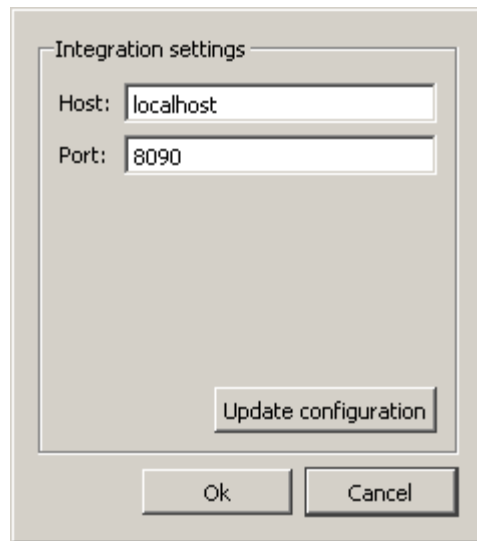


Figure 186. FortNet integration object settings window

Table 69. 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.

12.3.3 Yantar

The *Yantar* object is used to provide integration with the Yantar radiation monitoring system:

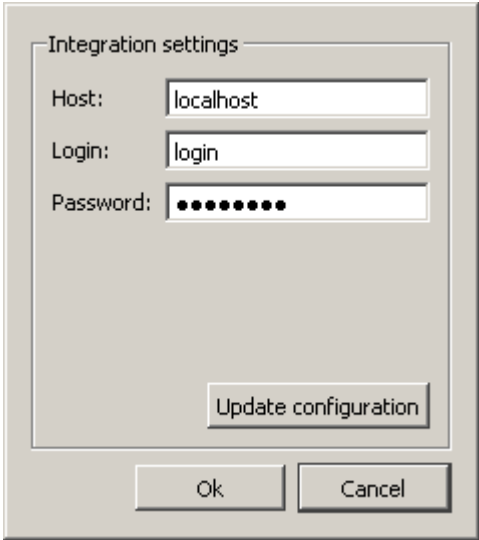


Figure 187. Yantar object settings window

Table 70. Yantar object settings

Parameter	Description
Host	IP address or network name of the computer where the Yantar integration internal executor is running. Default value is localhost.
Login	User name to log into the Yantar radiation monitoring system.
Password	User's password to log into the Yantar radiation monitoring system.
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 Yantar system's objects (modules):

- *Yantar root location*;
- *Yantar gamma-ray sensor*;
- *Yantar neutron sensor*.

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.

13 Keyboard Shortcuts

This section describes shortcuts used to perform actions on different SecurOS objects.

13.1 Administration Toolbar

Table 71. Object tree keyboard shortcuts

Shortcut	Description
Delete	Delete the selected object
Enter	Open the selected object properties window
Space	Disable/enable the selected object
Ctrl+N	Show object creation menu
*	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	Call context help section when object parameter settings window is opened

14 Appendixes

This section contains a description of system utilities and other additional information useful to configure and operate the system.

14.1 Appendix A. Upgrading/Uninstalling Software

This section describes SecurOS upgrading and uninstalling specifics.

14.1.1 Upgrading Software

To upgrade software do the following:

1. Start the installation program by launching the setup file of the new software version.
2. Wizard will display the following window (see figure 188).



Figure 188. Software upgrade query

3. Click **Yes** to continue. Further installation steps are similar to ones for the initial installation (see [SecurOS Installation](#)).

14.1.2 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 189)

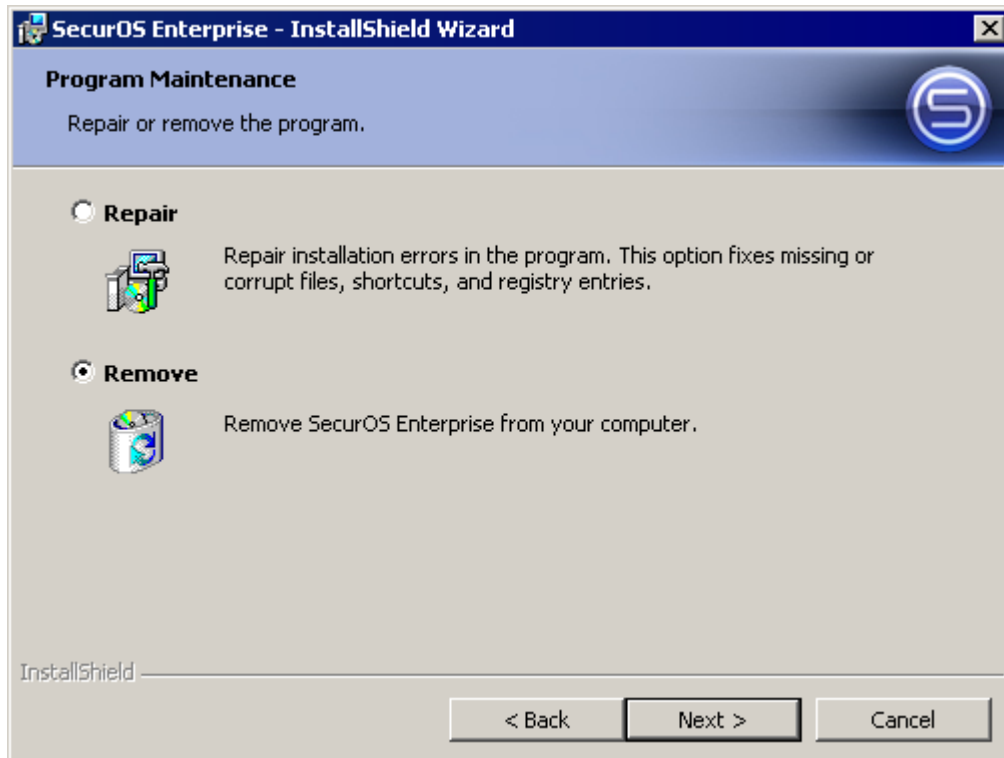


Figure 189. Program Maintenance Window

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.

14.1.3 Release 6.2 Updating Procedure

Since SecurOS Release 7.0 utilizes advanced technology to provide synchronization of the network configuration, the SecurOS Release 6.2 updating procedure is relative to the new architectural requirements.

To update installed release software determine the network server of any type (*Video Server* or *Administrator Workstation*) which will be assigned *Configuration Server*, then do the following:

1. **Software Updating On Configuration Server;**
2. **Updating Software On Peripheral Servers.**

For details on the server configuration procedure when updating SecurOS software see the relevant sections below.

14.1.3.1 Software Updating On Configuration Server

To update the *Configuration Server* do the following for the specific steps of the typical update procedure:

1. Run the SecurOS setup file on the assigned *Configuration Server*.
2. During installation select *Configuration Server* to specify the server type.

When the server will start after software installation is completed, the last configuration stored on the server before updating will be loaded.

Warning! Initial configuration (see [Initial Configuration](#)) with the help of the System Configuration Wizard is not performed on the updated *Configuration Server*.

14.1.3.2 Updating Software On Peripheral Servers

Note. It is assumed that the software update procedure on the *Configuration Server* is successfully completed.

To configure *Peripheral Servers* do the following for the specific steps of the typical update procedure:

1. During the installation select *Peripheral Server* to specify the server type.
2. Launch SecurOS after the InstallShield Wizard is completed (see [Launching And Configuring SecurOS On Peripheral Servers](#)).
3. System will display the following message (see figure 190):

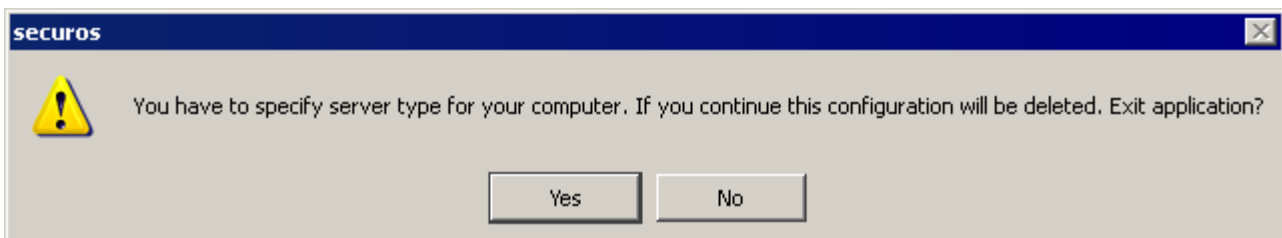


Figure 190. Query to Specify Server Type

At this step it is necessary to delete the Release 6.2 configuration database from configured *Peripheral Server* to ensure correct connection to the *Configuration Server* and allow for copying of the configuration file. To delete old database and continue configuring click **No**.

4. System will launch the System Configuration Wizard and display the **Security network server type** window (see figure 191).

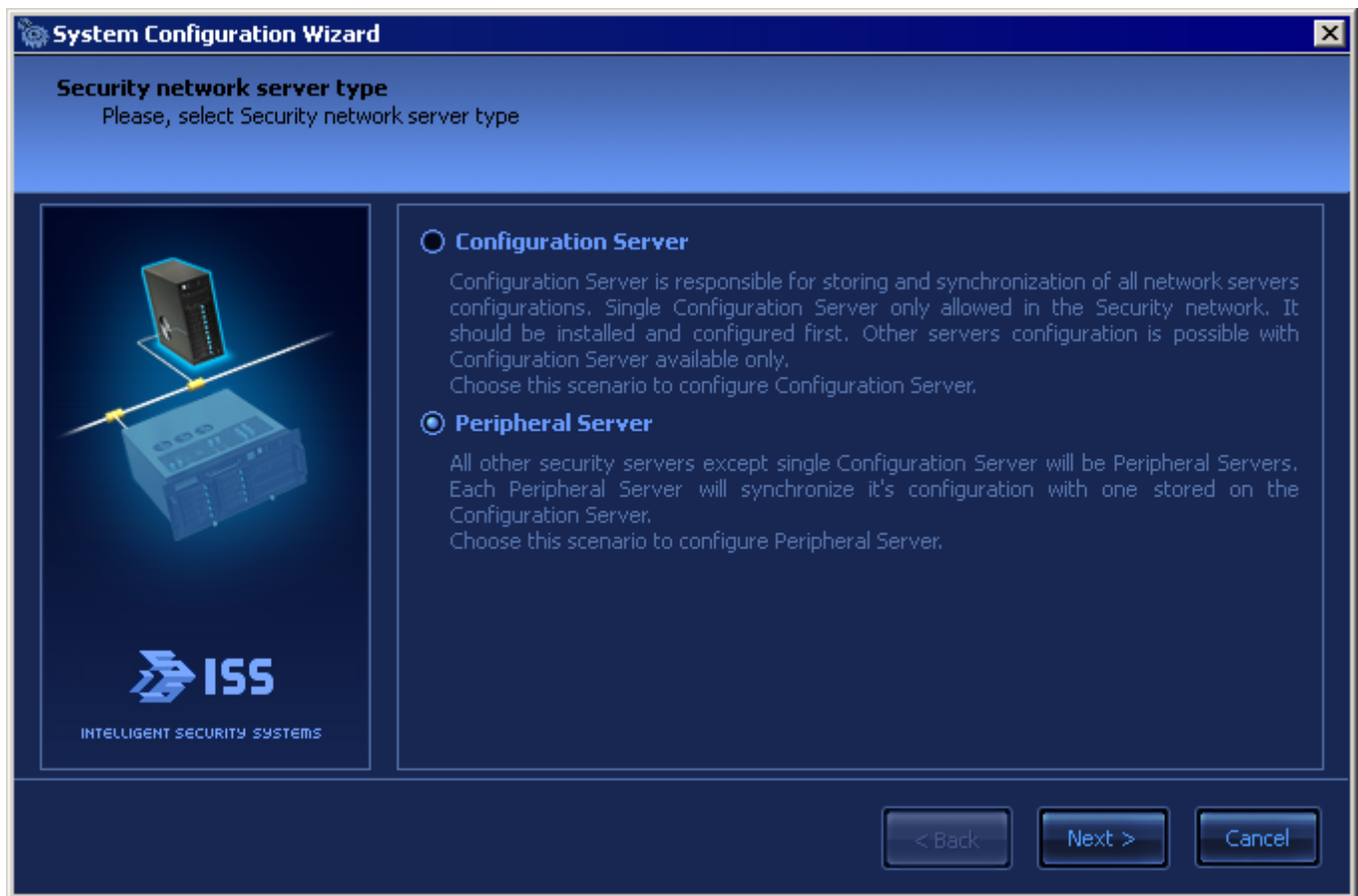


Figure 191. Security network server type

Select **Peripheral Server** option.

5. Further steps of the configuration procedure are similar to the SecurOS's first launch on the *Peripheral servers* (see [Launching And Configuring SecurOS On Peripheral Servers](#) section).

14.2 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*, *Monitor*.

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 (TVISS board, 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 camera connected to one of the TVISS boards, select the corresponding TVISS option.

- 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.
 - **PCI Channel, Format** — if using TVISS boards, set these parameters accordingly.
 - **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 **Title** (e. g. *Office, Street, Home* etc.). You may also use default ID/Name.

