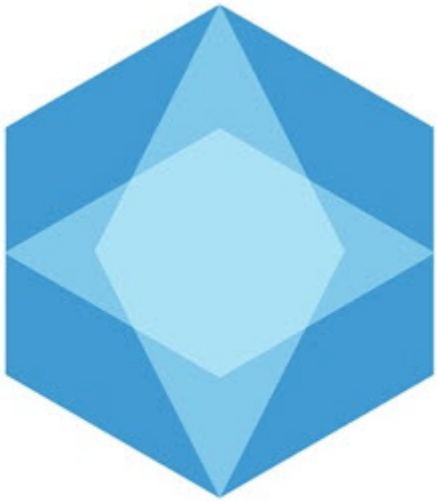


Monitoring

Administrator's Guide

Monitoring 14.0 (english)

Last update 12/08/2023

Table of Contents

1 Introduction

On the page:

1.1 Document purpose

This document, Monitoring: Administrator's Guide, is a reference aid for system administrators, configuration and installation specialists, and users with administrator rights on the *Monitoring of technical condition* software (hereinafter referred to as *Monitoring*).
This guide describes the following:

1. Purpose of *Monitoring.*
2. Hardware and software requirements for *Monitoring.*
3. Installation procedure for *Monitoring.*
4. Configuration of *Monitoring* components.

1.2 Purpose of Monitoring

Monitoring is designed to automate the activities of personnel at service companies involved in the operation of Intellect-powered video surveillance systems. The purpose of *Monitoring* is to improve the quality of operation for such video surveillance systems.

2 Monitoring general description

2.1 Features of Monitoring

Monitoring receives, records, and visualizes messages about the state of security system components, based on the following key parameters:

1. Camera operability.
2. Network functioning.
3. Operability of video subsystem software.
4. Amount of recorded video.
5. Hard disk operability.
6. Operability of fire/security and access control systems.
7. UPS signals.

In addition, *Monitoring* allows you to control the actions of *Monitoring* operators: recording is performed of whether an alarm has been accepted, how much time passed before the alarm was accepted, and so forth. The built-in system of statistical and analytical reports allows you to generate reports on the system operation: reports on alarms, downtime, statistics on security system operation, and more.

> **Note**
>
> If there is no activation key, then *Monitoring* operates in the demo mode for two months from 8:00 am to 12:00 am.

2.2 General information about Monitoring as a Service

Monitoring software, installed as a service (see Installing Monitoring), is launched before user authorization in Windows OS and before launching Windows applications (including the Explorer, which is used to launch interfaces of both Windows OS and various applications installed on server).

When the active account is changed, the following *Monitoring* modules are restarted:

- On *Agent of Control* — videosrv.exe;
- On *Server of Control* — videosrv.exe and loadersstv.exe;
- On *Central Server of Control* — CentralNetServer.exe.

If *Monitoring* is installed as a service, and the connection to the database is established using Windows credentials, then to ensure the operation on any user account other than the one who installed *Monitoring*, the user should have the appropriate rights to SQL server.

2.3 Monitoring restrictions

In the *Monitoring* software package restrictions are imposed when creating systems of technical condition monitoring:

1. Maximal number of **Agent of Control** objects that can be connected to a *Server of Control* is 2000.
2. Maximal number of **Partition of Control** objects being child objects for an **Agent of Control** is 255.
3. Maximal number of cameras which a **Partition of Control** can handle is 64.
4. Maximal number of cameras which a **Agent of Control** can handle is 320.

3 Hardware and software requirements

On the page:

3.1 Operating system requirements

Monitoring is provided as executable modules that that can be run on the operation systems supported by the Intellect software (see the Operating system requirements chapter in the *Intellect* software Administrator's Guide).

The software is compatible with standard operating system settings. On Windows Vista and later, UAC must be disabled. In Windows 8, 8.1 and 10 it is necessary to configure security policies in order to entirely disable UAC (configuring security policies is described in the Intellect software Administrator's Guide).

For the *Server of Control* and the *Central Server of Control* to operate, there must be an available database server. During installation of *Intellect*, MS SQL Server 2014 Express is installed to a "clean" (fresh) system.

The *Server of Control* and the *Central Server of Control* are compatible with the following servers:

- MS SQL Server 2008 R2
- MS SQL Server 2012
- MS SQL Server 2014

3.2 Hardware requirements

Monitoring can run on PCs that meet the following minimum hardware requirements:

- Intel Core i5 750 CPU
- 2 GB RAM
- 200 GB HDD
- NIC
- Graphics card with overlay support

4 Installing Monitoring

4.1 General description of Monitoring distribution kit

Monitoring is supplied as a software installation package (distribution kit). The current version of the distribution kit can be downloaded from the official AxxonSoft website.

The distribution kit contains all the necessary software components for installing the *Monitoring* software package on a base computer.

The distribution kit allows you to install, restore and remove the *Monitoring* software package.

Attention!

- Prior to installing, restoring or removing the *Monitoring* software package, the *Intellect* operation should be shut down.
- Administrator rights are required for installing, restoring or removing *Monitoring*.

4.2 Installation options

Monitoring can be installed in one of the following configurations:

Installation type	Purpose	License features	Additional components	Base Intellect installation type
Agent of Control	Is to be installed on the object for which receiving, recording, and visualizing messages about the state of security system components is required.	The program key, intellect.sec, should contain the **Agent of Control** object.	In addition to *Agent of Control* modules, the VideoSrv communication program is installed. It interacts with similar programs on the *Server of Control*.	Server/RAW

Server of Control	Is to be installed on the object from which the *Agents of Control* are monitored.	The program key, intellect.sec, should contain the **Server of Control** object.	In addition to *Agent of Control* modules the following components are installed: 1. VideoSrv communication module. It interacts with similar programs on the *Agent of Control*. 2. Data loader for Monitoring to record information collected by VideoSrv into the database.
Additional workplace	This is the *Server of Control* version which is installed without additional components and connects to the existing database of the main *Server of Control* while interface objects are created on the local computer.	*Intellect* distributed system configuration is not required for the additional workplace operation. The **Additional workplace** object is to be specified in the "intellect.sec" license key that is located on *Server of Control* in order to allow using the *Additional workplace* software.	-

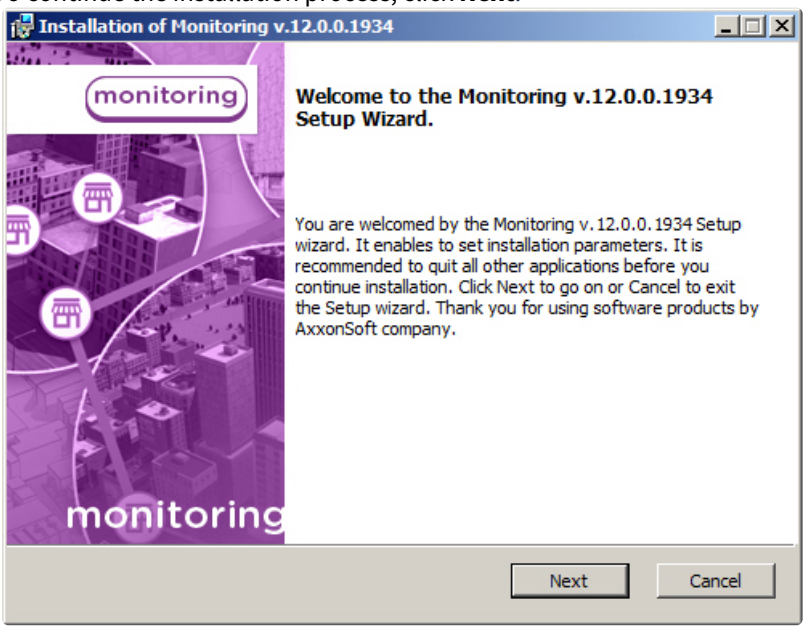
Central Server of Control	Allows to combine several *Servers of Control* into a single system.	The program key, intellect.sec, should contain the **Central Server of Control** object.	In addition to *Central Server of Control* modules the following components are installed: 1. CentralNetServer communication module. It interacts with VideoSrv modules on the *Server of Control*. 2. Data loader for *Central Server of Control* which records the information received from CentralNetServer into the database.
Additional workplace of CSC	This is the *Central Server of Control* version which is installed without additional components and connects to the existing database of the main *Central Server of Control* while interface objects are created on the local computer.	*Intellect* distributed system configuration is not required for the additional workplace operation. The **Additional workplace of CSC** object is to be specified in the "intellect.sec" license key that is located on *Central Server of Control* in order to allow using the *Additional workplace* software.	-

4.3 Agent of Control Installation

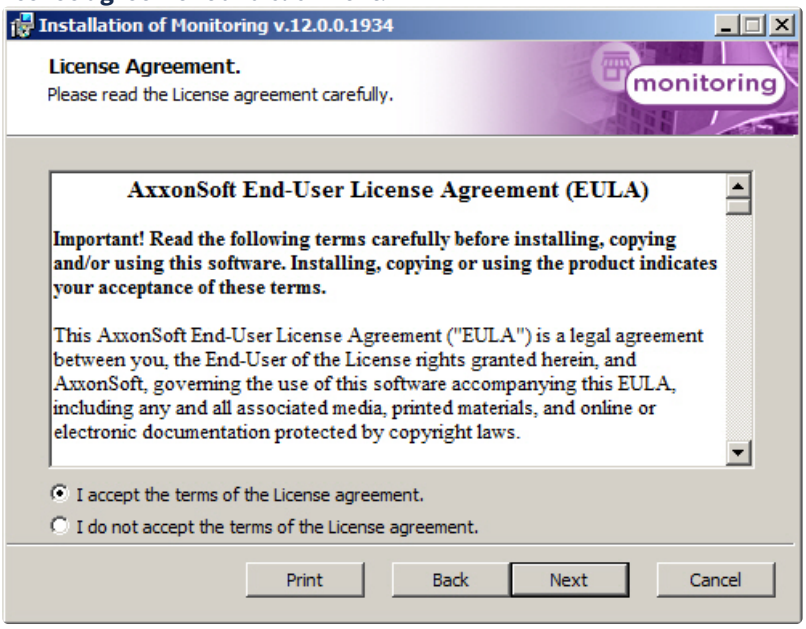
The *Monitoring* software is installed as a part of the *Intellect* software. Information about compatibility of the *Intellect* software versions and *Monitoring* is presented in the Obsolete. General information about product releases and versions compatibility section.

To install *Monitoring* software in the *Agent of Control* configuration, do the following:

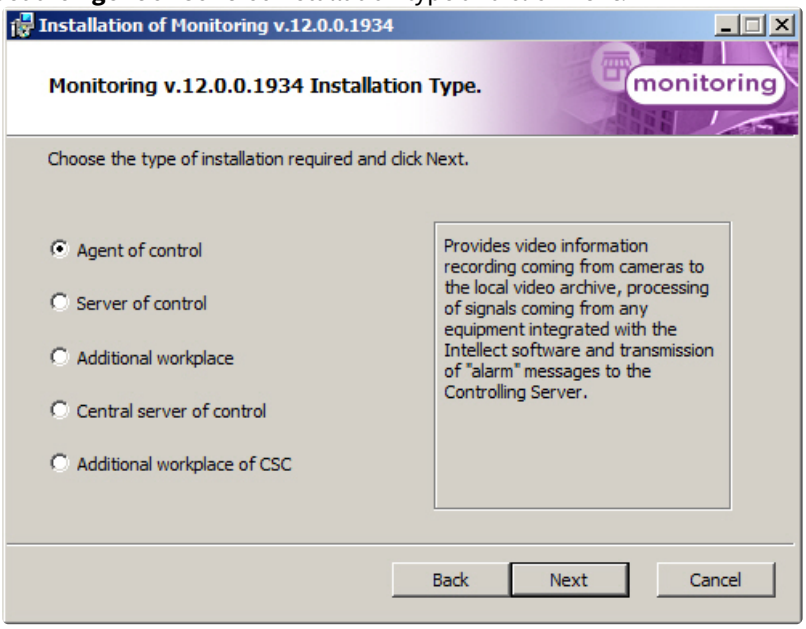
1. In the root directory of the distribution package, run the setup.exe executable file.
2. To continue the installation process, click **Next**.



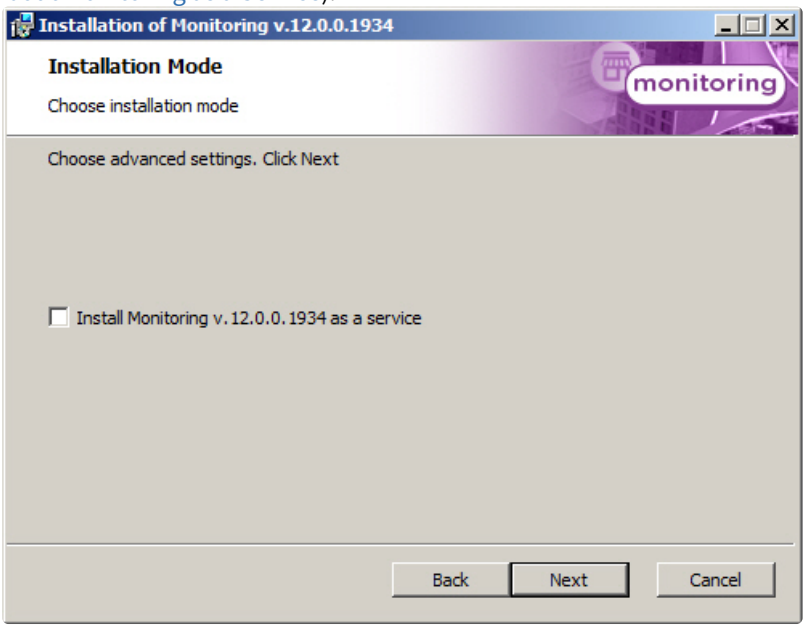
3. Read the terms of the license agreement carefully. Then set the radio button to **I accept the terms of the License agreement** and click **Next**.



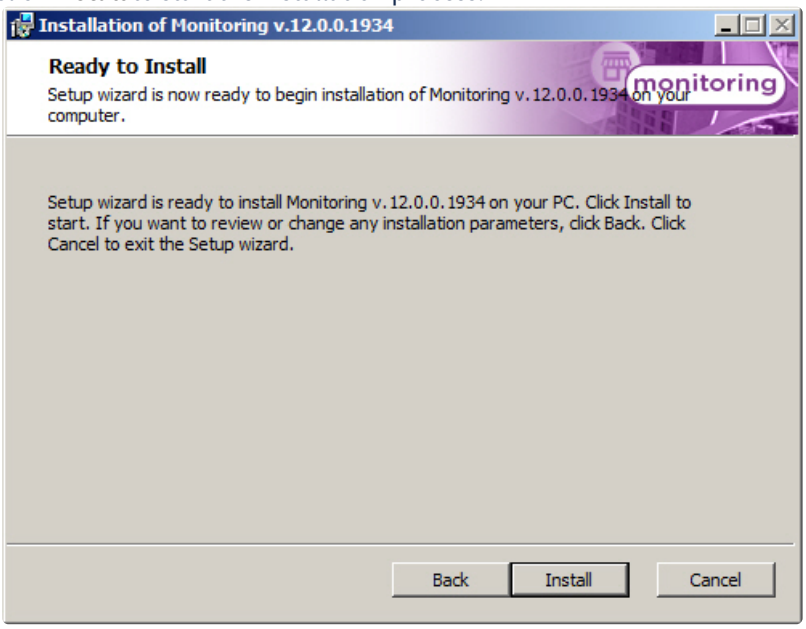
4. Set the **Agent of Control** installation type and click **Next**.



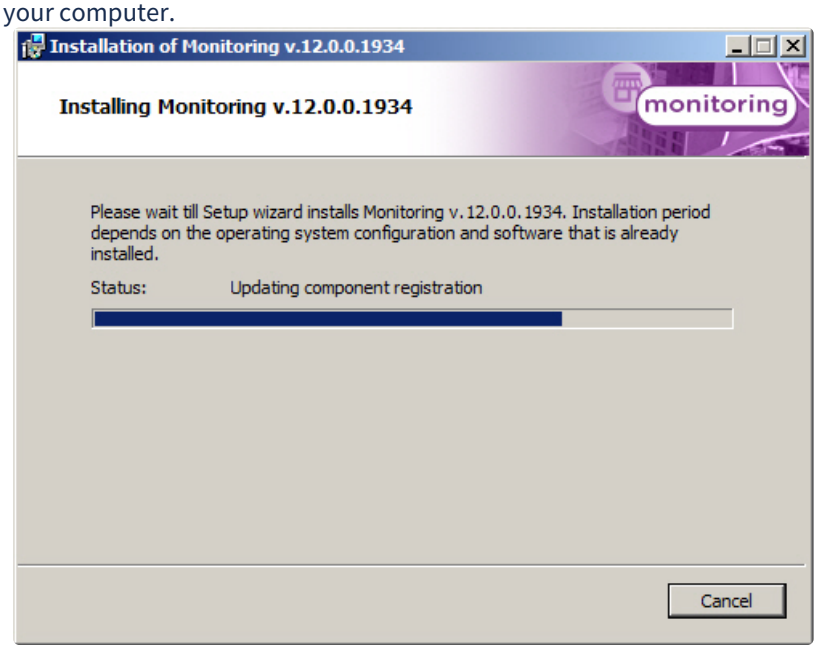
5. If *Intellect* software is installed as a service, and it is necessary that *Monitoring* is also installed as a service, then set the **Install Monitoring as a service** checkbox and click **Next** (for details, see General information about Monitoring as a Service).



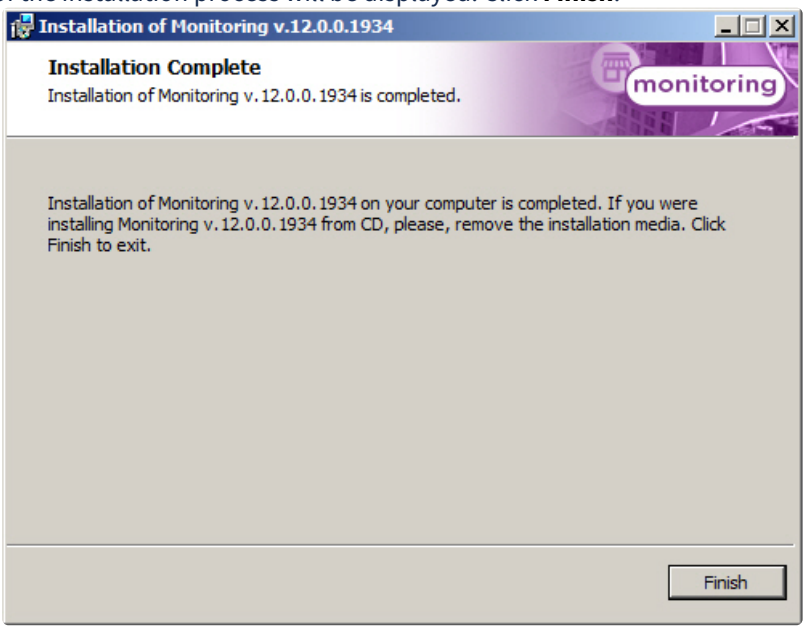
6. Click **Install** to start the installation process.



7. As a result, the necessary components of the *Monitoring* software package will be copied to hard drive of your computer.



8. After all software components are successfully copied on your hard drive, the message about the completion of the installation process will be displayed. Click **Finish**.



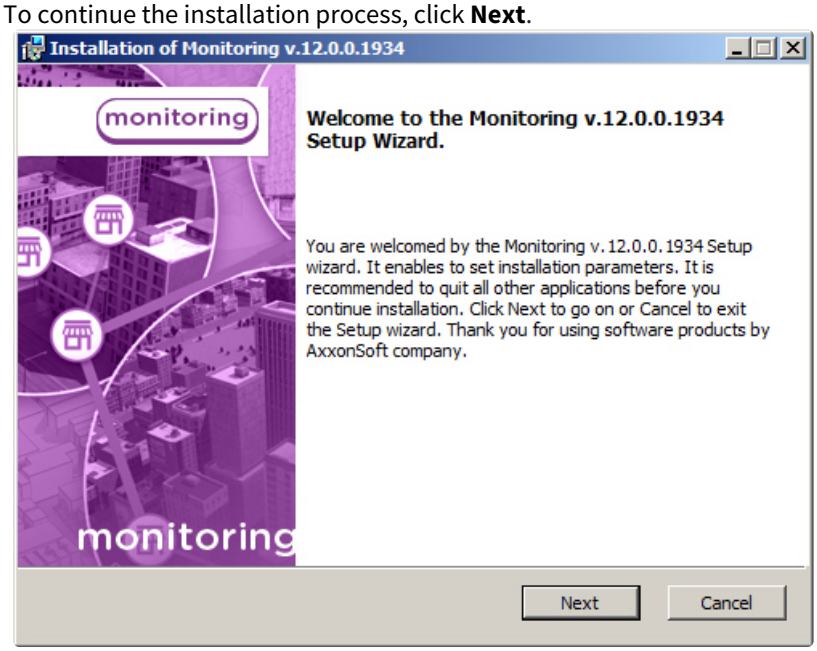
Installation of *Agent of Control* is now complete.

4.4 Server of Control Installation

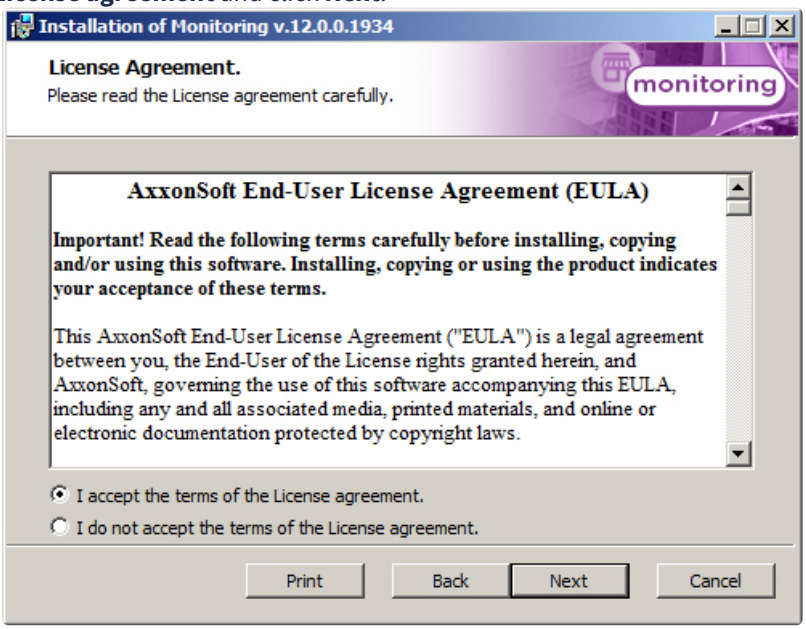
The *Monitoring* software is installed as a part of the *Intellect* software. Information about compatibility of the *Intellect* software versions and *Monitoring* is presented in the Obsolete. General information about product releases and versions compatibility section.