Notes:

1. For cameras connected to TVISS-RT/MX boards, one *Video Capture Device* object will be created (per board) with multiple *Cameras* as child objects.
 2. For single lens IP cameras, one *Video Capture Device* object will have one *Camera* child object.
 3. 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*.
 4. 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 connected to a TVISS board, then this number should correspond to the number on the label of the input of the communication cable (dongle).
 - 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` to use IP-camera native telemetry, or specify previously created third-party `PTZ` device which will be used to control the analog camera.
 - **Image Settings** — specify parameters on the **Advanced** tab.
4. Configure *Monitor* object parameters:
- Add cameras to the monitor. To add all the cameras of the system, click **Add all** button near the **Cameras** table. To add cameras individually, double click in the first empty field under the **Id** column (in the **Camera** table) and select the corresponding camera identifier. To add next camera, select the last row of the table and press `↓` key. To delete a camera from the table, select corresponding row and press **Ctrl+Delete** on keyboard.

14.3 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:

- **ISS Hardware Report Utility** (`HardwareReportUtility.exe`) reports all installed TVISSx video

capture cards and Guardant keys (see [ISS Hardware Report Utility](#)).

- **ISS System Report Utility** (ISSInfo.exe) collects system information required by Intelligent Security Systems Technical Support (see [ISS System Report Utility](#)).
- **ISS Media Export Utility** (Backup.exe) plays archived video/audio and exports selected parts of archive to AVI, ASF and BMP files (see [ISS Media Export Utility](#)).
- **gtUSB Configuration Utility** (gtusbconfig.exe) configures video capture USB devices (see [gtUSB Configuration Utility](#)).
- **ISS Startup Configuration Utility** (RegService.exe) configures SecurOS to run as a Windows Service or as a normal application (see [ISS Startup Configuration Utility](#)).
- **DSAdmin Utility** (dsadmin.exe) defines connection strings to databases used by SecurOS (data, protocol, video; see [DSAdmin Utility](#)).
- **ISS Database Update Utility** (idb.exe) defines access to system database: for updating and configuring purposes (see [ISS Database Update Utility](#)).
- **ISS Object Types Database Editor** (DDI.exe) edits the SecurOS object types database (not actual Securos database) (see [ISS Object Types Database Editor](#)).

14.3.1 ISS Hardware Report Utility

Location:

SecurOS folder>/Tools/HardwareReportUtility.exe

Start menu:

Start → Programs → SecurOS → Hardware Report Utility

This utility is used to detect all installed TVISSx video capture cards and Guardant keys (see figure 192). The report is used to generate the system license key file key.iss by the Intelligent Security Systems Technical Support Team.

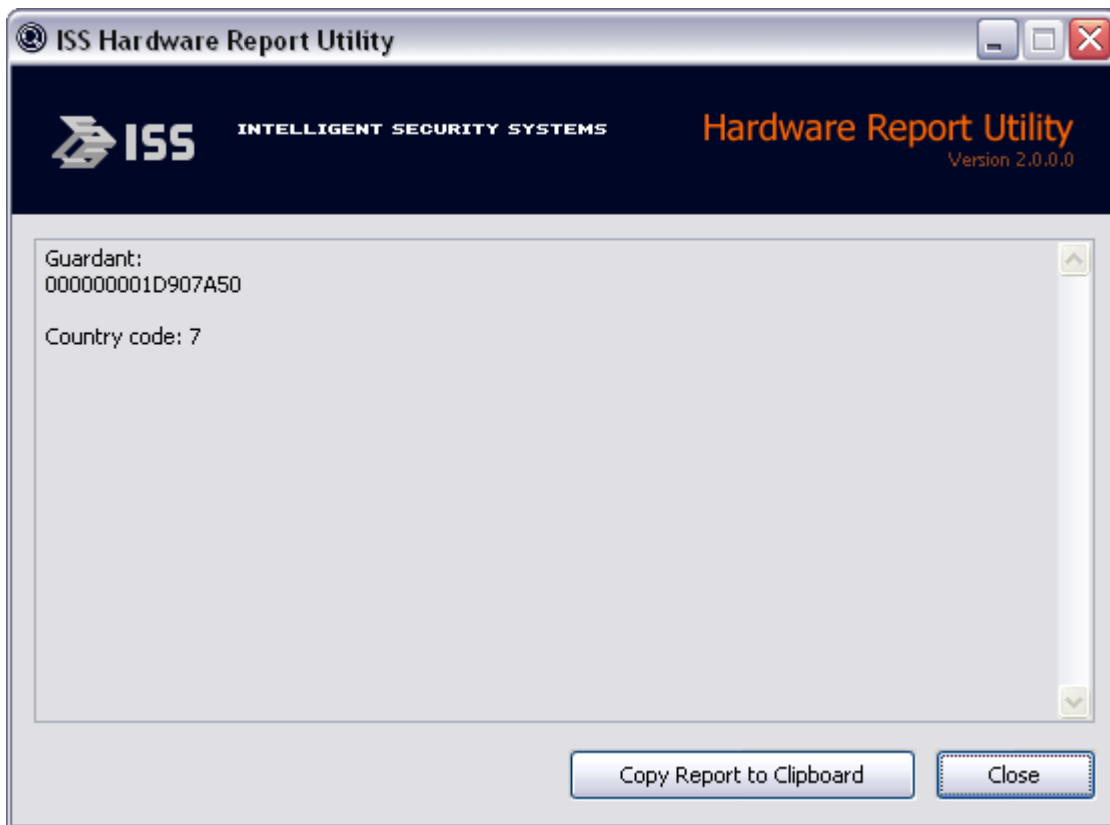


Figure 192. ISS Hardware Report Utility window

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.

14.3.2 ISS System Report Utility

Location:

SecurOS folder>\Tools\ISSInfo.exe

This utility is intended for collecting technical information about the SecurOS installation and your computer (see figure 193). This information is necessary to resolve problems and will always be requested by the Technical Support Team.

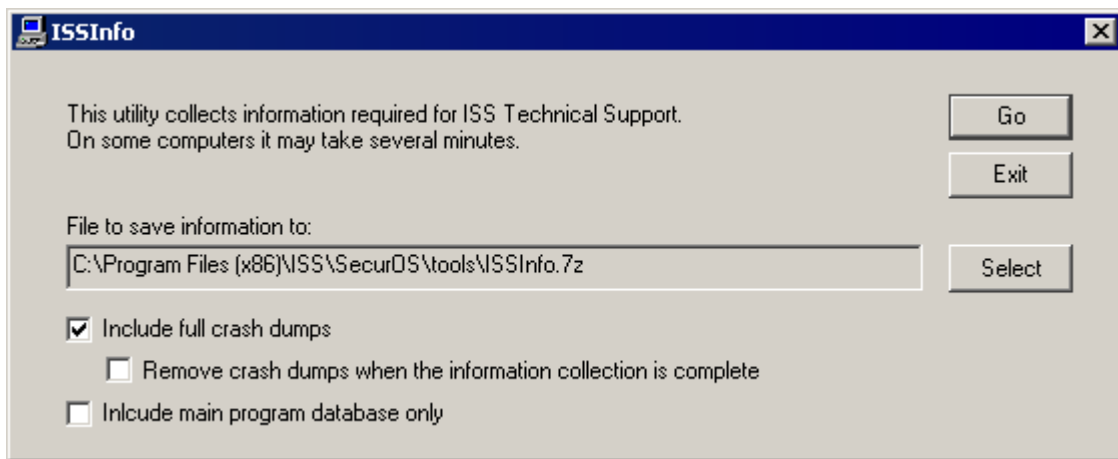


Figure 193. ISS System Report Utility window

The **ISS System Report Utility** collects the following data:

- the `Modules` file which contains the list of all dll and exe-files in the system and information about their version from the SecurOS folder.
- the `CurrentDriver` file contains information on the version of the installed drivers of TVISSx boards.
- the `DallasCodes` file contains information on codes of the installed devices: TVISSx or Guardant.
- the `ISS_Config` file contains information from the following registry folder: `HKEY_LOCAL_MACHINE\SOFTWARE\ISS`.
- the `data`, `videoi`, and `protocol` files contain information from the `securos`, `fsindex` and `protocol` databases accordingly.
- the `SystemInfo` file contains information about the computer on which the SecurOS was installed and on which the given utility has been started.

The `\ISSInfo\cur` folder contains log and dump files, program and script files, and also the `key.iss` file.

The `\ISSInfo\devices` folder contains xml library files of integrated cameras and video servers.

The `\ISSInfo\system32` folder contains files from the system libraries.

Note. **ISS System Report Utility** does not collect any private information.

To start the process, click the **Go** button. The `\Tools\ISSInfo` subfolder with the collected data will be created. The contents of this directory will be zipped/compressed into single archive file and will be placed into the specified directory. You can change the output directory before starting the process of data collection by pressing the **Select** button and choosing the target directory and the file name.

If the **Include full crash dumps** option is selected, then all the logs and both minimal and full dumps generated after system crash will be included in the ISSInfo report (increasing the report size). Otherwise only logs and minimal dumps will be included.

If the **Remove crash dumps when the information collection is complete** option is selected, all dumps (both minimal and full) are automatically deleted from SecurOS root directory after utility work is complete.

If the **Collect additional databases** option is selected, then all SecurOS related databases will be included into ISSInfo report. Otherwise only the configuration database (*securos*) will be included.

14.3.3 ISS Media Export Utility

Location:

SecurOS folder>\Backup.exe

Start menu:

Start → Programs → SecurOS → ISS Media Export Utility

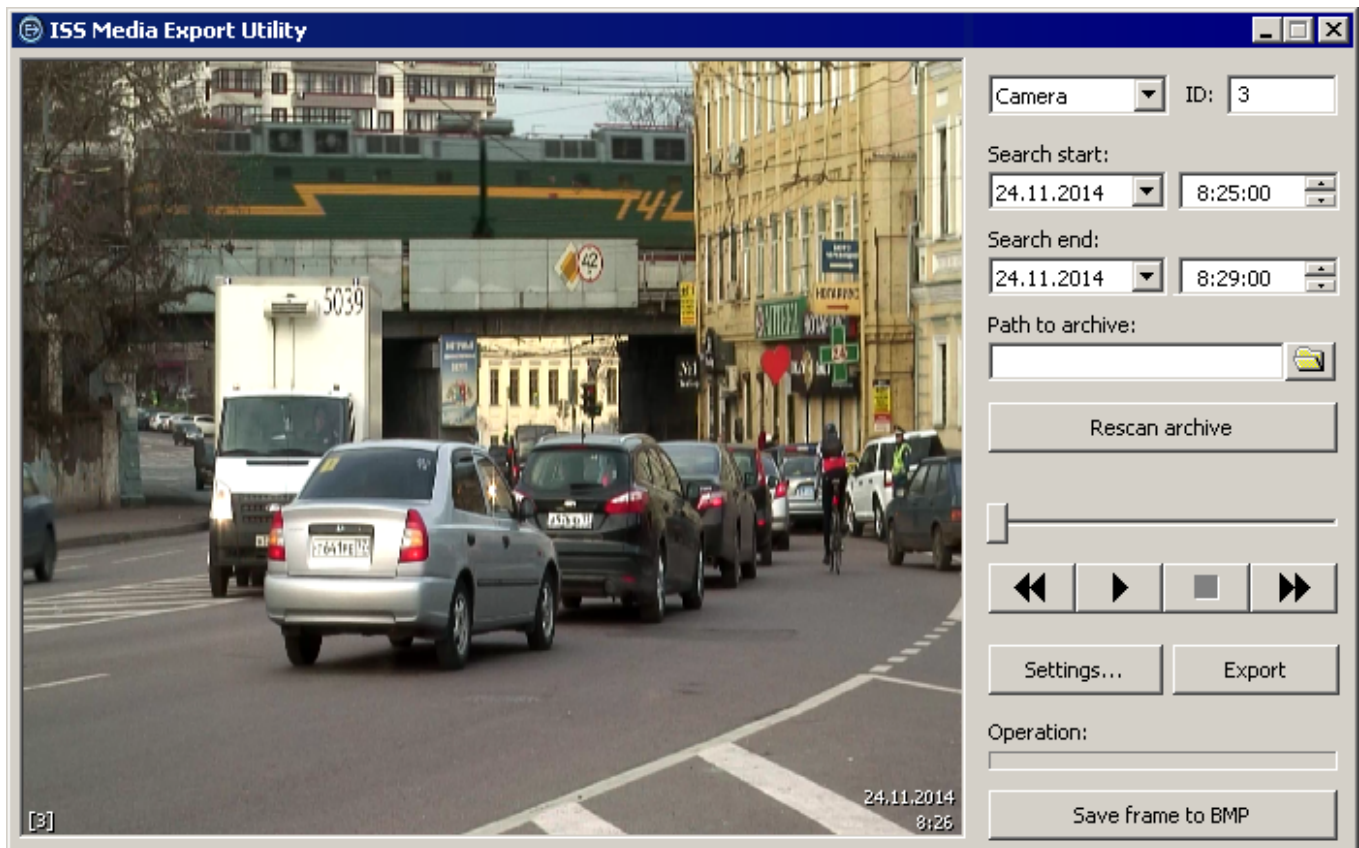


Figure 194. ISS Media Export Utility window

This utility (see figure 194) 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*. If the archive is password-protected and the password from **Export Settings** dialog is not set or invalid, you will be asked for the password.
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 (video/audio codecs, output directory, password 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, password 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.