To install *Monitoring* software in the *Server of Control* configuration, do the following:

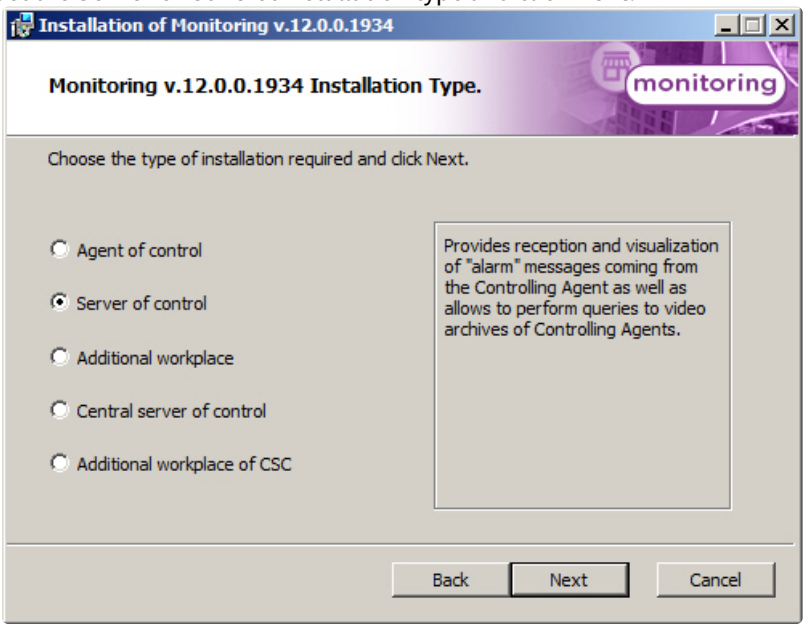
1. In the root directory of the distribution package, run the setup.exe executable file.
2. To continue the installation process, click **Next**.



3. Read the terms of the license agreement carefully. Then set the radio button to **I accept the terms of the License agreement** and click **Next**.

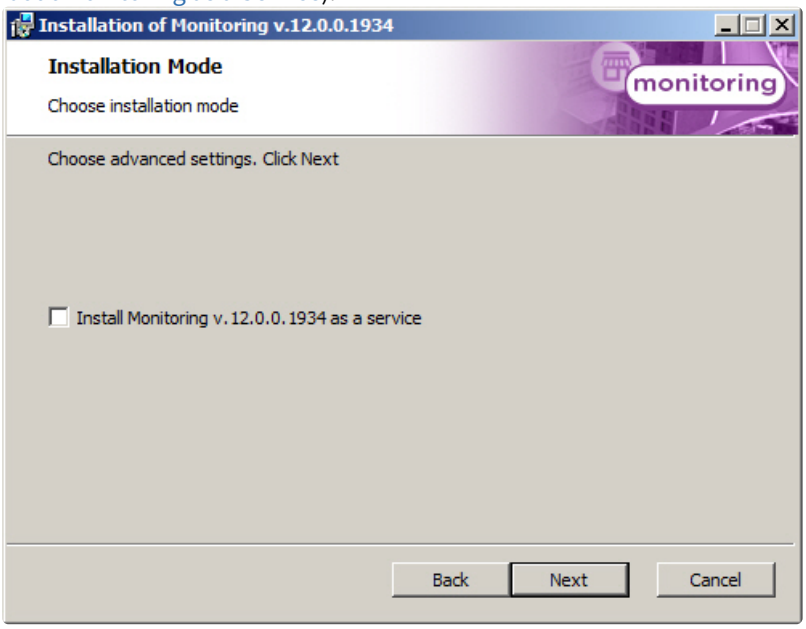


4. Set the **Server of Control** installation type and click **Next**.



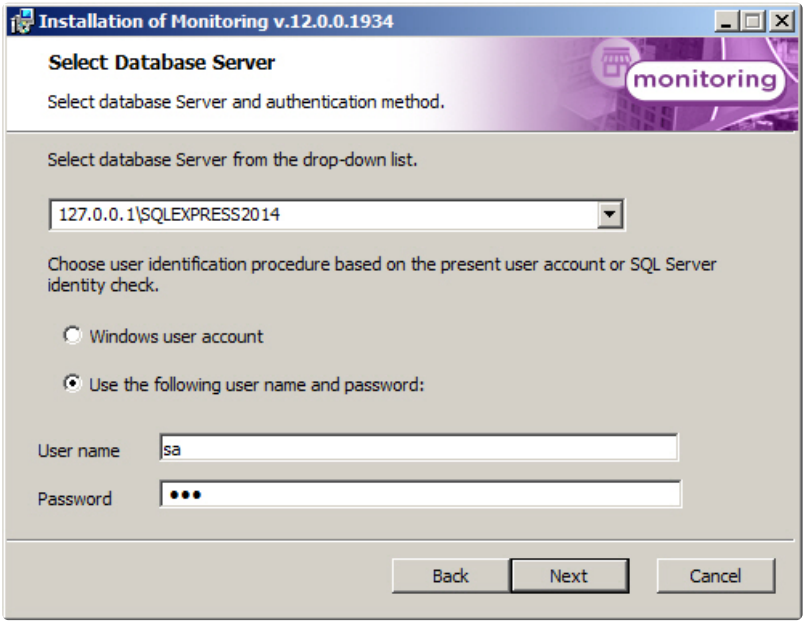
5. If *Intellect* software is installed as a service, and it is necessary that *Monitoring* is also installed as a service, then set the **Install Monitoring as a service** checkbox and click **Next** (for details, see General information

about Monitoring as a Service).



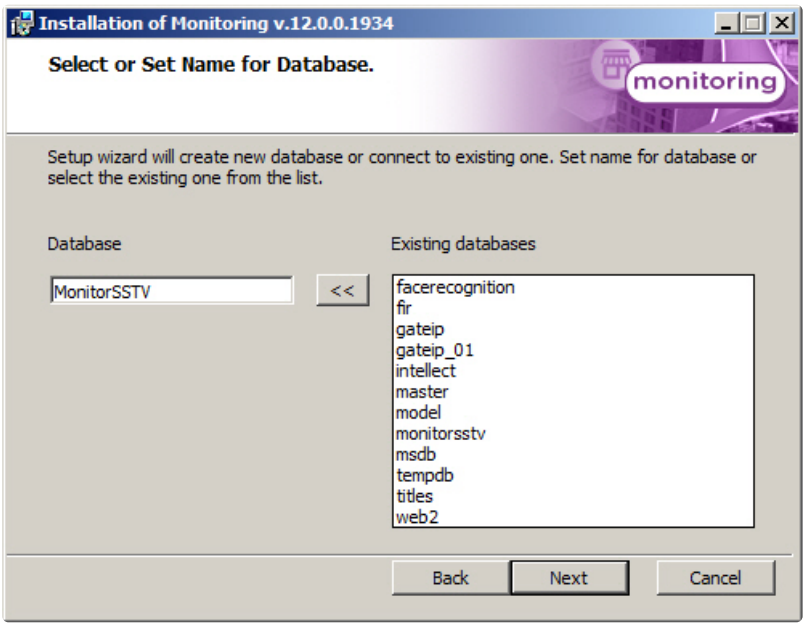
6. Select the database MS SQL Server and specify the authorization parameters for connection. For details, see Installation of INTELLECT™ software as a Server/Remote administrator workplace. To continue the installation process, click **Next**.

> **Note.**
>
> In the **Select database Server from the drop-down list** field specify the **127.0.0.1** value instead of computer name or "(local)" value, e.g. "127.0.0.1\SQLEXPRESS". Otherwise *Server of Control* will lose connection with its local database when the network cable is disconnected.

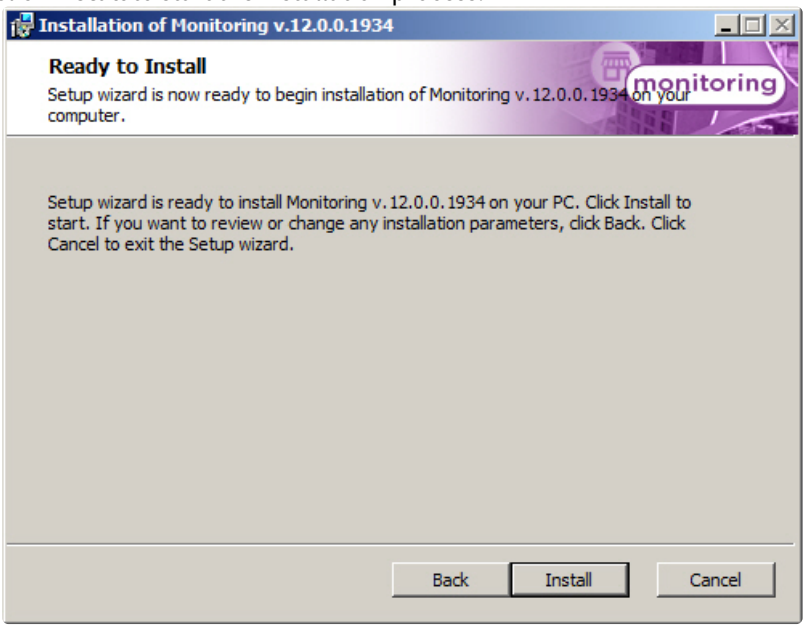


7. In the **Database** field specify the name of the database or select it on the right part of the window in the list of databases, which are created in the server, and click **<<**. Then click **Next**.

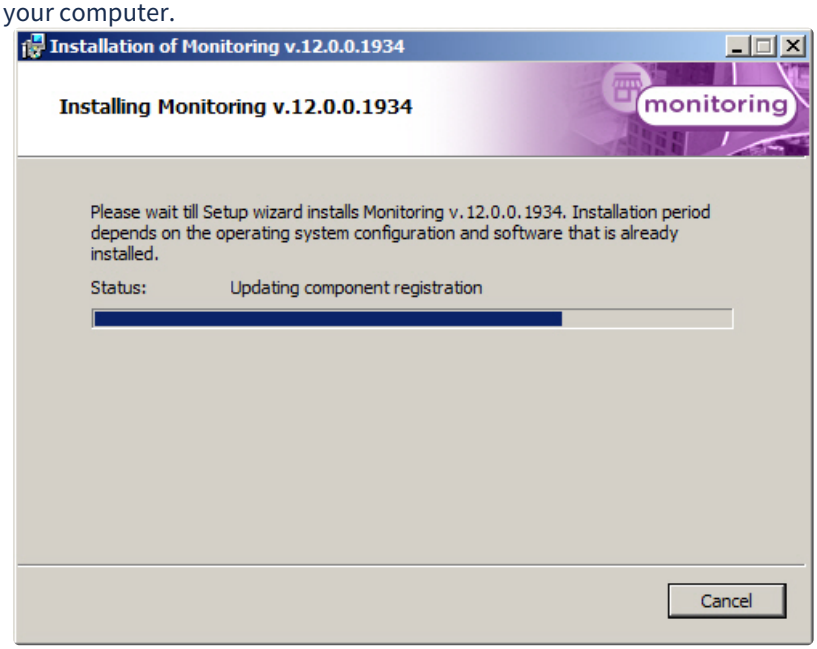
> **Note.**
>
> By default, the name of the database is "MonitorSSTV" and its files will be stored in the SQL Server folder.



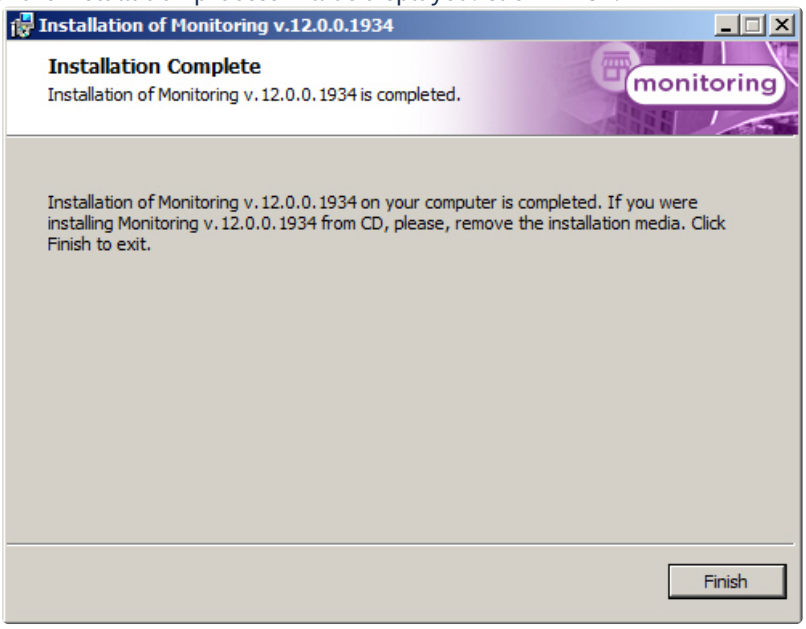
8. Click **Install** to start the installation process.



9. As a result, the necessary components of the *Monitoring* software package will be copied to hard drive of your computer.



10. After all software components are successfully copied on your hard drive, the message about the completion of the installation process will be displayed. Click **Finish**.



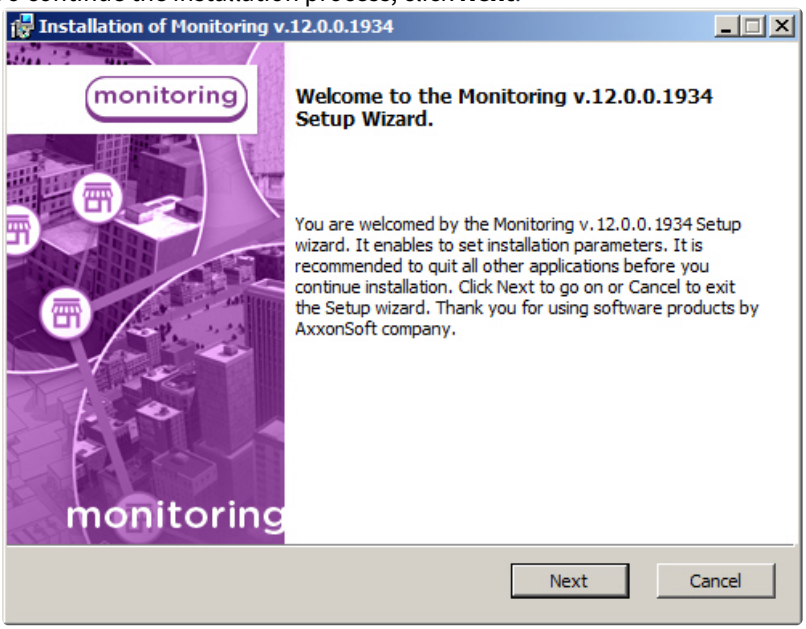
Installation of *Server of Control* is complete.

4.5 Additional workplace installation

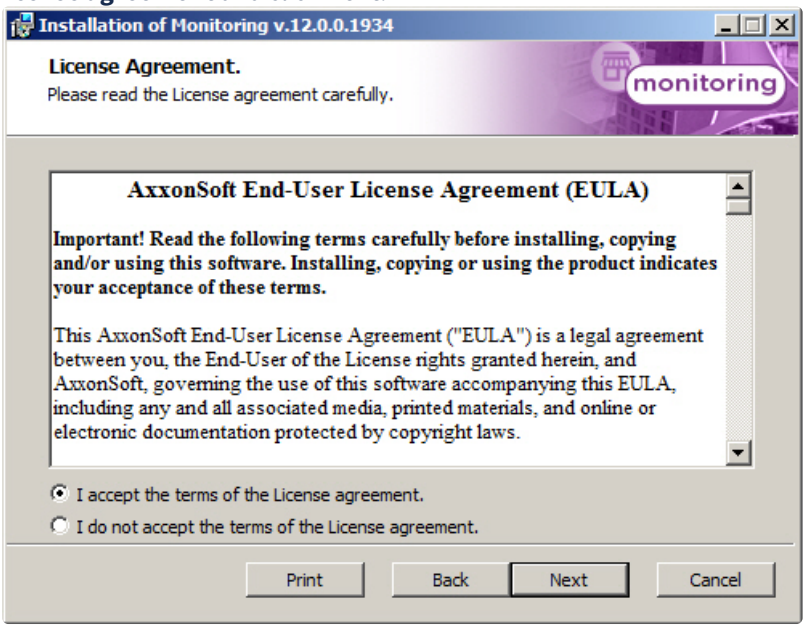
The *Monitoring* software is installed as a part of the *Intellect* software. Information about compatibility of the *Intellect* software versions and *Monitoring* is presented in the Obsolete. General information about product releases and versions compatibility section.

To install *Monitoring* software in the *Additional workplace* configuration, do the following:

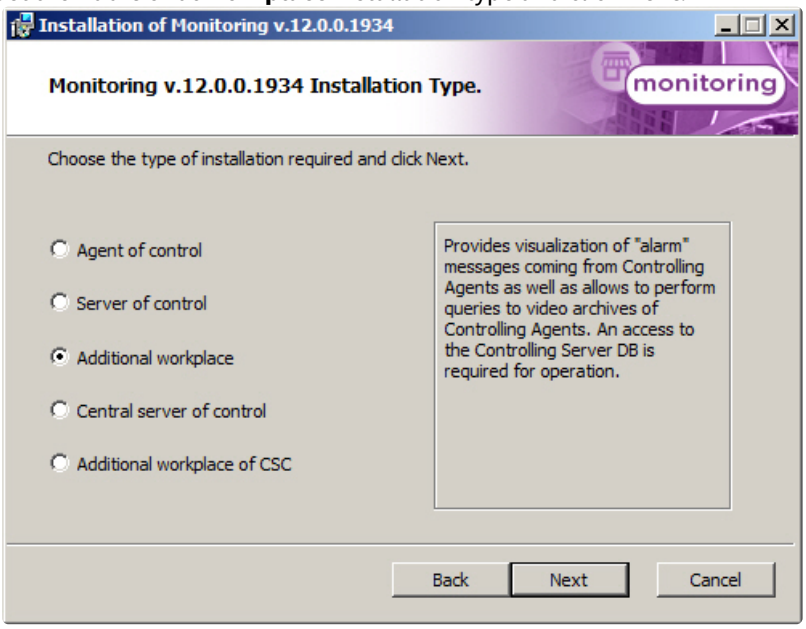
1. In the root directory of the distribution package, run the setup.exe executable file.
2. To continue the installation process, click **Next**.



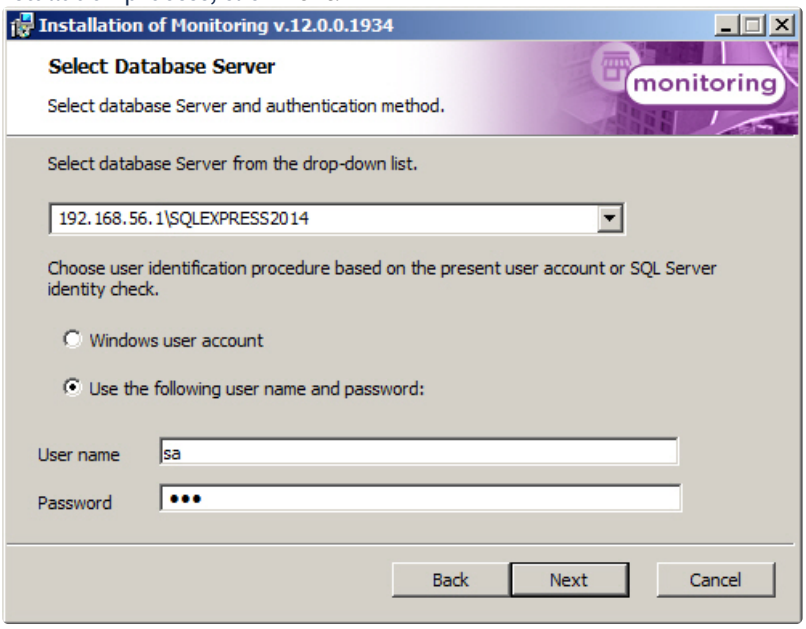
3. Read the terms of the license agreement carefully. Then set the radio button to **I accept the terms of the License agreement** and click **Next**.



4. Set the **Additional workplace** installation type and click **Next**.

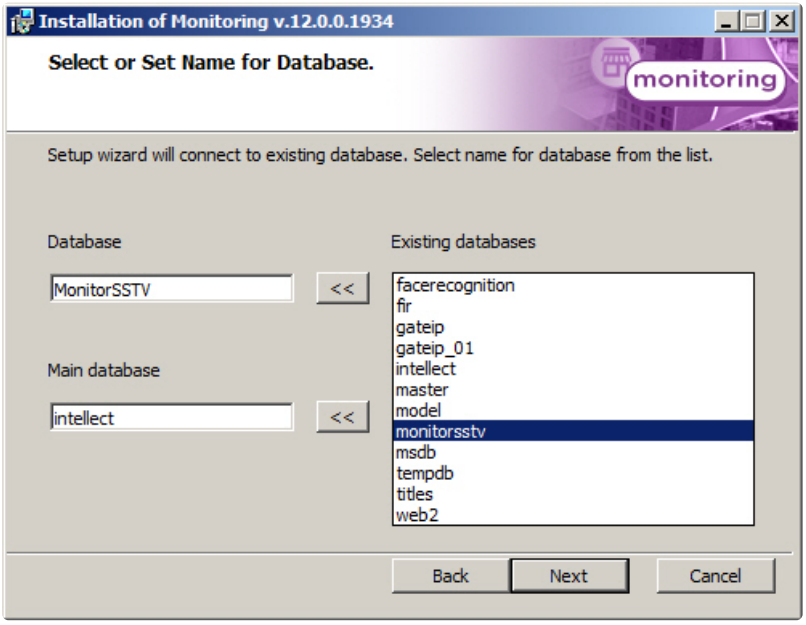


5. Select the database MS SQL Server and specify the authorization parameters for connection. For details, see Installation of INTELLECT™ software as a Server/Remote administrator workplace. To continue the installation process, click **Next**.

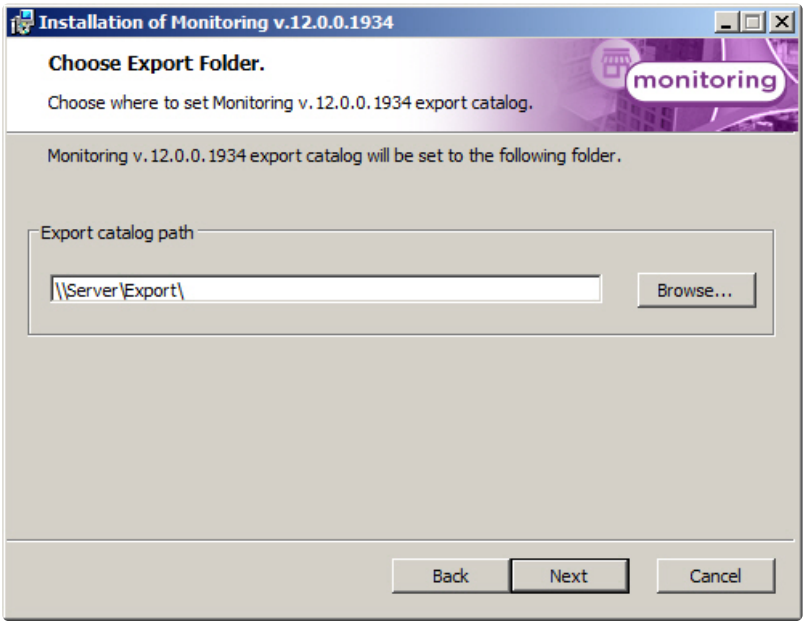


6. In the **Database** field specify the name of the database or select it on the right part of the window in the list of databases, which are created in the server, and click **<<**. Then click **Next**.

> **Note**
>
> By default, the name of the database is "MonitorSSTV" and its files will be stored in the SQL Server folder.