14.3.3.1 Export Settings dialog

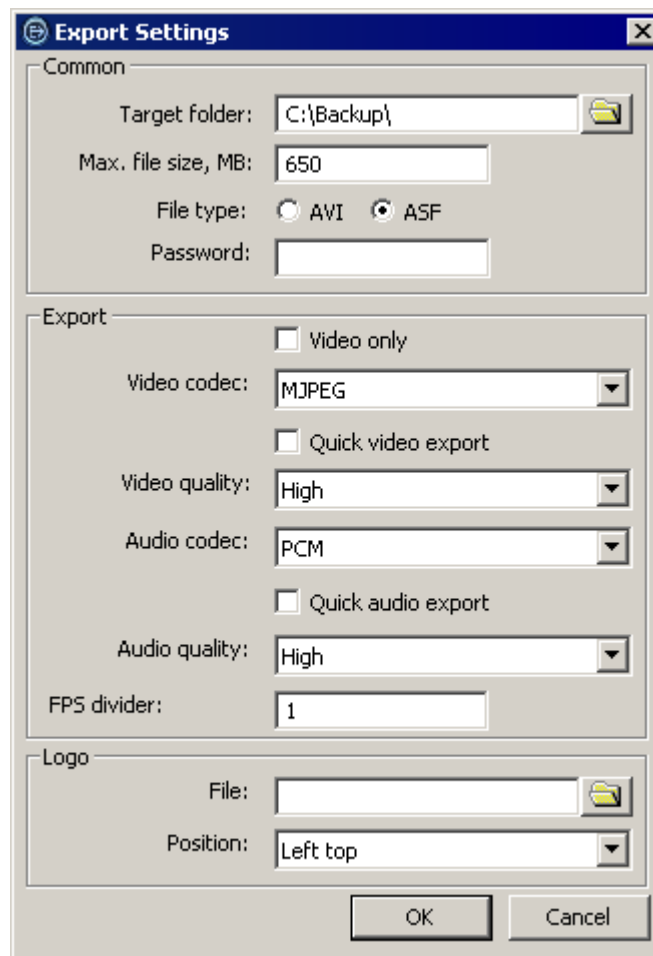


Figure 195. Export settings dialog window

Table 72. 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).
Password	If your video archive is password-protected, set the valid password here before exporting video.
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: 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: 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 or High quality, High Resolution and Standard— for analog cameras (all for min compression level). 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.

14.3.3.2 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 --out <out_file> --cam <camera_number> --from "<start_date_time>"
```

```
--to "<end_date_time>" --span <span_size> --silent
```

Table 73. 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 operative 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.

14.3.4 gtUSB Configuration Utility

Location:

<SecurOS root folder>\Tools\gtusbconfig.exe

This utility is used to configure parameters of USB video capture devices. These devices correspond to selection of USB 2.0 value from the **Type** list of the *Video Capture Device* object settings (see **Video Capture Device**).

Note. The utility supports Grand AV USB 2.0 Pro and X Guard USB devices manufactured by Grandtec.

Warning! Before utility starts, it is necessary to install drivers and plug-in the video capture device, then run SecurOS system, create and configure corresponding object in SecurOS.

On starting utility, the video capture device properties window appears (see figure 196). When finish configuration, click **OK** button to apply parameters or **Cancel** to cancel.

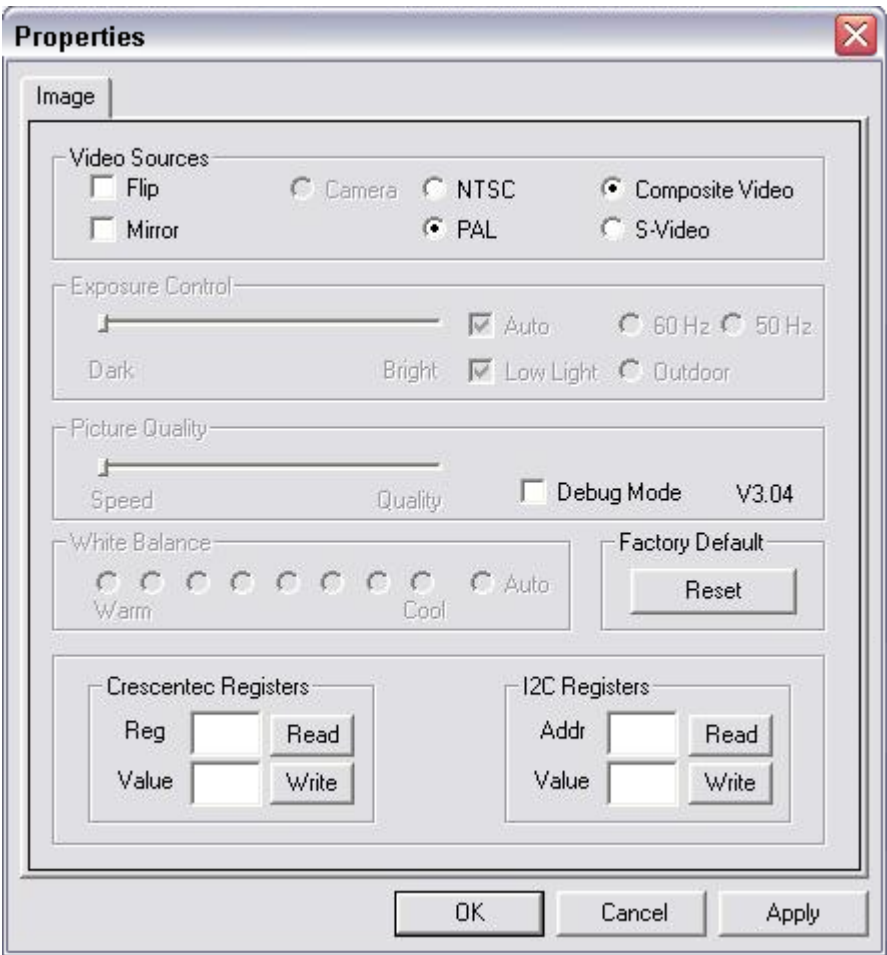


Figure 196. gtUSB Configuration Utility window

Table 74. gtUSB Configuration Utility parameters

Parameter	Description
Video Sources	
Flip, Mirror	Enable these fields to process input image: frame vertical flipping or mirroring.
PAL, NTSC	Select one of these options corresponding to output video signal – PAL or NTSC.
Composite Video, S-Video	Select one of these options corresponding to input video signal interface.
Debug Mode	Enable this field to activate debug mode of the device.
Factory Default	
Reset	Click this button to restore factory default settings.

14.3.5 ISS Startup Configuration Utility

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

Location:

SecurOS folder>\Tools\RegService.exe

This utility configures SecurOS to run as a Windows service or as a normal Win32 application (see figure 197). If you choose Run as service, SecurOS will start automatically at Operating System startup.



Figure 197. ISS Startup Configuration Utility window

To properly configure SecurOS as a Windows service it is recommended to use the **SecurOS Control Service** utility that itself runs SecurOS as a service.

Warning! For security reasons Services only run in a session with zero identifier, while in the 0 session interactive applications cannot be loaded. For this reason, the functionality of the SecurOS Administrator Workstation and SecurOS Operator Workstation when running in daemon mode is limited. Interaction with the application interface in this case can only be done through the *Interactive Services Detection*.

Warning! After SecurOS is updated it is necessary to configure SecurOS to run as a Windows service.

Location:

SecurOS folder>\securos_svc.exe

Help information on syntax and utility keys is displayed when running this utility from the command line with the `-h` parameter.

SecurOS Control Service} Utility Syntax:

```
securos_svc -h -i n -r -s -k -t n -u s -p s -l s -d
```

- `-h` — gives utility keys with description.
- `-i n` — register SecurOS as a Windows service. Specify `n` service running type (1 — disable, 2 — automatic, 3 — manual).
- `-r` — delete service from Windows services list.
- `-s` — run the service.
- `-k` — stop the service.
- `-t` — specify service running type of already registered service (1 — disable, 2 — automatic, 3 — manual).
- `-u s` — specify `s` user name to run service.
- `-p s` — specify `s` user password to run service.
- `-l s` — specify names of dependent services.
- `-d` — enable verbose mode.

It is recommended to register automatic start of SecurOS service for correct work of SecurOS and to set dependency on PostgreSQL service:

```
securos\_svc.exe -i 2 -l "PostgreSQL8.4"
```

It is necessary to check real name of PostgreSQL service on your computer (the above example uses PostgreSQL8.4).

To find PostgreSQL service name:

1. Open Windows **Control Panel** (**Start** → **Settings** → **Control Panel**).
2. Choose **Administrative Tools**, then **Services**.
3. Locate **PostgreSQL8** service in the services list and choose **Properties**. Service name is specified in **Service name** field.

After such registration, upon starting of SecurOS service it will wait until the PostgreSQL service starts.

Note. It is recommended to use automatic Windows login in case when SecurOS is configured as Windows service (see automatic login configuration description in [Win7/Win8.1/Windows Server Automatic Login Configuration](#)).

14.3.6 DSAdmin Utility

Location:

SecurOS root folder>\dsadmin.exe

This utility stores the connection strings to the 3 default SecurOS databases. The SecurOS database is intended for storing settings for all the system objects. The Protocol database stores records of the events/reactions occurring in the system. The fsindex database stores data about recording/motion alarms and about bookmarks.

Note. All connection strings are automatically defined during SecurOS installation.

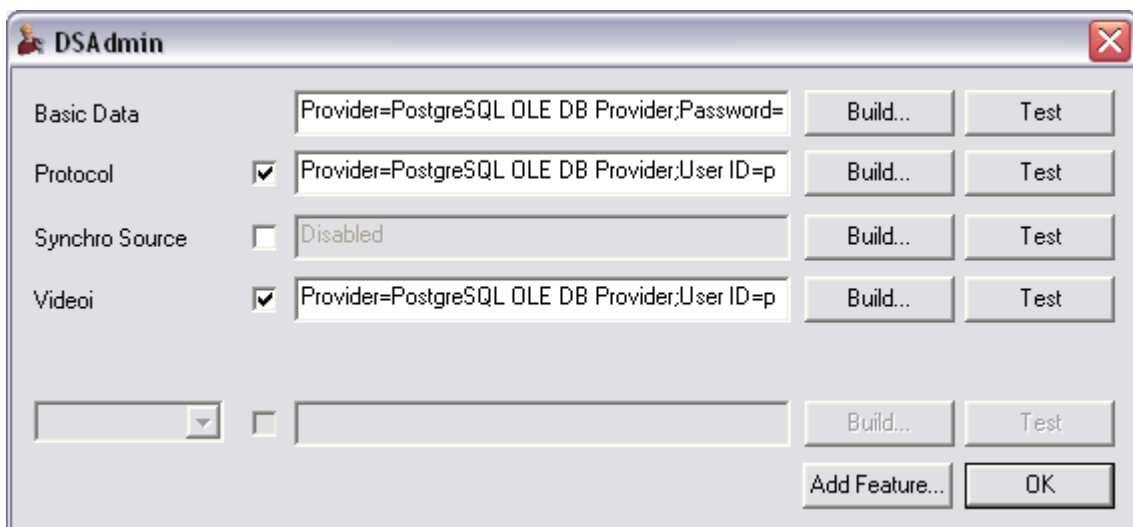


Figure 198. DSAdmin Utility window

There are four fixed fields to set connection strings:

- **Basic Data** – string to connect to general database which holds settings for all the system objects (the `Securos` database).
- **Protocol** – string to connect to database of the events occurring in the system (the `Protocol` database).
- **Synchro Source** – string to connect to database of synchronization (optional).
- **Videoi** – data recording about alarms and about video archive bookmarks (the `fsindex` database).

Note. There is an additional field **New feature** to set and configure a new database.

To change a connection string, click its **Build** button. To test a connection – **Test** button.

On **Build** button click **Data Link Properties** and a window will appear that will help build the connection string:

- **Provider** tab: select **PostgreSQL OLE DB Provider** from the list.
- **Connection** tab:
 - Type in server's name or address in **Data Source** field (e. g., `127.0.0.1`, `localhost`).
 - Type in database name in **Location** field (e. g., `securos_db`).
 - Type in database account in **User Name** and **Password** fields.

Warning! Use Latin characters only when specifying a **Password**. `Latin-1` code page (Western European character set) is acceptable.

To apply changes in connection strings, click **OK** button. The changes will be applied and the utility window will be closed.

14.3.7 ISS Database Update Utility

Location:

<SecurOS root folder>\idb.exe

This utility allows to configure and update SecurOS database.

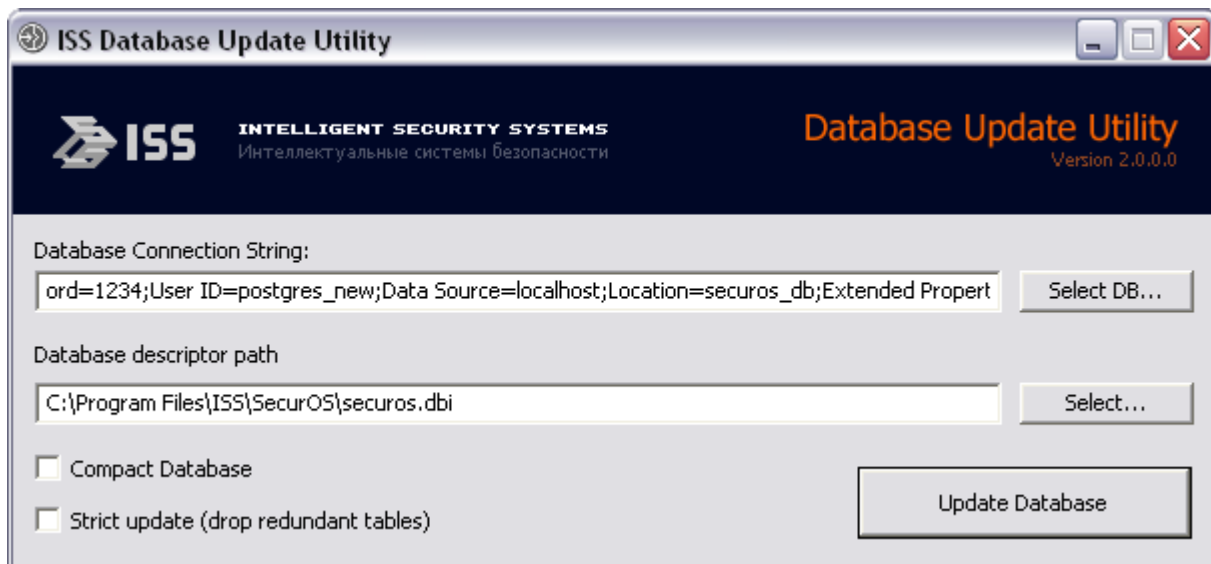


Figure 199. ISS Database Update Utility window

Table 75. ISS Database Update Utility parameters

Parameter	Description
Database Connection String	String to connect to database. Type in manually according to mask or click Select DB button to build it automatically (see below).
Database Descriptor Path	Path to database description file. Type in manually or click Select button to choose the corresponding file from the standard Open window.
Update Database button	Start SecurOS database update process.

Clicking **Select DB** button will cause **Data Link Properties** window displaying. For the detailed description see [DSAdmin Utility](#).

14.3.8 ISS Object Types Database Editor

Location:

SecurOS root folder>\Tools\DDI.exe

This utility allows the viewing and editing of the SecurOS object types database. This utility can also be used to preview files or alter file names for sound notifications (see figure [200](#)).

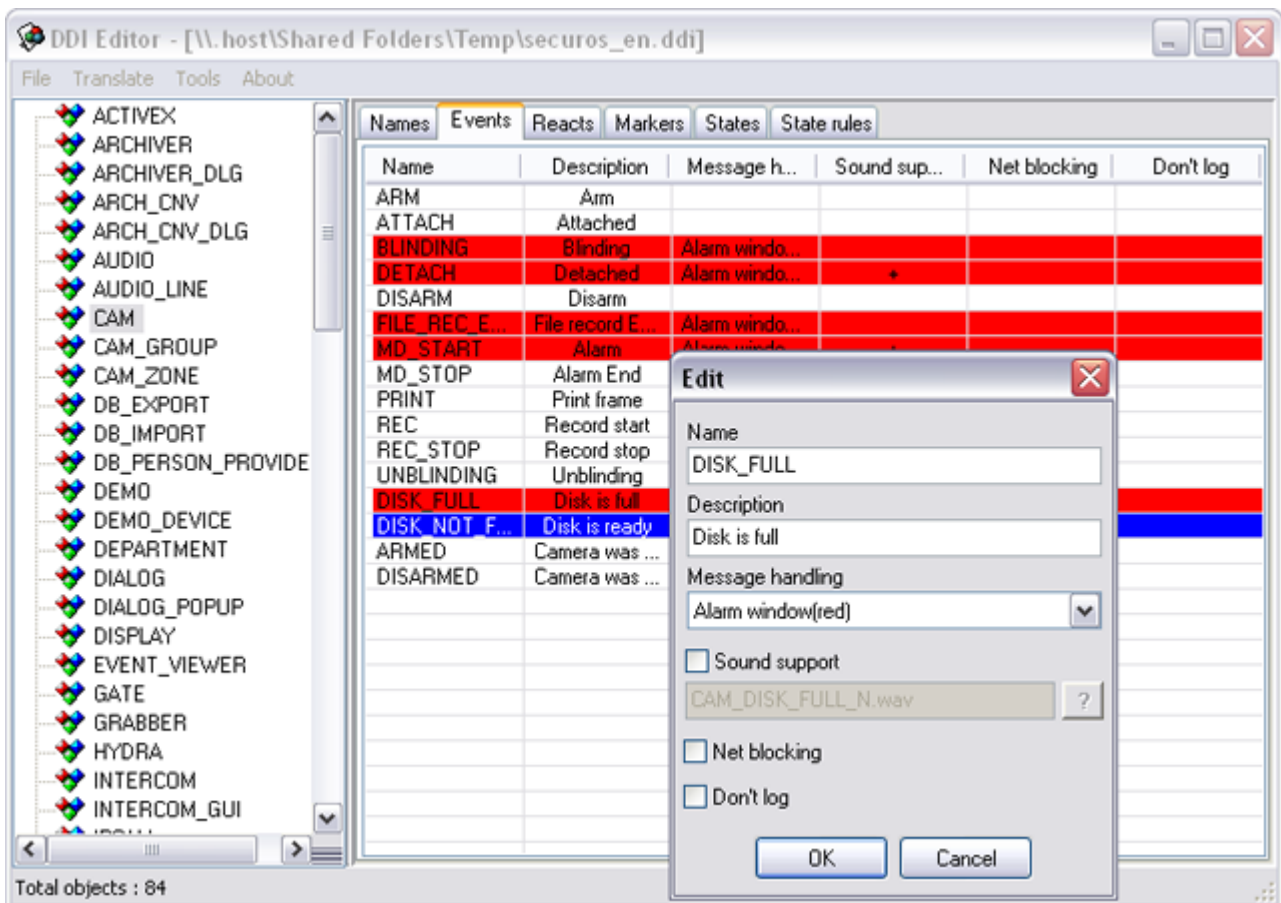


Figure 200. ISS Object Types Database Editor

The left pane of the utility window contains the list of all possible system objects, which can be used by the loaded SecurOS configuration. The right pane contains the following tabs, which allow to view and edit properties of the different types of the SecurOS objects:

- **Names** — displays the selected object name and its group name. Also may be used to search for object by its name or type (see [Names Tab](#)).
- **Events** — contains the selected object events and its parameters: event description, window type, sound support, net blocking and log (see [Events Tab](#)).
- **Reacts** — contains the selected object commands and its parameters: command description and flags (see [Reacts Tab](#)).
- **Markers** — contains a list of the selected object markers (see [Markers Tab](#)).
- **States** — contains a list of the selected object's possible states and its parameters: image file name, description, enabling blinking, etc. (see [States Tab](#)).
- **State rules** — displays rules for changing states of the selected object's type (see [State Rules Tab](#)).

To see certain object information, select it in the objects tree. Data on the chosen object will be displayed on tabs.

14.3.8.1 Names Tab

This tab contains the name of the chosen object and its group (see figure 201). Object search on its type or identifier can be started from this tab.

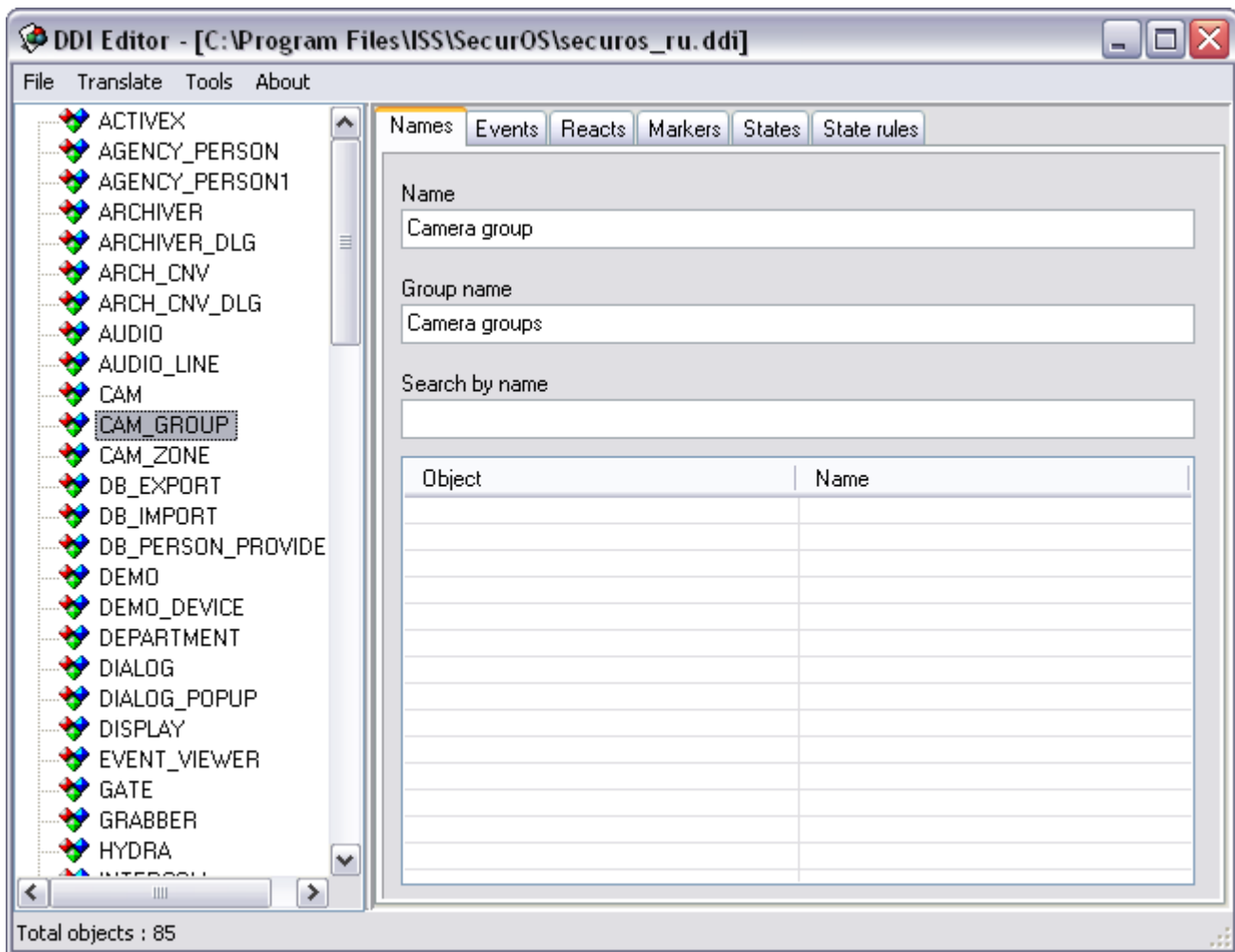


Figure 201. Names tab of Object types database editor

To find an object by its type:

1. Specify part or complete object type name/identifier in the "Search by name" field. The list of objects containing the specified value in their names will appear in the table below.
2. Select the required object in the table. Data on the chosen object will be displayed on all tabs.

14.3.8.2 Events Tab

This tab contains the table of system events which can be generated by the selected object type (see figure 200).

Table 76. Events Tab Table - Column settings and Edit window actions

Parameter	Description
Name	Event identifier which is generated from selected object.
Description	Event description.

Parameter	Description
Message handling	Additional system reaction on the event (alarm/informational window color settings). The row will be colored with the chosen color. Possible values: Alarm window (red) — red colored highlight on the incoming event. Information window (blue) — blue colored highlight.
Sound support	Sound accompanying event. Enable this field to specify sound file name like this: OBJECT_NAME_EVENT_NAME_N, where N is the actual object name in the SecurOS object tree.
Net blocking	Event notification will not transfer into security network in case of local event. Enable this field to turn off sending of notifications.
Don't log	Event will not be logged in the system log. Enable this field to turn off event logging.

To edit system event table cells, select a field for editing and right-click. Context menu with available actions will appear.

Context menu contains the following items:

- **Add** — add event into the table (all parameters will be specified). Edit window will appear where all fields of the event can be specified (see above).

Note. Only events that always exist for a chosen object can be created (on developing system stage).

- **Edit** — edit chosen event parameters. Events parameter editing window will appear.
- **Delete** — delete chosen events. Deleted events will no longer have an effect on the system.
- **Copy events** — copy event parameters into clipboard.
- **Paste events** — add event from clipboard into the table.
- **Add event for all objects** — equal to **Add** item, but event is added for all system objects.

14.3.8.3 Reacts Tab

This tab contains the reactions table for the chosen object type.