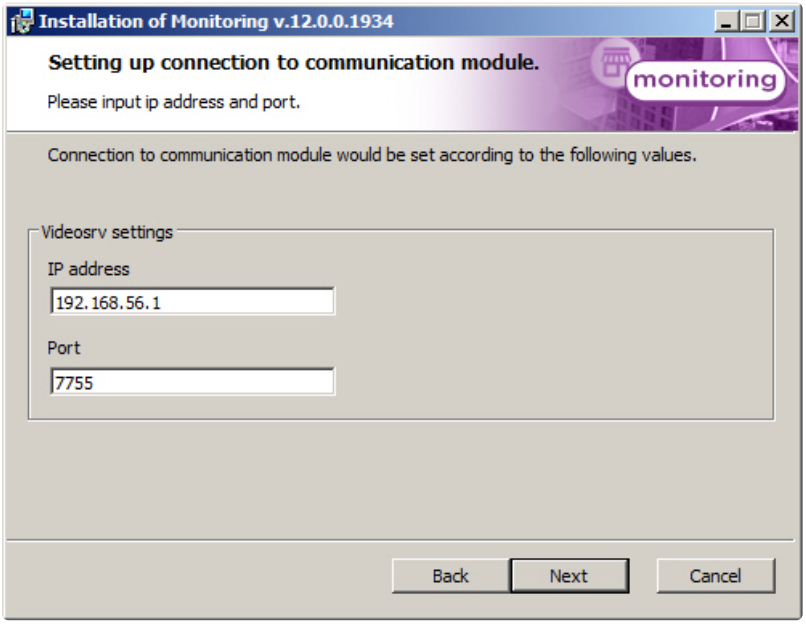


7. Specify the export catalog path. This catalog will contain video data received from *Agent of Control*. Click **Next**.

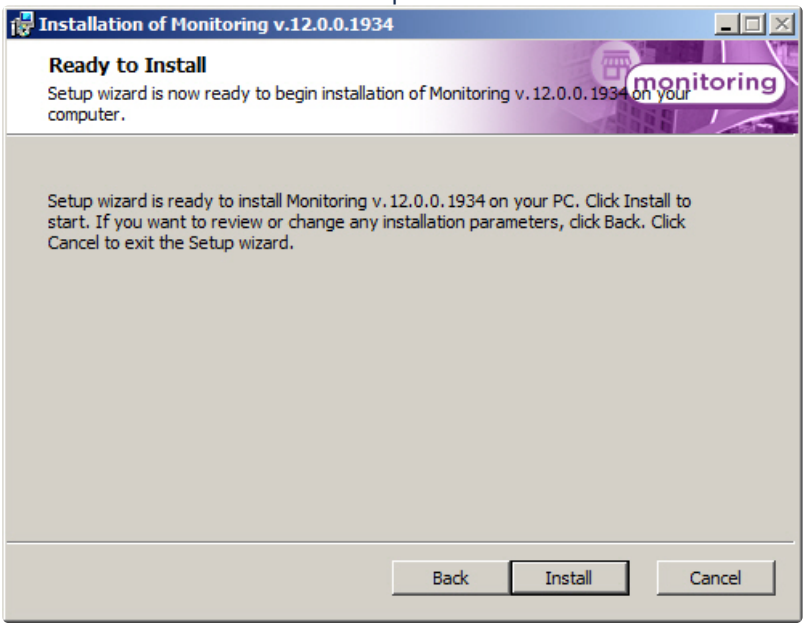


8. Specify IP-address and port for connection to *Server of Control* communication module videosrv. Click **Next**.

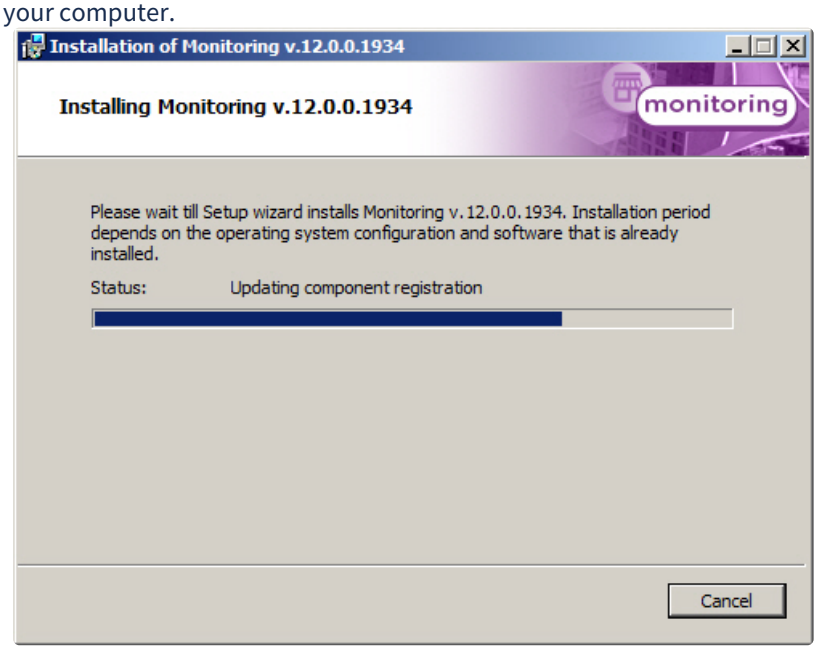
> **Note.**
>
> It is strongly recommended to change default **Export catalog path** and **IP address** on steps 6-7. Otherwise, after the installation is completed, it will be necessary to configure Additional workplace (see Configuring Additional workplace and Additional workplace of CSC).



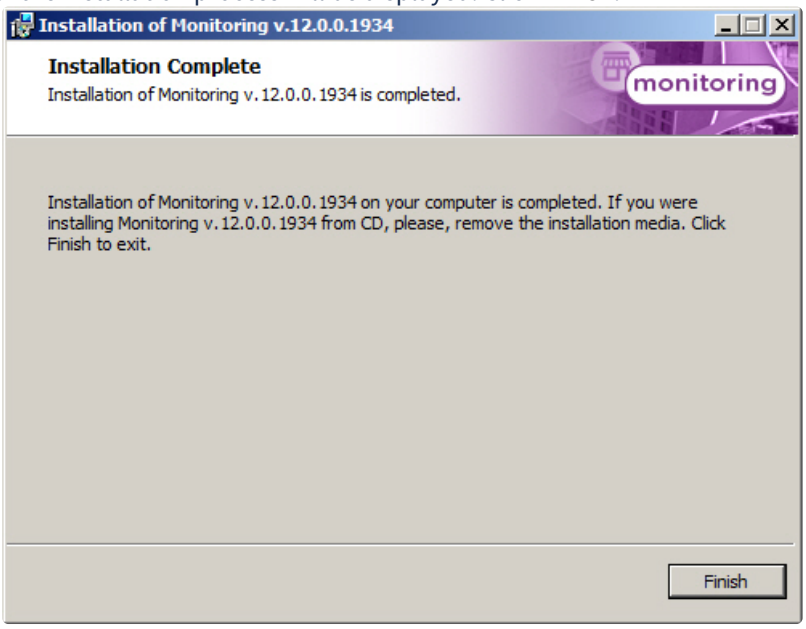
9. Click **Install** to start the installation process.



10. As a result, the necessary components of the *Monitoring* software package will be copied to hard drive of your computer.



11. After all software components are successfully copied on your hard drive, the message about the completion of the installation process will be displayed. Click **Finish**.



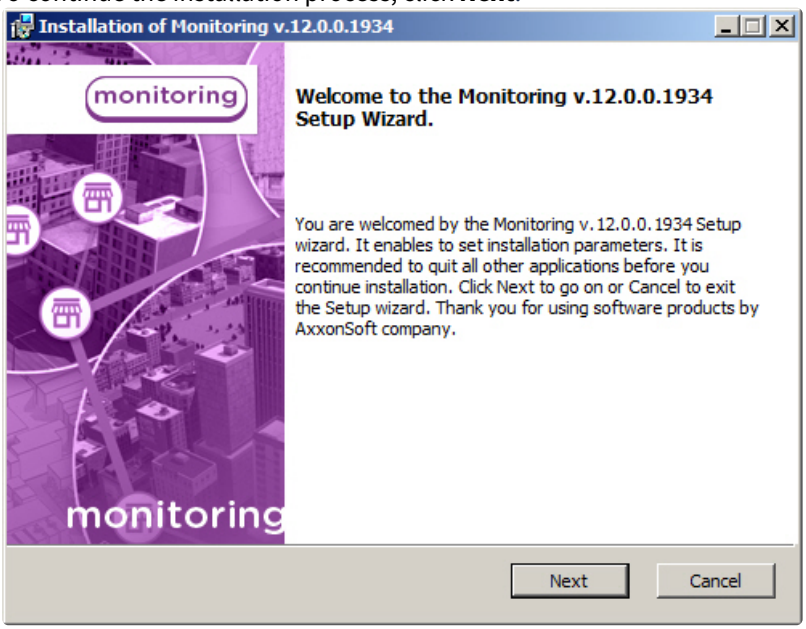
Installation of *Additional workplace* software is complete.

4.6 Central Server of Control installation

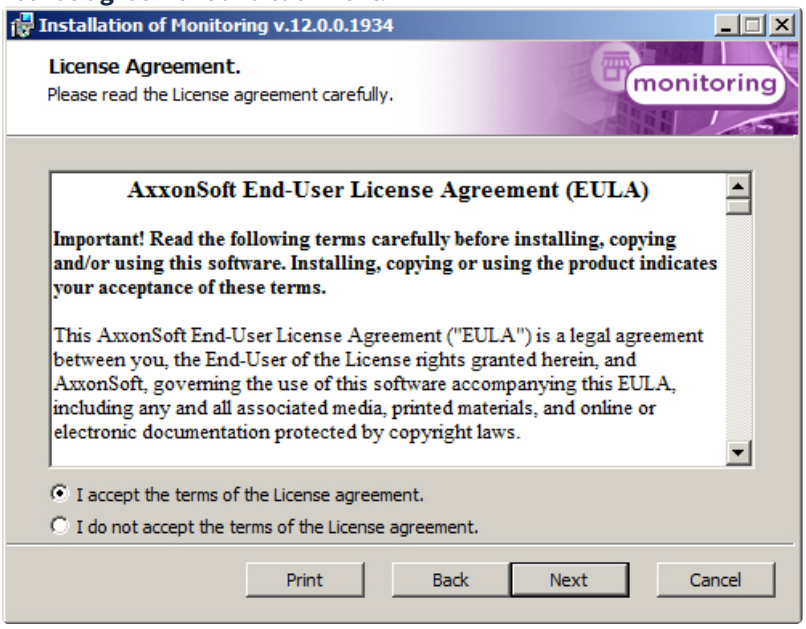
The *Monitoring* software is installed as a part of the *Intellect* software. Information about compatibility of the *Intellect* software versions and *Monitoring* is presented in the Obsolete. General information about product releases and versions compatibility section.

To install *Monitoring* software in the *Central Server of Control* configuration, do the following:

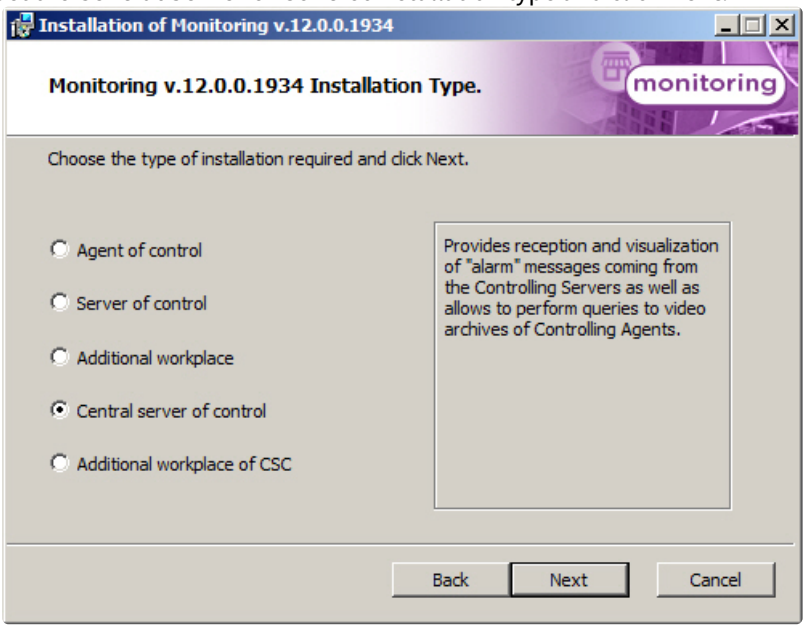
1. In the root directory of the distribution package, run the setup.exe executable file.
2. To continue the installation process, click **Next**.



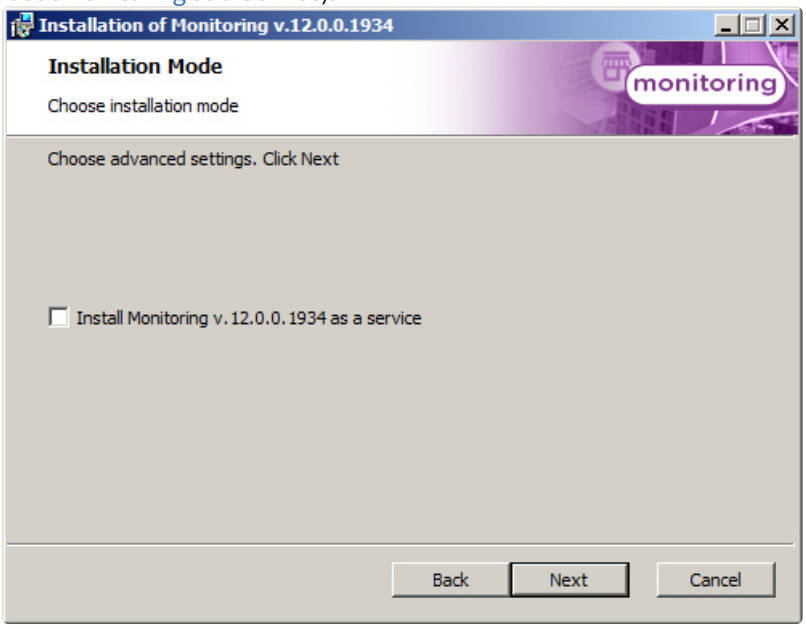
3. Read the terms of the license agreement carefully. Then set the radio button to **I accept the terms of the License agreement** and click **Next**.



4. Set the **Central Server of Control** installation type and click **Next**.

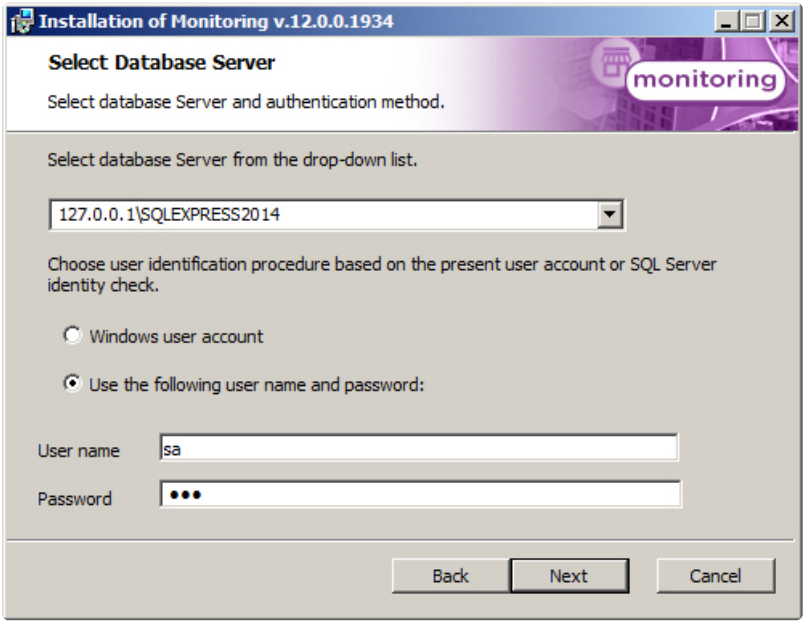


5. If *Intellect* software is installed as a service, and it is necessary that *Monitoring* is also installed as a service, then set the **Install Monitoring as a service** checkbox and click **Next** (for details, see General information about Monitoring as a Service).



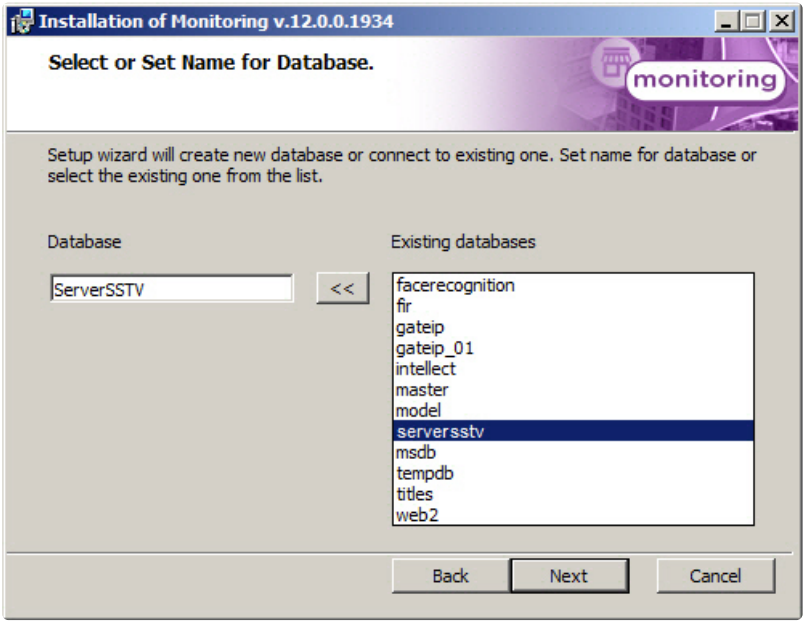
6. Select the database MS SQL Server and specify the authorization parameters for connection. For details, see Installation of INTELLECT™ software as a Server/Remote administrator workplace. To continue the installation process, click **Next**.

> **Note**
>
> In the **Select database Server from the drop-down list** field specify the **127.0.0.1** value instead of computer name or "(local)" value. Otherwise *Central Server of Control* will lose connection with its local database when the network cable is disconnected.

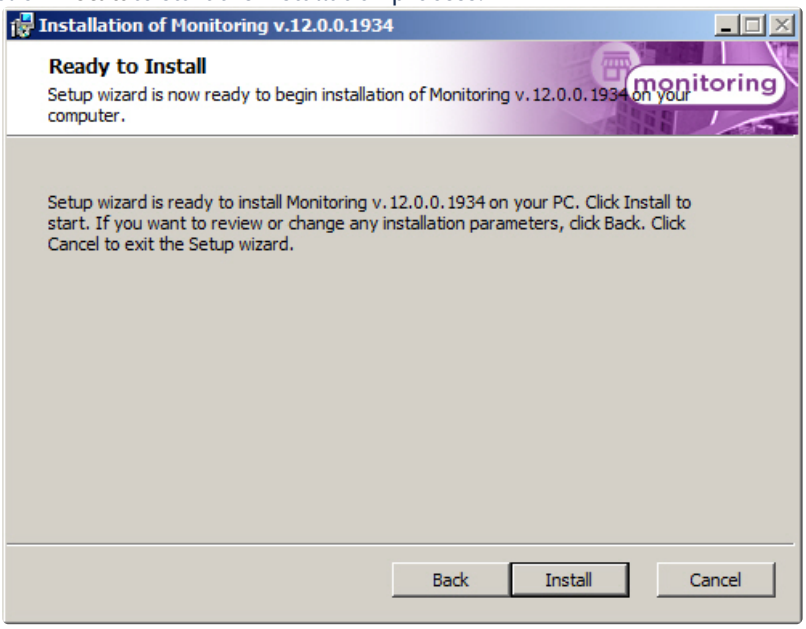


7. In the **Database** field specify the name of the database or select it on the right part of the window in the list of databases, which are created in the server, and click **<<**. Then click **Next**.

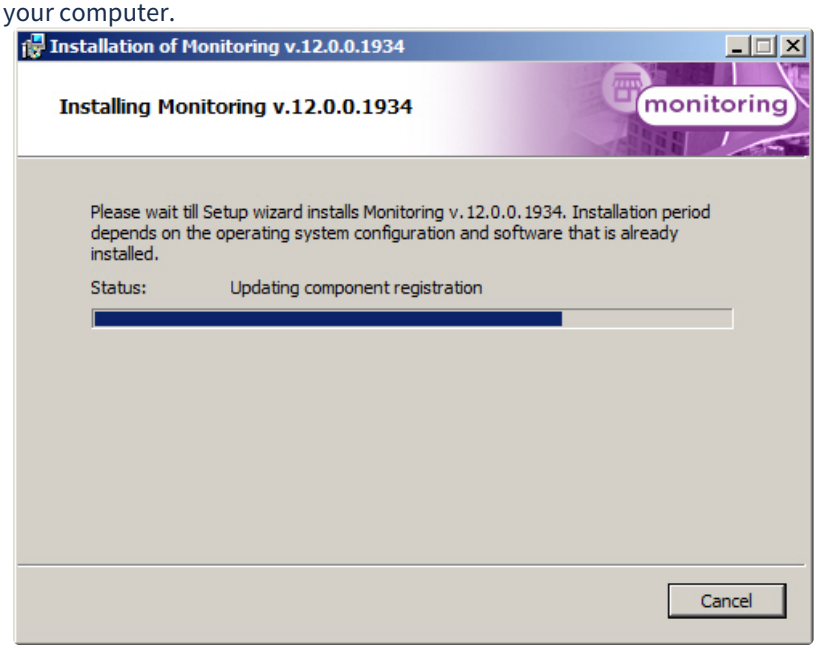
> **Note**
>
> By default, the name of the database is "ServerSSTV" and its files will be stored in the SQL Server folder.



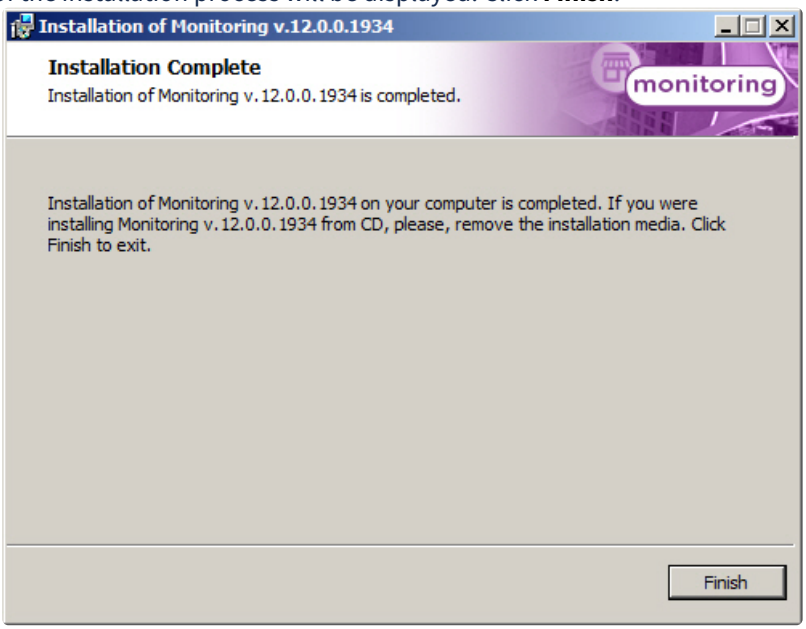
8. Click **Install** to start the installation process.



9. As a result, the necessary components of the *Monitoring* software package will be copied to hard drive of your computer.



10. After all software components are successfully copied on your hard drive, the message about the completion of the installation process will be displayed. Click **Finish**.