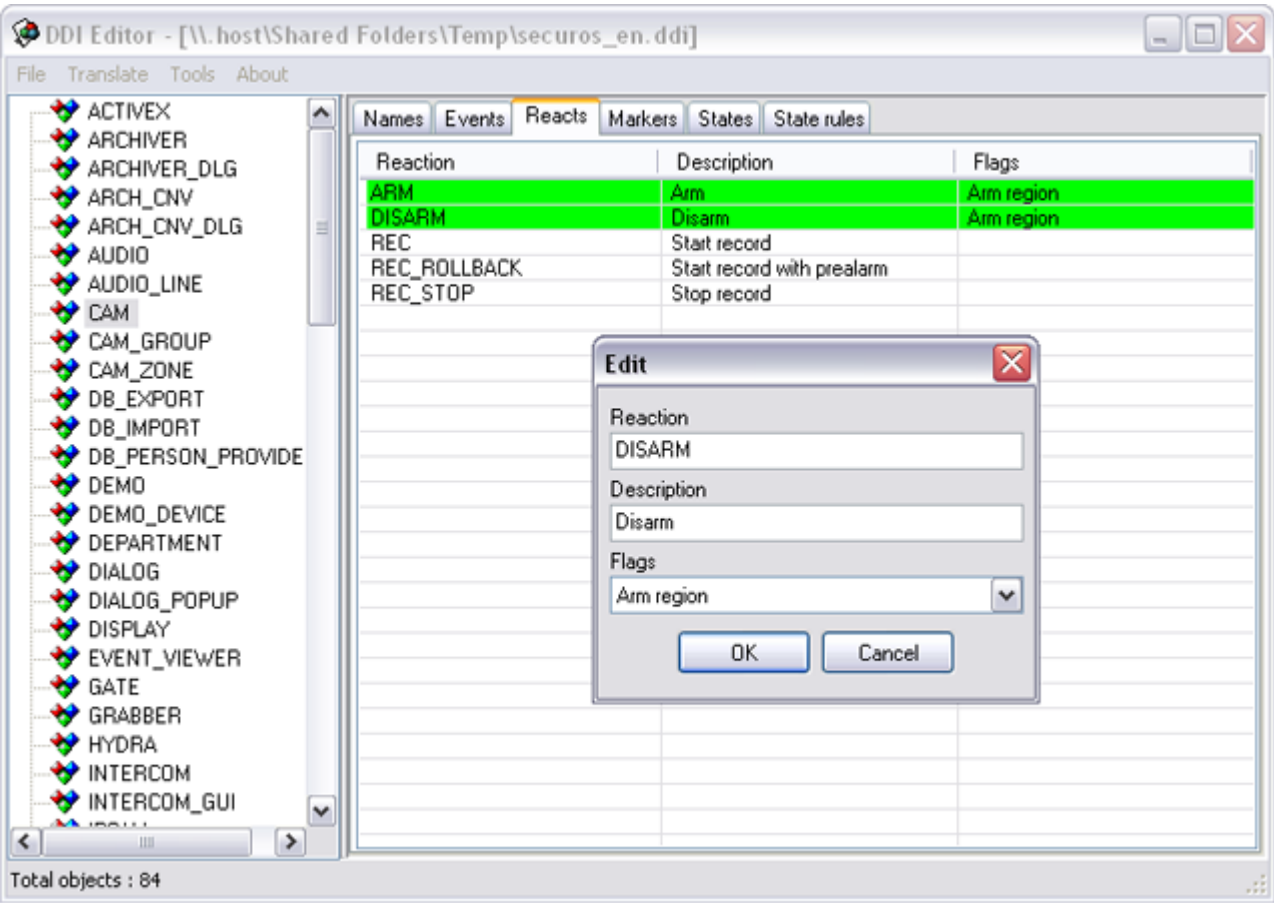


Figure 202. Reacts tab of Object types database editor and Add window

Table 77. Reacts tab Table - Column settings and Edit window actions

Parameter	Description
Reaction	Reaction identifier of the selected object.
Description	Reaction description.
Flags	Additional reaction flags. The row will be colored with chosen color. Possible value: Arm region — certain reaction relates to arm or disarm.

To edit system reacts table cells, select a field for editing and right-click. Context menu with available actions will appear.

Context menu contains the following items:

- **Add** — add react into the table (all parameters will be specified). Edit window will appear where all fields of the reaction can be specified (see above).

Note. Only reacts that always exist for a chosen object can be created (on developing system stage).

- **Edit** – edit chosen react parameters. Reacts parameter editing window will appear.
- **Delete** – delete chosen reacts. Deleted reacts will no longer have an affect on the system.
- **Copy reacts** – copy react parameters into clipboard.
- **Paste reacts** – add react parameters from clipboard into the table.

14.3.8.4 Markers Tab

This tab contains icons table which will be depicted on a map (see [Maps Working Principles](#)) for chosen object type.

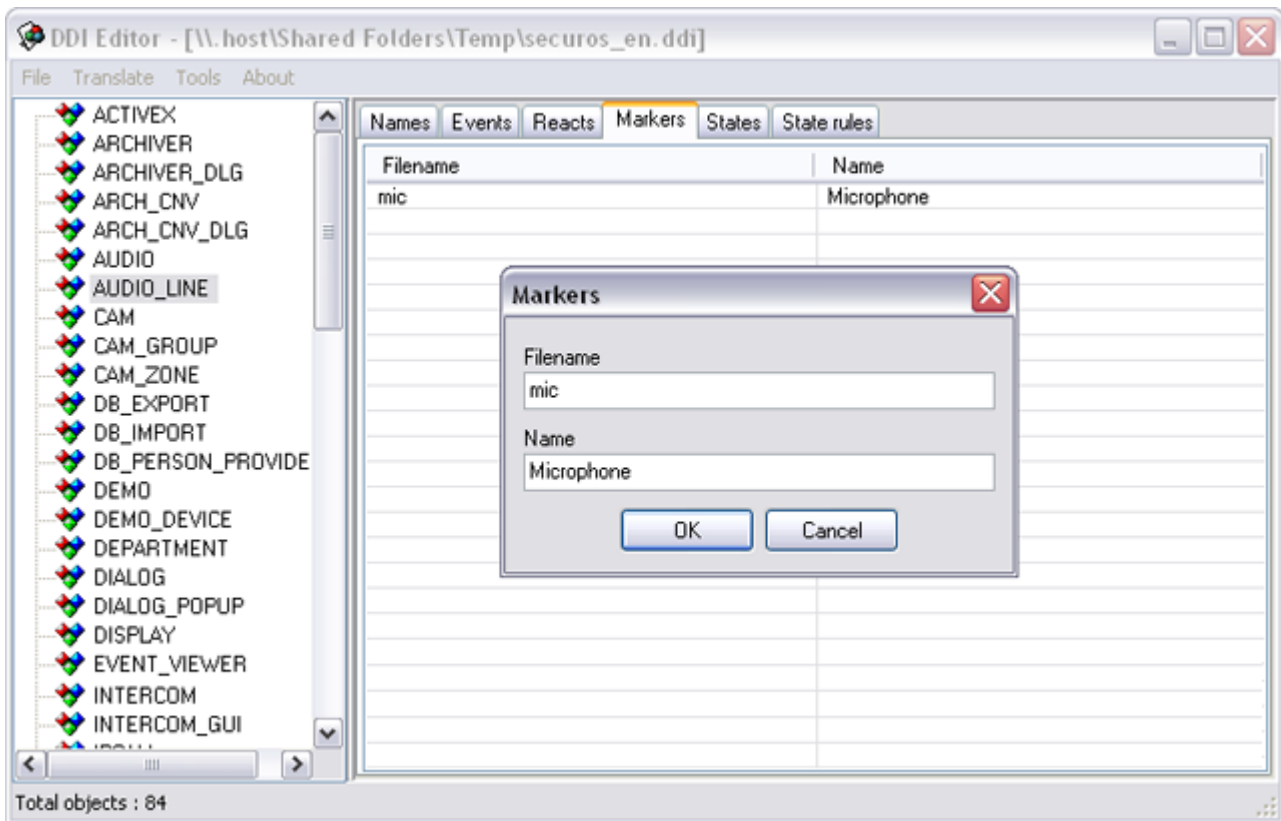


Figure 203. Markers tab of Object types database editor and Markers window

Table 78. Markers tab Table - Column settings and Markers window actions

Parameter	Description
Filename	Icon file name (with bmp extension).
	Note. Corresponding file has to be in the \Bmp sub-folder of system root directory!
Name	Icon description.

To edit markers table cells, select a field for editing and right-click. Context menu with available actions will appear.

Context menu contains the following items:

- **Add** – add icon into the table (all parameters will be specified). Edit window will appear where all fields of the new icon can be specified (see above).

Note. Corresponding file has to be in the \Bmp sub-folder of system root directory.

- **Edit** – edit chosen icon parameters. Icons parameter editing window will appear.
- **Delete** – delete chosen icons. Deleted icons will no longer have an affect on the system.
- **Copy markers** – copy icon parameters into clipboard.
- **Paste markers** – add icon parameters from clipboard into the table.

14.3.8.5 States Tab

This tab contains table of all possible states for chosen object type.

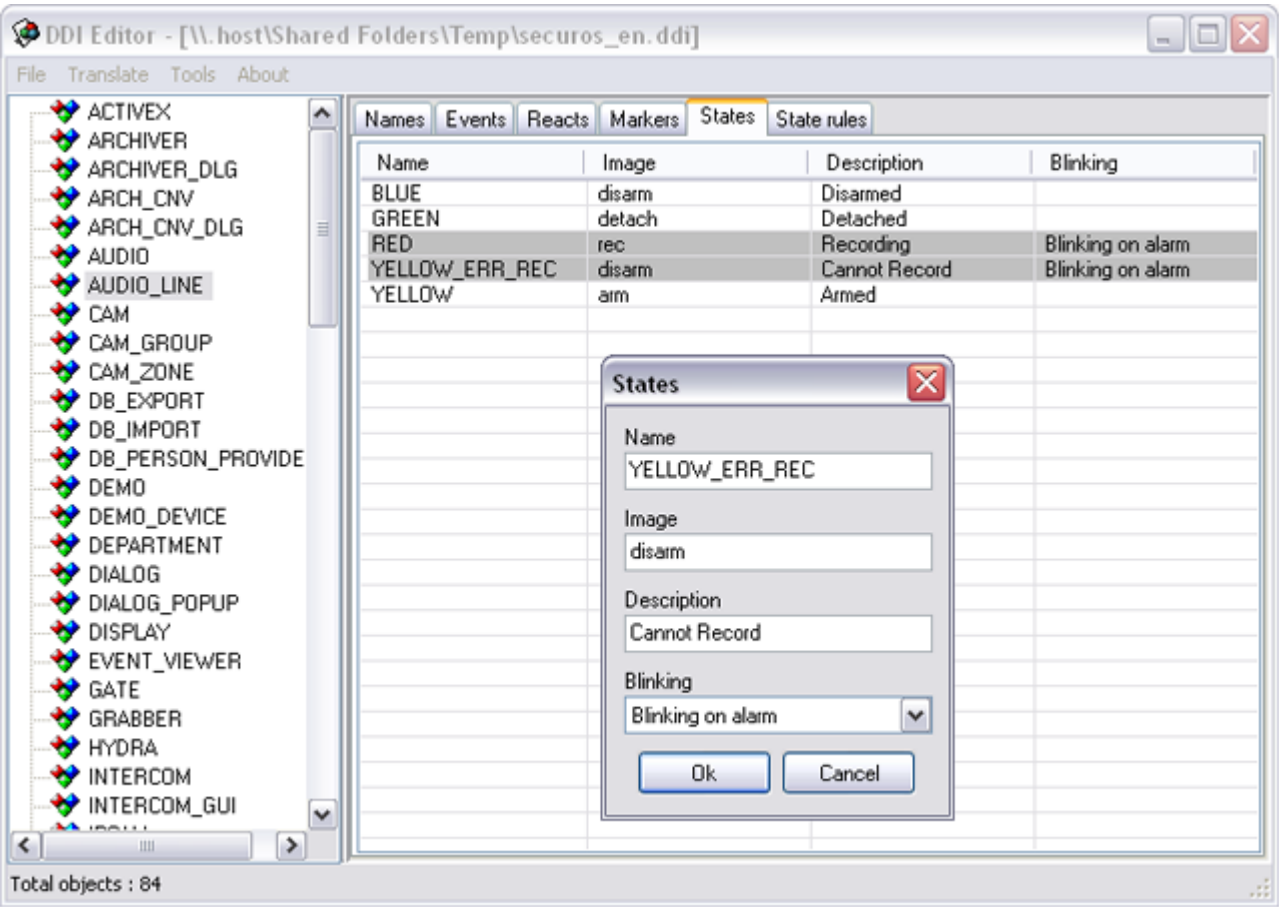


Figure 204. States tab of Object types database editor and State window

Table 79. States tab Table columns settings and States window actions

Parameter	Description
Name	State name.
Image	Name of icon file (with bmp extension) displaying the object state on map. Note. Corresponding file has to be in \Bmp subfolder of system root folder!
Description	State description.

Parameter	Description
Blinking	Additional state parameters. Object icon on a map will be blinking on this state' coming. Possible value: Blinking on alarm — this state corresponds to the alarmed one.

To edit states table cells, select a field for editing and right-click it. Context menu with available actions will appear.

Context menu contains the following items:

- **Add** — add state into the table (all parameters will be specified). Edit window will appear where all fields of the new state can be specified (see above).
- **Edit** — edit chosen state parameters. States parameter editing window will appear.
- **Delete** — delete chosen states. Deleted state will not be used in system working.
- **Copy states** — copy state parameters into clipboard.
- **Paste states** — add state from clipboard into the table.

14.3.8.6 State Rules Tab

This tab contains transmission rules from one state of the object to another. Transmission rules control initial and final states that the chosen object has upon receiving certain events. Initial event, initial state and final state are specified in the table.

Note. If correspondence is not established, then the object transforms to default state.

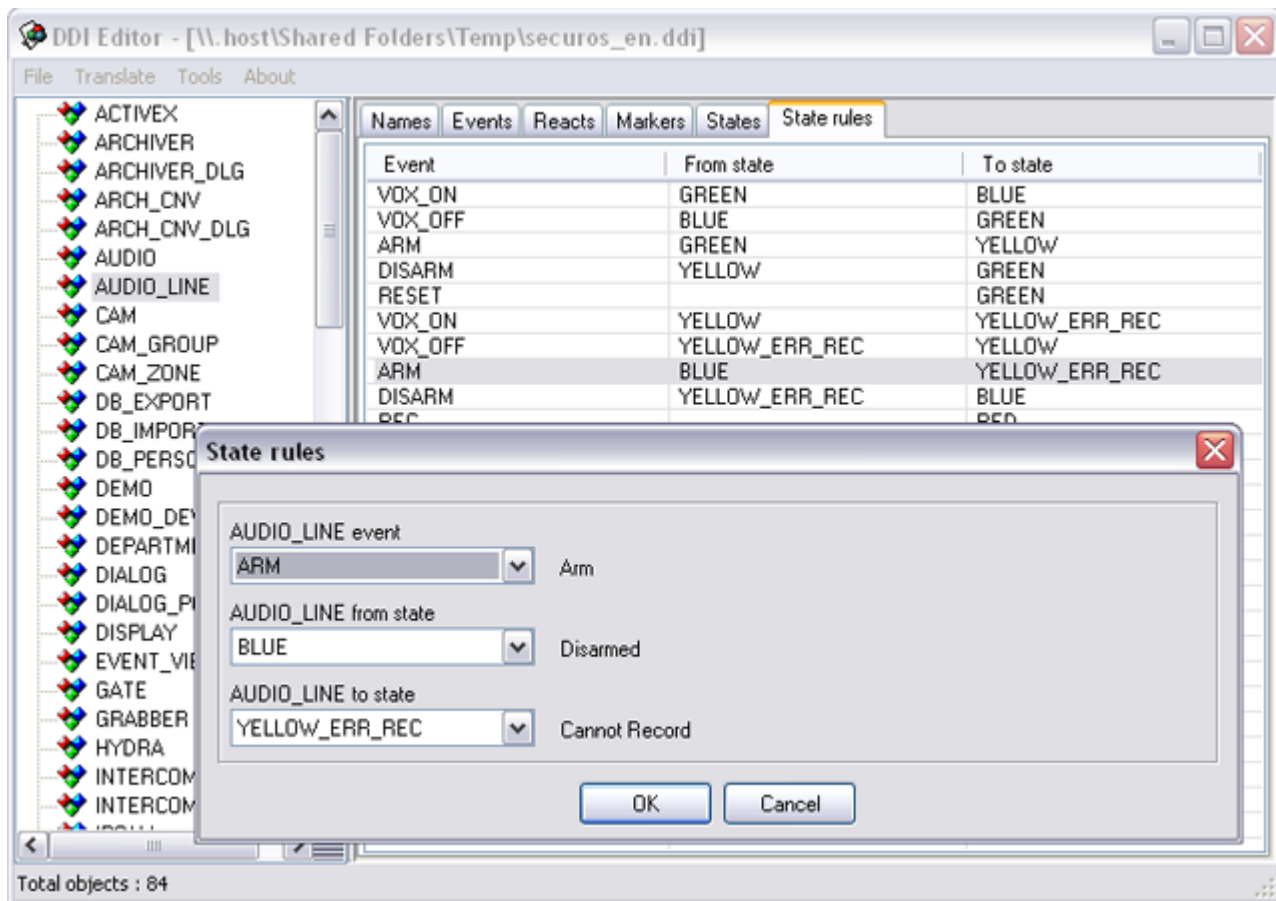


Figure 205. State rules tab of Object types database editor and State rules window

Table 80. State rules tab Table - Column settings and State rules window actions

Parameter	Description
Event	Initial event for transmission. Select from the list of available events for chosen object.
From state	Identifier of initial state for transmission upon event specified in the previous field. If left blank then transmission will be done from any state. Select from the list of available states for chosen object.
To state	Identifier of final state for transmission upon event specified in the first field. Select from the list of available states for chosen object.

To edit state rules table cells, select a field for editing and right-click. Context menu with available actions will appear.

Context menu contains the following items:

- **Add** – add state rule into the table (all parameters will be specified). Edit window will appear where all fields of the new state rule can be specified (see above).
- **Edit** – edit chosen rule parameters. State rules parameter editing window will appear.
- **Delete** – delete chosen rule. Deleted rules will no longer have an affect on the system.
- **Copy state rules** – copy state rule parameters into clipboard.
- **Paste state rules** – add state rule from clipboard into the table.

14.3.9 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 folder>\ServerRoleManager.exe

To reassign current *Configuration Server* do the following:

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 206).

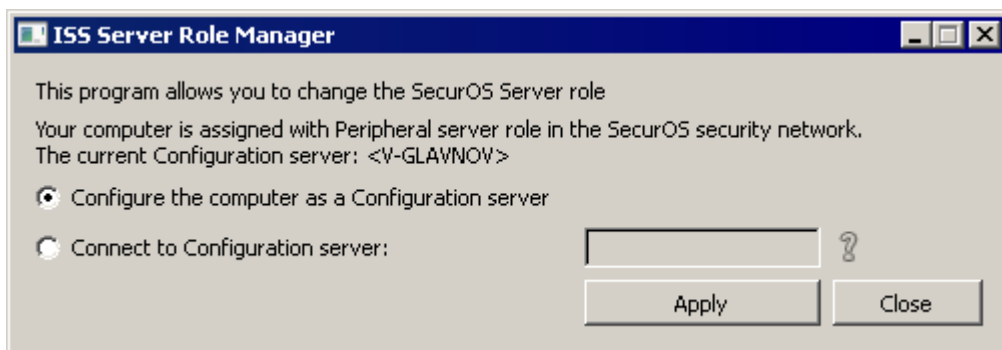


Figure 206. Specifying new Configuration Server

Note. The **current configuration** 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 207).

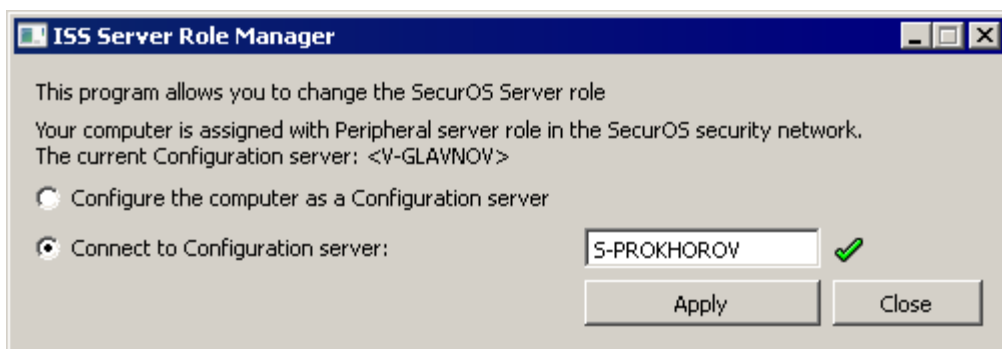


Figure 207. Connect to Configuration Server option

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.

14.4 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 81. TCP/IP Ports

Service	Port numbers
Core	
Core interconnection	21111 (this port must be opened prior to installing SecurOS)
Core services	
Configuration Server	20950
Graphical map	21051
System event log	21055
Programmable keyboard	21005
IIDK interface	21030
Space Keeper	22429
Video subsystem	
Video monitor, video capture, video cameras	21050
Media Client	22428
PTZ device	21010
Live video stream	20900
Archive Converter	22131
Archive Converter Dialog	22138
Videowall Monitor	21413
Video Wall Control Panel	21434

Service	Port numbers
Barco Monitor	22413
Self-diagnostic subsystem	
Health Monitor	23322
Interface subsystem	
HTML Dialog	30300
Audio subsystem	
Microphone	21008
Audio stream	20910
Audio player	22025
Notification subsystem	
Short Message Service	22092
E-mail Message Service	22093
Audible Notification Service	22094
Access Control subsystem	
Access Control Service	21057
LPR Module	
Detector camera	21033
Detector engine	21081
Operator UI	21062 (21091)
External database interconnection	22100
Transit Module	
Server (Pro)	22120
Server (Light)	21121
Detector camera	21122
Face recognition Module	
Engine	21080
Face data stream	20920
Operator UI	21061
Activity analyzer Module	
Engine	22110

Service	Port numbers
Engine (Pro)	22111
POS Module	
POS Terminal	22125

14.5 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.

14.5.1 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, video capture boards and 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.

14.5.2 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.