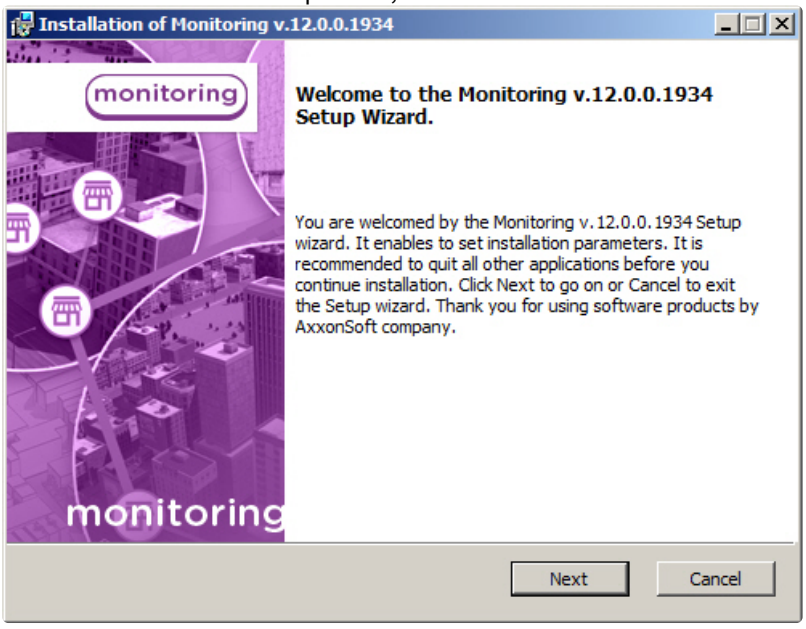
Installation of *Central Server of Control* software is complete.

4.7 Additional workplace of CSC installation

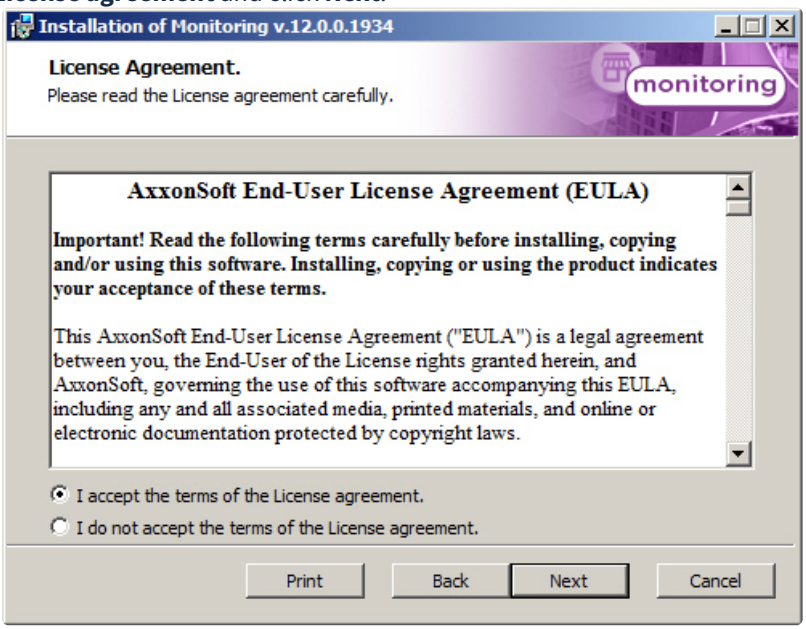
The *Monitoring* software is installed as a part of the *Intellect* software. Information about compatibility of the *Intellect* software versions and *Monitoring* is presented in the Obsolete. General information about product releases and versions compatibility section.

To install *Monitoring* software in the *Additional workplace of CSC* configuration, do the following:

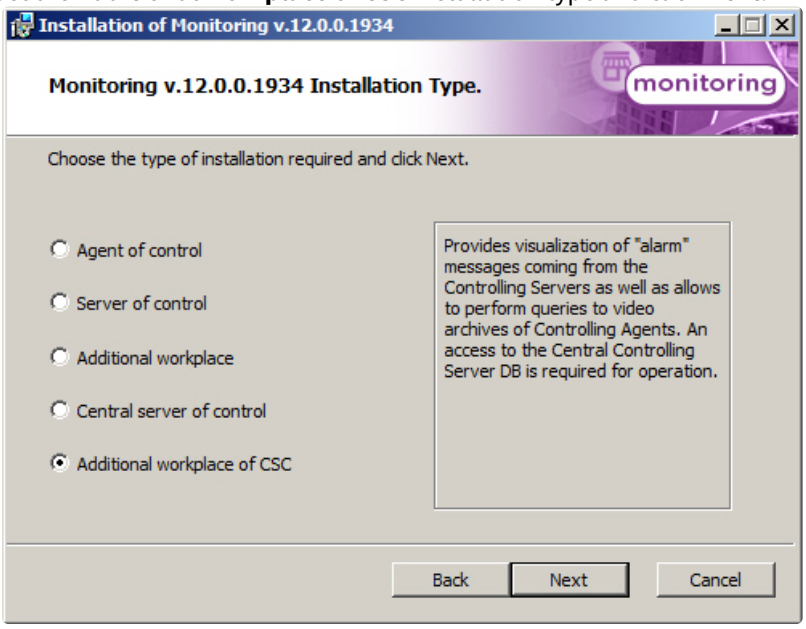
1. In the root directory of the distribution package, run the setup.exe executable file.
2. To continue the installation process, click **Next**.



3. Read the terms of the license agreement carefully. Then set the radio button to **I accept the terms of the License agreement** and click **Next**.

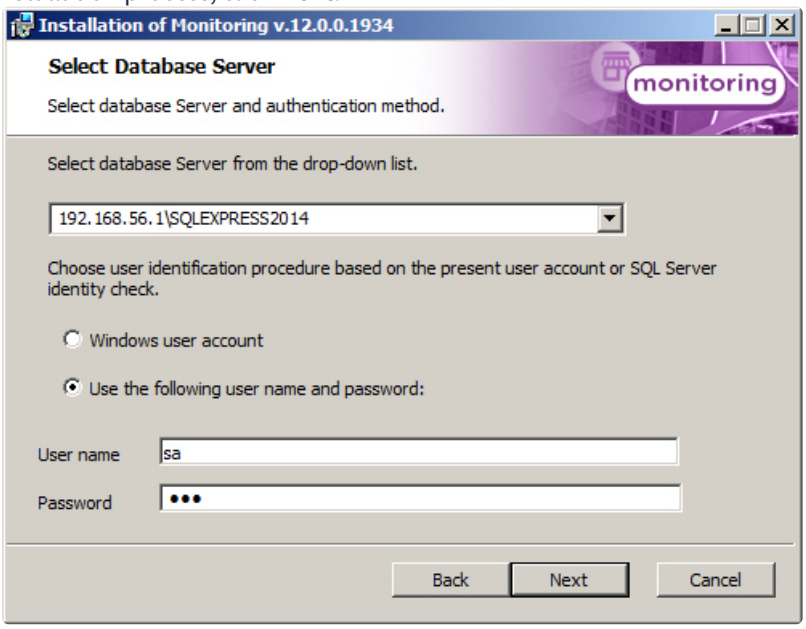


4. Set the **Additional workplace of CSC** installation type and click **Next**.



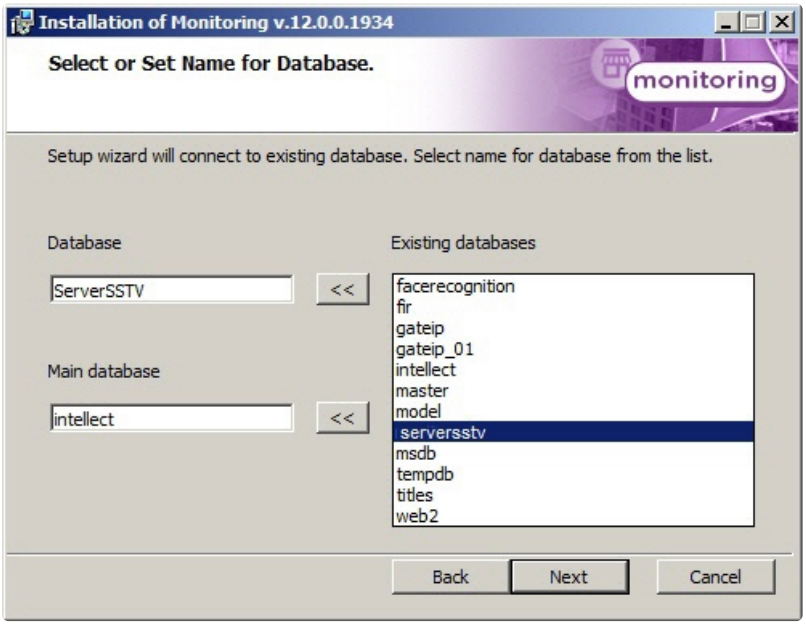
5. Select the database MS SQL Server and specify the authorization parameters for connection. For details, see Installation of INTELLECT™ software as a Server/Remote administrator workplace. To continue the

installation process, click **Next**.

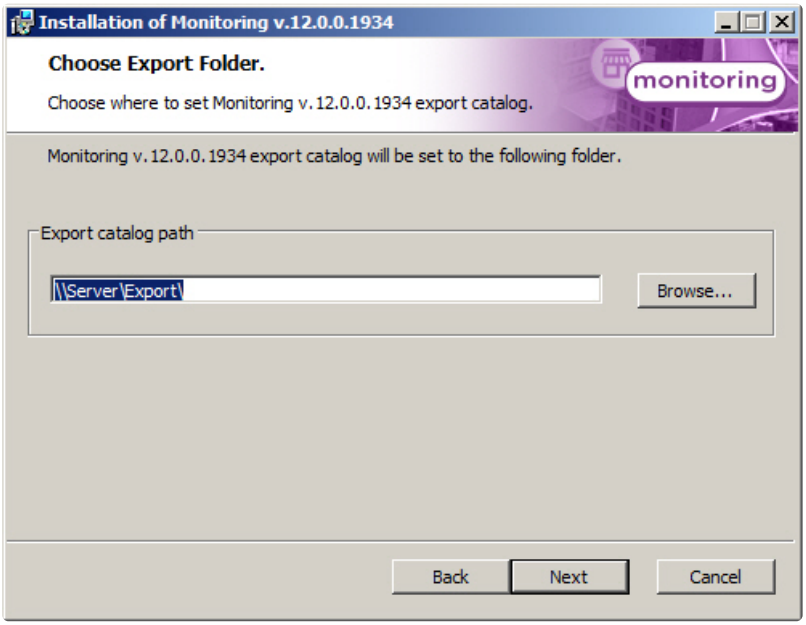


6. In the **Database** field specify the name of the database or select it on the right part of the window in the list of databases, which are created in the server, and click **<<**. Then click **Next**.

> **Note**
>
> By default, the name of the database is "MonitorSSTV" and its files will be stored in the SQL Server folder.

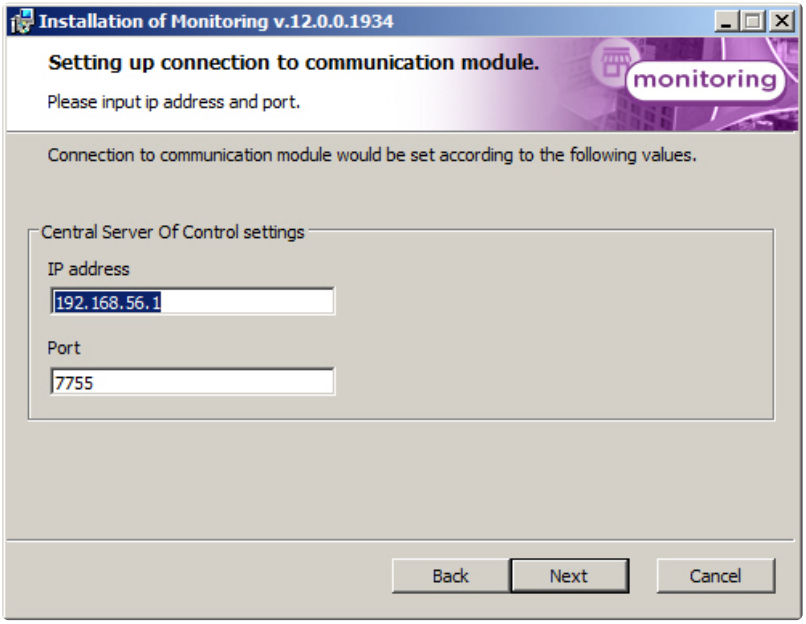


7. Specify the export catalog path. This catalog will contain video data received from *Agent of Control*. Click **Next**.