14.5.3 Installing Microsoft .NET Framework 3.5 under MS Windows Server 2012 R2

To provide correct operation of SecurOS on MS Windows Server 2012 R2 the .NET Framework 3.5 is required. However, the required version cannot be installed by the SecurOS InstallShield Wizard automatically because the .NET Framework 4.5 platform is installed by the OS by default.

To install the .NET Framework 3.5 manually use the **Server Manager** (see <http://technet.microsoft.com/en-us/library/dn482071.aspx>):

1. Open the **Server manager** console application.
2. In the **Manage** menu select the **Add roles and features** option.
3. On the **Select installation** page select the **Role-based or feature-based installation** option.
4. Click **Next** to select features. Select the **.Net Framework 3.5 Features**.
5. If the target computer does not have access to **Windows Update**, click the **Specify an alternate source path** link on the **Confirm installation selections** screen to specify the path to the \sources\sxs folder on the installation media and then click **OK**. Click the **X**, and then the **Install**.
6. Restart the server if needed.

14.5.4 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 208).

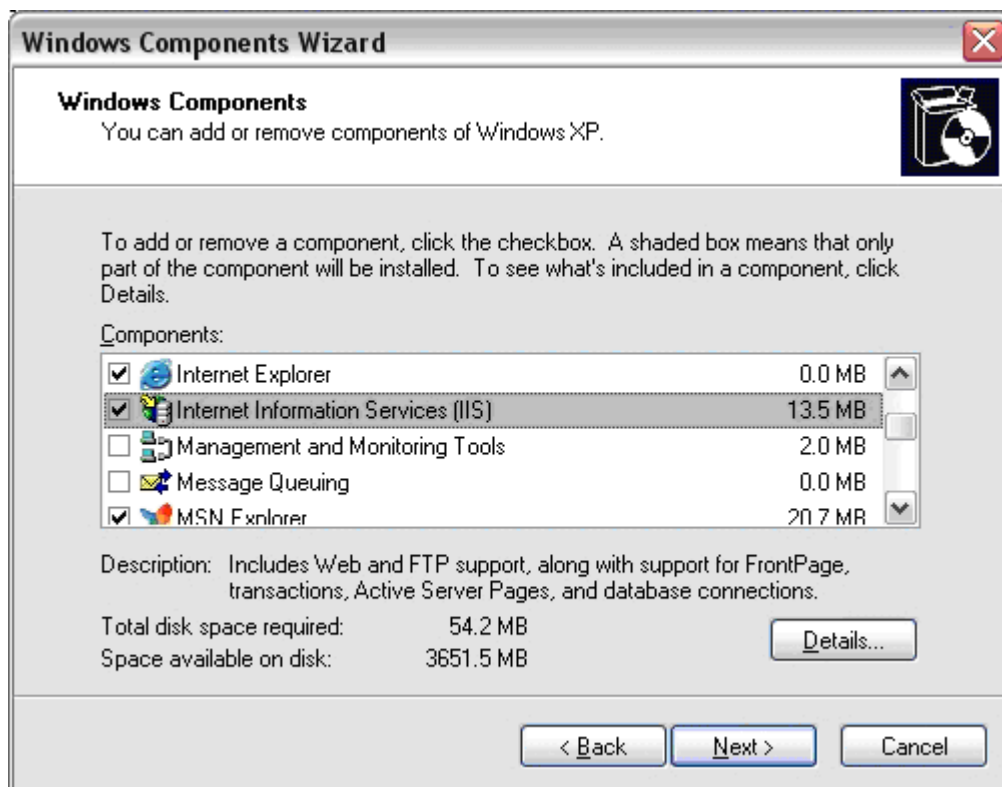


Figure 208. Windows Components Wizard

Enable **SMTP Service** in the list (see figure 209). Click **OK** and **Next** buttons.

Note. Windows installation CD might be necessary at this step.

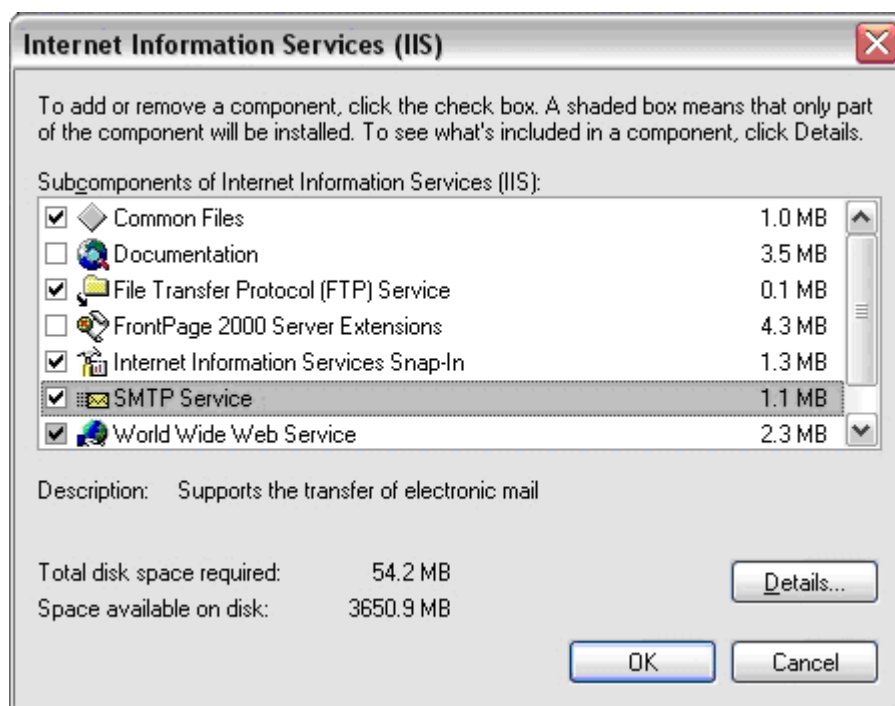


Figure 209. Internet Information Services Components

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 210) right-click **Default SMTP Virtual server** (or

another name, given by default) and choose **Properties**.

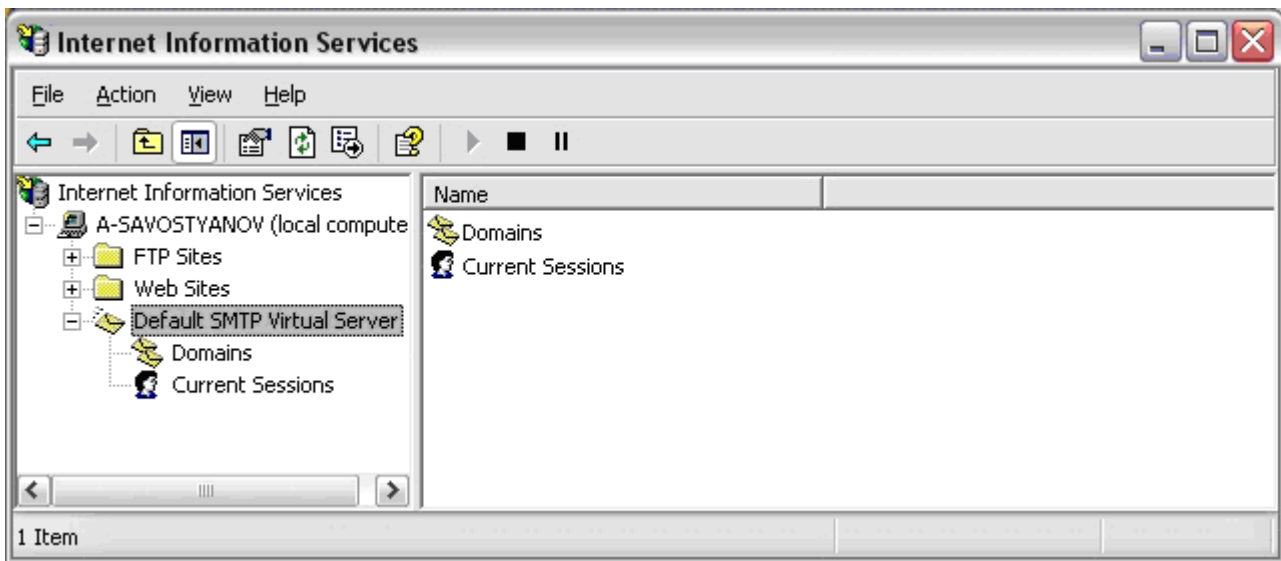


Figure 210. IIS Services tree

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 211).



Figure 211. SMTP server relay restrictions settings

5. Choose **Delivery** tab and click the **Advanced** button.
6. In new **Advanced Delivery** window (see figure 212) specify remote server to route all sending mail in **Smart Host** field and click **OK**.

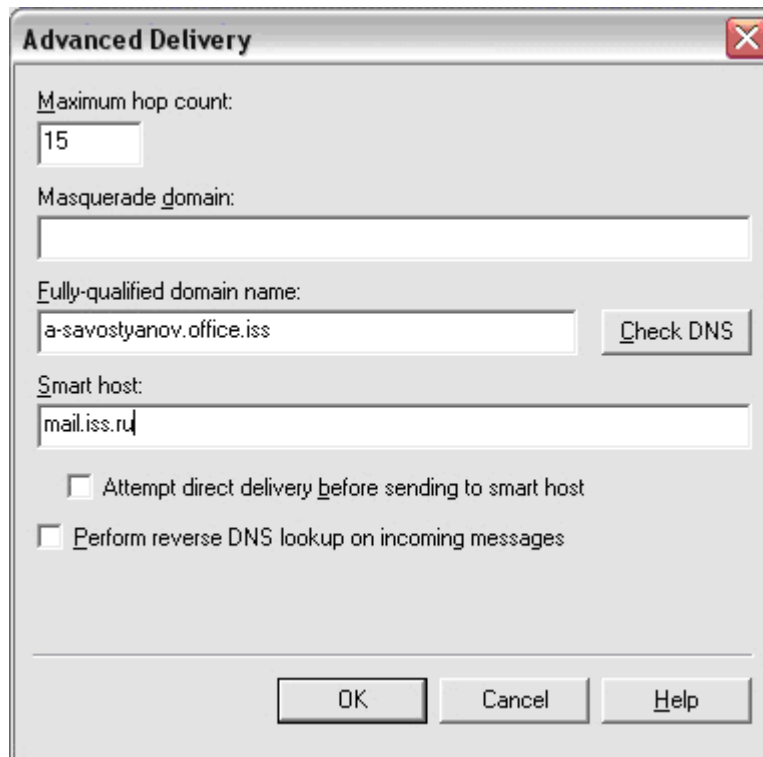


Figure 212. Mail routing remote server settings

7. Click **OK** to close SMTP server properties window and save all changes.
8. Choose **Action** → **Run** to run SMTP server service.

14.5.5 Win7/Win8.1/Windows Server Automatic Login Configuration

Note. All actions must be performed under local or domain administrator account.

Warning! Be careful when editing registry. Wrong use of the registry editor may result in serious problems requiring Operating System re-installation.

To activate automatic Windows login:

1. Open registry editor (**Start** → **Run** → **regedit**).
2. Choose `\HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` registry branch and specify the following value for `DefaultUserName` parameter: user name used for auto-login.
3. In the same branch create `DefaultPassword` string parameter and specify user password as its value. user password.

Note. If `DefaultPassword` parameter value is not specified, then auto-login will be deactivated.

4. In the same registry branch specify 1 value for `AutoAdminLogon` parameter.
5. Close registry editor and reboot the computer. Windows login will be performed automatically after the reboot.

To disable auto-login procedure or login to system under another user account, click-hold **Shift** button after logoff or Windows restart. To apply this procedure permanently, specify 1 value for ForceAutoLogon parameter in

\HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon registry branch.

Warning! After auto-login configuration, each person that can physically access the computer, will get access to its resources including all networks connected to this computer. In this case, password is publicly saved in registry. Registry branch is accessible in remote mode by members of the **Authorized Users** group. Therefore, auto-login procedure is justified when system physical security is guaranteed and registry access is forbidden for users without special permission.

14.5.6 Starting Interactive Services Detection Service under Win8/8.1/Server 2012 R2

Windows 8, Windows 8.1 and Windows Server 2012 R2 no longer allows interactive services, by default, which makes the **Interactive Services Detection service** unnecessary.

If you must run a legacy application that installs an interactive service on Windows 8, Windows 8.1 and Windows Server 2012 R2, the **Interactive Services Detection service** is required.

To start the **Interactive Services Detection service** do the following:

1. Open registry editor (**Start → Run → regedit**).
2. Choose HKLM\SYSTEM\CurrentControlSet\Control\Windows registry branch and change the NoInteractiveServices parameter value from 1 (default value) to 0.
3. Reboot the system.

After rebooting the computer start the **Interactive Services Detection service**.

14.5.7 Complete Disabling UAC under Win8/8.1/Server 2012 R2 with the help of System Registry

To completely disable **UAC** with the help of system registry editor do the following:

1. Open registry editor (**Start → Run → regedit**).
2. Choose HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System registry branch and change the EnableLUA parameter value from 1 (default value) to 0.
3. Reboot the system.

After rebooting the **User Account Control (UAC)** will be disabled on the computer.

14.5.8 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.

14.6 Appendix F. 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 by e-mail on Intelligent Security Systems Technical Support e-mail address (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:
 - (*) video capture cards serial number and Dallas code, 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.
 - video capture cards driver version.
 - total number of video servers, remote administrator 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, 95
 - Control, 95
 - Full access, 95
 - Inherited rights, 95
 - No access, 95
 - View, 95
- account,
 - postgres, 50
- Action, parameter, 236
- Activate Desktop, property, 98
- Active Directory Storage object description, 91
- Add all property,
 - Monitor, 173
- Add all, parameter,
 - Audio Player, 218
- Additional information, property, 91
- Administration Mode, 51
- Alarm condition, parameter, 221
- Alarming, property, 156
- All property,
 - Archiver, 167
 - Archiver Dialog, 197
- Allow auto login for User(s), property,
 - Computer, 98
- Allow configure system, property, 95
- Analyze reduced FPS stream, max FPS parameter, 157
- Archive Converter Dialog object description, 196
- Archive Converter object description, 161
- Archive converting, temporary files, 135
- Archive Engine property, 176
- Archive recording, 134
 - frames number, 134
 - frames queue, 135
 - free disk space, 134
 - long-term archive, 135
 - threshold, 134
- Archive, tab,
 - Computer, 97
- Archiver Dialog object description, 197
- Archiver object description, 165
- Armed always, property, 156
- Attachment, parameter,
 - E-mail Message, 230

- Audible Notification Service object description, 231
- Audio Capture Device object description, 212
- Audio Player object description, 217
- Audio property, 98
- Automation subsystem,
 - Macros, 232
 - Scripting, 232

B

- Base, parameter,
 - Media Client, 183
- Blinding detection property,
 - Camera, 146
- Block system shutdown in NT service mode, 99
- Bolid, integration, 248
- Bound, parameter, 216

C

- Camera,
 - Image settings, 133
- Camera alarm mode control, parameter,
 - Media Client, 180
- Camera is defocused when camera sharpness reduces by, parameter,
 - Defocus detector, 150
- Camera is focused, parameter,
 - Defocus detector, 151
- Camera object description, 140
- Camera property,
 - Monitor, 173
- Camera, setting up, 200
- Cameras and Microphones list, parameter,
 - Media Client, 180
- Cameras, parameter,
 - RTSP Server, 168
- CC, parameter, 230
- CCTV keyboard or joystick object description, 222
- Cells, parameter,
 - Layout, 153
- Center on screen, property, 125
- Channel to play, parameter, 218
- Channel, parameter,
 - Microphone, 216
 - Relay, 221
 - Sensor, 220
- Channel, parameter,
 - Audible Notification Service, 231
- Channel, property,
 - Camera, 140
- Check syntax, button,
 - VB/JScript program, 239
- Checking period, parameter,

- Checking period, parameter,
 - Defocus detector, 150
- Clear all, parameter,
 - Audio Player, 218
- Clear all, property (Zone), 157
- Codec property,
 - Archive Converter (Audio), 163
- Codec, property,
 - Archive Converter (Video), 163
- Compression property,
 - Monitor, 173
- Compression, parameter,
 - Microphone, 216
- Compression, parameter,
 - Audio Player, 218
- Computer object description, 96
- Computer's role, property, 97
- configuration,
 - quick steps, 256
- configuration examples, 197
 - domain for LDAP provider, 115
 - domain for Windows NT provider, 115
 - standalone configuration, 198
 - Video Server and Operator Workstation, 199
- Configuration, property, 82
- Contrast property,
 - Camera, 146
- Contrast, property,
 - Zone, Motion detection, 156
- Create level, button,
 - Map, 118

D

- Database object description, 88
- Date, Period, parameter, 234
- Days of week, parameter, 234
- Days property, 167
- Delay, parameter,
 - Microphone, 216
- Department object description, 90
- Desktop object description, 116
- Detection area, parameter,
 - Defocus detector, 150
- Device, parameter, 230
- Digital zoom, parameter,
 - Media Client, 180
- Disable alarm mode control property, 176
- Disable frame export and print property, 176
- Disable if Event Viewer exists, parameter, 231
- Disable image adjustment property, 176
- Disable PTZ control via mouse property, 176
- Disable recording control property, 176

- Disable saving data into local Protocol DB, property, 98
- Disable shared PTZ control property,
 - Camera, 147
- Disable system shutdown for user, property, 94
- Disable visualization property, 176
- Disable wiper control property, 176
- Display area,
 - Map, 117
- Display property,
 - Archive Converter Dialog, 196
 - Archiver Dialog, 197
- Display titles property, 176
- Display, parameter,
 - Map Window, 122
 - Media Client, 180
- Display, property,
 - Event Viewer, 123
- Drive, property, 97
- DSAdmin Utility, 269
- DTR, RTS property, 160
- Duration of post-recording property,
 - Camera, 145
- Duration of pre-recording property,
 - Camera, 145
- Dwell time property, 174

E

- EdgeStorage Sync object description, 171
- Edit, button,
 - VB/JScript program, 239
- E-mail Message object description, 229
- E-mail Message Service object description, 228
- E-mail, property, 91
- Enable Cameras and Microphones grouping, parameter,
 - Media Client, 180
- Enable shared Views setup, parameter,
 - Media Client, 185
- Event redirection property, 84
- Event Viewer object description, 123
- Event, parameter,
 - Macro, 235
- events,
 - event redirection, 84
- Events, property, 126
- Export,
 - Audio, 262
 - Video, 261
- Export engine property, 176
 - Archive Converter Dialog, 196
- Export to property, 163
- Export video with audio, parameter, 163
- External Window object description, 123

F

- Fetch property, 166
- File type property, 162
- Fill all, property, 157
- For IP-device, parameter, 213
- For Sound Card or Sound Circuits of the TVISS Video Capture Cards, parameter, 214
- For SoundMixer module, parameter, 214
- Forbid to hide interface, property, 95
- Format, property,
 - Video Capture Device, 139
- FortNet, integration, 250
- FPS divider property, 163
- fps property,
 - Monitor, 173
- FPS reduction performed on server property, 163
- Frame Export, parameter,
 - Media Client, 181
- Frames per second property, 167
- Free GB, property, 98
- From, parameter, 229
- Full FPS on alarm property,
 - Camera, 145

G

- Gain, parameter, 216
- Grid, parameter,
 - Layout, 153
- gtUSB Configuration Utility, 266
- Guardant key, 258
 - installation, 21

H

- Hardware Acceleration property, 175
- Hardware acceleration, parameter,
 - Media Client, 181
- Hardware, parameter, 221
- HDD property, 166
- Hidden, parameter, 235
- Hide, parameter,
 - Audio Player, 217
- High resolution stream for display, parameter,
 - Camera, 143
- High resolution, parameter,
 - Media Client, 183
- Holidays, parameter,
 - Security Zone, 234
- Holidays, property,
 - Security Zone, 84
- Host property,

- Bolid integration, 249
- FortNet integration, 250
- Yantar integration, 251
- Host, parameter,
 - Remote system, 106
- HTML Dialog object description, 125
- HTML Form object description, 124
- HTTP Event Gate object description, 240
- HTTP port, parameter,
 - RTSP Server, 168

I

- ID, 54
- Id property,
 - Archiver, 167
 - Archiver Dialog, 197
 - Monitor (Cameras), 173
 - Monitor (Display), 172
- Id property (PTZ Device), 161
- Id, parameter,
 - Macro (Actions), 236
 - Macro (Event), 235
- ID, parameter,
 - Audio Player, 217
- Id, property,
 - Department, 90
 - User Account, 91
- Identifier (Presets) property,
 - Camera, 147
- Identifier (Tours), parameter,
 - Camera, 148
- IIDK Interface object description, 239
- Image Processor object description, 167
- Import Cameras with IDs, parameter,
 - Remote system, 106
- Import, button,
 - Map, 118
- Import/Export, parameter,
 - Program, 237
- Inner zone property, 159
- Integration with 3rd Party Systems, 233
- IP address, property, 139
 - Computer, 97
- IP-Device Manager object description, 61
- ISS Database Update Utility, 270
- ISS Hardware Report Utility, 258
- ISS Media Export Utility, 261
- ISS Object Types Database Editor, 271
- ISS Startup Configuration Utility, 268
- ISS System Report Utility, 259

J

joystick,
 configuring, 210

K

keyboard shortcuts, 252

L

Language, parameter,
 VB/JScript program, 238
Layout object description, 152
Layouts panel, parameter,
 Media Client, 185
Layouts type property, 173
Level, parameter,
 Microphone, 216
License key, 22
 expiration date remainder, 60
 expiration date remainder setup, 61
 request, 22
 updating, 60
Light Detector object description, 158
Local, parameter, 235
Log on using Secure Password Authentication (SPA),
property, 93
Login property,
 Bolid integration, 249
 Yantar integration, 251
Login, Password, parameter, 229
Low resolution stream for display, parameter,
 Camera, 143
Low resolution, parameter,
 Media Client, 183

M

Macro object description, 234
Map,
 Adding level, 119
 Base image, change, 120
 Child level, create, 120
 layers image, 118
 Level link, 120
 Level, change text color, 120
 Level, Delete, 120
 Level, rename, 120
 Objects, deleting, 121
 Objects, moving, 121
 Objects, positioning, 121
 Objects, rotating, 121
 Objects, searching by name, 121

 working principles, 118
Map object description, 116
Map Window object description, 122
Map, parameter,
 Map Window, 122
Maximum Protocol DB size, property, 99
Memory frames, property, 157
Message field, parameter,
 E-mail Message, 230
Message, parameter,
 Short Message, 231
Microphone object description, 215
Microphone tree, parameter,
 Media Client, 191
Microphone, property,
 Camera, 141
Min, Max property, 175
Minimum/Maximum, parameters,
 Media Client, 183
Mode property, 174
Model, parameter,
 Audio Capture Device, 213
Model, property,
 Video Capture Device, 138
Monitor object description, 171
Monitoring center agent object description, 105
Multi-cell zoom without stream switching, parameter,
 Media Client, 181

N

Name, 54
 Map, 117
Name of the system, property, 82
Name pattern, property, 164
Name property,
 Archiver Dialog, 197
Name property (PTZ Device), 161
Name, property,
 Department, 90
 User Account, 91
New password, parameter,
 System, 83

O

Object tree, 52
 Child object, 52
 Map, 117
 Parent object, 52
Object tree, parameter,
 Media Client, 187
OK/Cancel, property (buttons), 157

Operator reaction on alarm event, property, 123
Operator, property, 95
Outer zone (secondary) property, 159
Outer zone property, 159

P

Pack, parameter, 230
Page dwell time when auto scrolling, parameter,
 Media Client, 181
Pan/Tilt/Zoom, property,
 Camera, 141
Parameters, parameter, 236
Parity property, 160
Password property,
 Bolid integration, 249
 Monitor, 174
 Yantar integration, 251
Password, property,
 User Rights, 95
 Video Capture Device, 139
PCI channel property,
 setting up, 137
PCI channel, property, 139
Phone, parameter,
 Short Message, 231
Phone, property,
 User Account, 91
Please retype, password,
 System, 83
Port property,
 Bolid integration, 249
 FortNet integration, 250
 PTZ Controller, 160
Port, parameter,
 E-mail Message Service, 229
 Remote system, 106
Port, property,
 Active Directory Storage, 92
Program object description, 236
Program, property,
 External Window, 124
Protect with password property,
 Camera, 145
Protocol database length, property, 84
Protocol property,
 Relay, 221
Protocol, parameter,
 E-mail Message Service, 229
Protocol, property,
 Video Capture Device, 139
Provider, property, 92
Providers, property, 95

PTZ channel property,
 Camera, 147
PTZ control via mouse, parameter,
 Media Client, 181
PTZ Control, parameter,
 Media Client, 180
PTZ Controller object description, 159
PTZ Device object description, 160
PTZ protocol property, 160
 Camera, 147

Q

Quality property,
 Archive Converter (Audio), 163
Quality, property,
 Archive Converter (Video), 163
 Zone, 157
Quick audio export property, 163
Quick video export property, 163

R

Record buffer settings, 133
Recording control, parameter,
 Media Client, 180
Recording mode, property,
 Camera, 144
Reduce frame rate property, 163
Reduce max FPS to property,
 Camera, 145
regedit system registry editor, 135
Relay number, parameter, 221
Relay, object, description, 221
Remote system object description, 106
Remove after property,
 Camera, 145
Rights, property, 94
RTSP port, parameter,
 RTSP Server, 168
RTSP Server object description, 167
Run macro at start, property, 84
Run on, parameter,
 Program, 236

S

Samplerate, parameter, 213
Save configuration property, 83
Scale, parameter,
 Map, 117
Script text area, parameter,
 Program, 237
Search, box,

- Search, box,
 - Map, 117
- Security Zone object description, 83
- SecurOS Control Service utility, 268
- SecurOS Logging, 59
- Sensitivity property,
 - Light Detector, 159
- Sensor, object, description, 220
- Server, property, 92
- Servers to connect, tab,
 - Computer, 98
- Short Message object description, 230
- Short Message Service object description, 230
- Show alarm cameras only property, 174
- Show alarmed levels, parameter,
 - Map Window, 122
- Show all cameras from table above property, 174
- Show all zones, property, 157
- Show Camera ID, parameter,
 - Media Client, 181
- Show camera IDs property, 176
- Show camera list property, 174
- Show control toolbar property, 174
- Show level tree, parameter,
 - Map Window, 122
- Show PTZ control property, 176
- Show single active camera only property, 175
- Single-cell zoom with stream switching, parameter,
 - Media Client, 181
- Size property,
 - Camera, 146
- Size, property,
 - Zone, 156
- Smart Search, property, 156
- SMTP Server requires authentication, parameter, 229
- SMTP Server, parameter, 228
- SNMP agent object description, 111
- Sound card, parameter,
 - Audible Notification Service, 231
 - Audio Player, 217
- SoundMixer object, 212
- Source, parameter, 218
- Speed property, 160
- Split into files up to property, 162
- Standard layouts, parameter,
 - Media Client, 183
- Store at least property,
 - Camera, 145
- Store bookmarks and alarms, property, 99
- Stream 1, parameter,
 - Camera, 142
- Stream 2, parameter,

- Camera, 142
- Stream 3, parameter,
 - Camera, 143
- Stream for recording, parameter,
 - Camera, 143
- Stream property,
 - Monitor, 175
- Streams for display, parameter,
 - Camera, 143
- Subject, parameter, 230
- superuser, 58
- System object description, 82

T

- technical support,
 - gathering system information utility, 258
 - how to get, 9
 - how to prepare service information, 289
- Text color,
 - Map, 117
- Time intervals, parameter, 234
- Time of acknowledgment of alarm event by the operator, property, 123
- Time to display Camera after alarm ends, parameter,
 - Media Client, 179
- Time Zone object description, 233
- Time zone, parameter,
 - Program, 236
 - VB/JScript program, 239
- Title (Presets) property,
 - Camera, 148
- Title (Tours), parameter,
 - Camera, 148
- Title property,
 - Archiver, 167
- Title, parameter,
 - Macro (Actions), 236
 - Macro (Event), 235
- To, parameter, 229
- Token property,
 - Monitor, 173
- Type property,
 - Microphone, 216
- Type, parameter,
 - Audio Capture Device, 213
 - Macro (Actions), 235
 - Macro (Event), 235
- Type, property,
 - Video Capture Device, 138

U

- Update configuration, button,

- Update configuration, button,
 - Remote system, 107
- Use credentials provided at system login, property, 92
- Use default directory, property, 126
- Use event filter, property, 99, 123
- Use only selected Cameras, parameter,
 - Media Client, 187
- Use only selected microphones, parameter,
 - Media Client, 191
- Use only selected shared Views, parameter,
 - Media Client, 185
- Use primary domain controller, property, 92
- Use remote Camera IDs, parameter,
 - Remote system, 106
- Use remote device property, 160
- Use secure connection, parameter, 229
- Use SSL, property, 92
- Use standard script file, property, 125
- User account object, 114
- User Account object description, 90
- User name, Password, property, 92
- User Rights object,
 - settings for LDAP provider, 115
- User rights object,
 - settings for Windows NT provider, 115
- User Rights object description, 93
- User, property,
 - Video Capture Device, 139
- User's Layouts, parameter,
 - Media Client, 183

V

- VB/JavaScript program object description, 237
- Video Capture Device object description, 137
- Video Monitor,
 - additional settings, 133
- Video, property,
 - Computer, 98
 - Zone, 157
- View object,
 - Add to the Views quick access bar, 195
 - Create, 193
 - Creating on the base of existing view, 193
 - Delete, 194
 - Delete from the Views quick access bar, 195
 - Edit, 194
 - Rename, 194
 - Types, 191
- View object description, 154
- Viewing, property,
 - Camera, 141
- Views list, parameter,

- Media Client, 185
- Views quick access bar,
 - Setting up with the help of context menu, 195

W

- W, H, parameters,
 - Media Client, 180
- Wide layouts, parameter,
 - Media Client, 183
- Wiper control, parameter,
 - Media Client, 181
- Wiper property,
 - Camera, 147
- Work in selected Time Zone, parameterDefocus detector, 150
- Work with audio, parameter,
 - Media Client, 190
- Work with Views, parameter,
 - Media Client, 185
- Working mode, parameter,
 - Media Client, 178
- Write secondary event parameters into Protocol DB, property, 99

X

- X, Y, parameters,
 - Media Client, 180
- X, Y, property, 125
- X, Y, W, H property,
 - Archive Converter Dialog, 196
 - Archiver Dialog, 197
- X, Y, W, H, parameter,
 - Audio Player, 217
- X, Y, W, H, property,
 - Event Viewer, 123
 - External Window, 124
 - HTML Form, 125
 - Map, 122
 - Monitor, 173

Y

- Yantar, integration, 251

Z

- Zone,
 - working principles, 131
- Zone object description, 154
- Zone types, property, 155