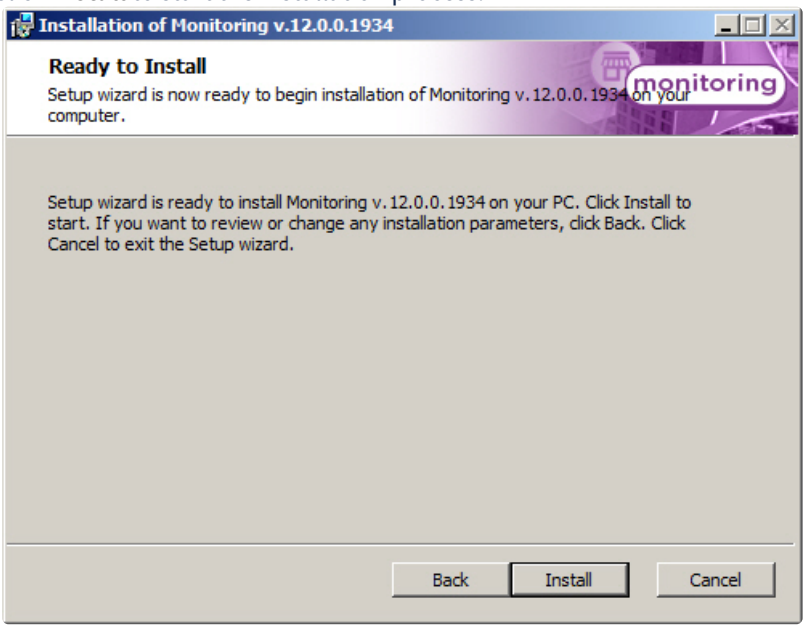


8. Specify IP-address and port for connection to *Central Server of Control* communication module CentralNetServer. Click **Next**.

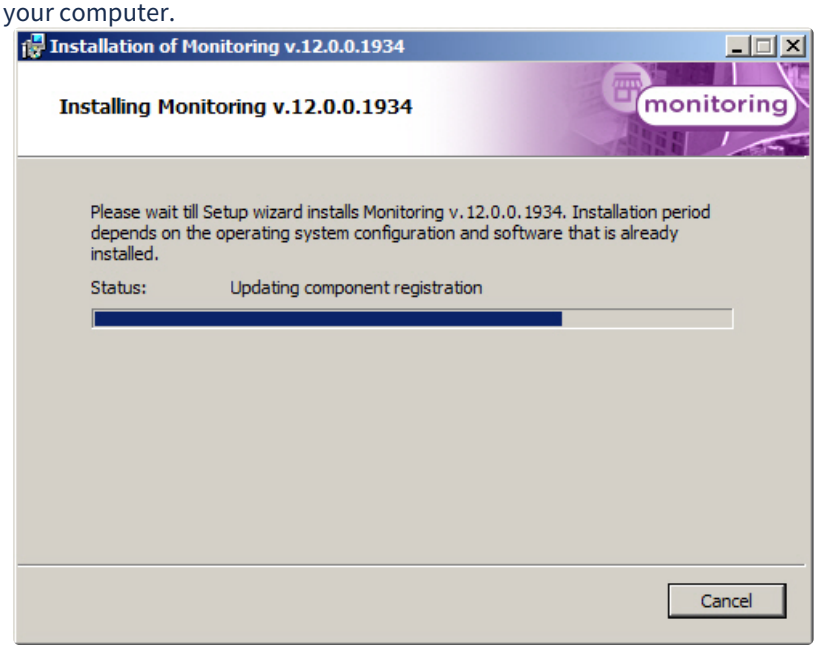
> **Note.**
>
> It is strongly recommended to change default **Export catalog path** and **IP address** on steps 6-7. Otherwise, after the installation is completed, it will be necessary to configure *Additional workplace of CSC* (see Configuring Additional workplace and Additional workplace of CSC).



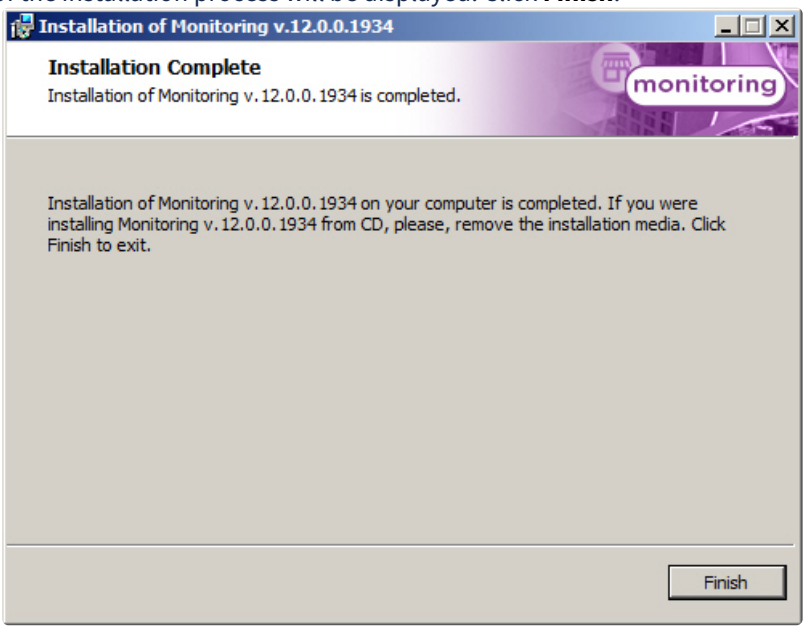
9. Click **Install** to start the installation process.



10. As a result, the necessary components of the *Monitoring* software package will be copied to hard drive of your computer.



11. After all software components are successfully copied on your hard drive, the message about the completion of the installation process will be displayed. Click **Finish**.



Installation of *Additional workplace of CSC* software is complete.

5 Configuring Agent of Control

To configure Agent of Control, go to the **System settings** window. Use of this window is described in Intellect Software Package: Administrator's Guide.

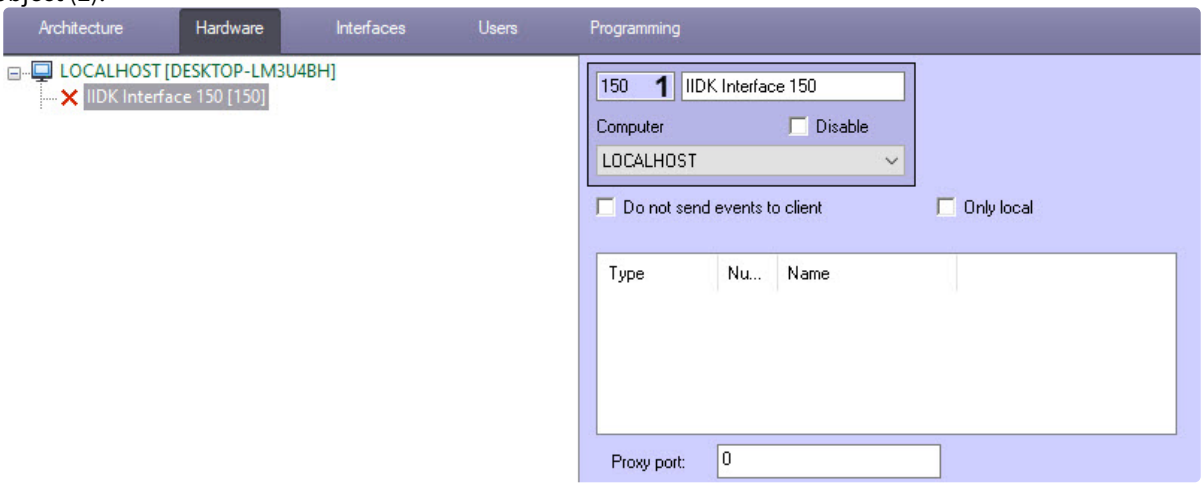
5.1 Creating necessary Agent Of Control objects

> **Attention!**
>
> Every time *Agent Of Control* is started, it checks for a **Backup** folder at the root of the disk on which *Intellect* is installed. If this folder is missing, *Agent Of Control* creates it. It is forbidden to delete this folder.

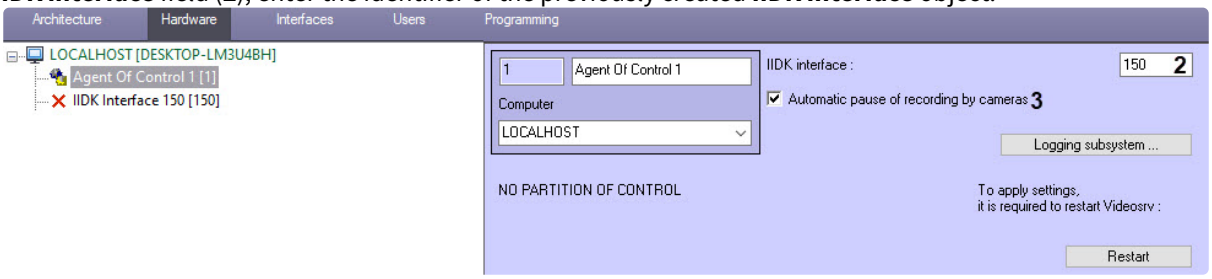
> **Note**
>
> *Agent Of Control*, like *Server Of Control*, can operate in a distributed configuration, at the same time *Agents Of Control*, *Servers Of Control* and *Central Servers Of Control* can see where each of them is installed and can be configured.

To create necessary *Agent Of Control* objects, do the following:

1. In the **System settings** dialog window, go to the **Hardware** tab.
2. Create an **IIDK Interface** object based on the **Computer** object. Set the identifier of the **IIDK Interface** object (**1**).



3. Create an **Agent Of Control** object based on the **Computer** object. On the settings panel of this object, in the **IIDK interface** field (**2**), enter the identifier of the previously created **IIDK Interface** object.



4. The **Automatic pause of recording by cameras** checkbox (**3**) is set by default, so that the scripts from the code are executed automatically. The **SleepAfterDisarm** and **SleepAfterRecStop** registry keys are used for fine-tuning these scripts (for the description of the registry keys, see Registry keys reference guide). When the checkbox is clear, you can use the scripts described here to pause recording by cameras.

5. Create one or more **Partition Of Control** child objects based on the **Agent Of Control** object.

> **Note**
>
> The **Partition Of Control** object name cannot contain the following characters: underscore "_", backslash "\", angle brackets "**>**" and "**<**", single quote "'".

It is also necessary to create **Video Capture Device**, **Camera**, and **Sensor** objects in the hardware tree that correspond to the connected hardware. Creation and configuration of these objects is described in INTELLECT Software Package. Installing and configuring security system components.

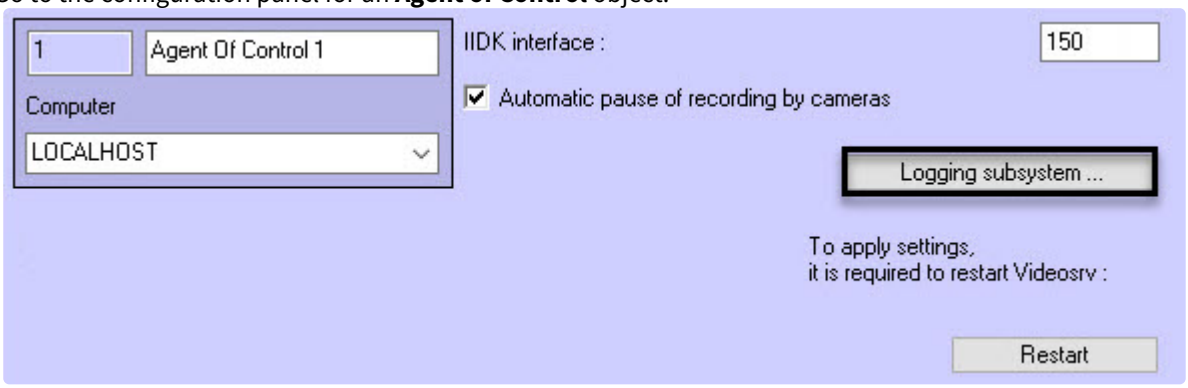
Creation of the necessary objects in the hardware tree is now complete.

5.2 Configuring the logging subsystem

The logging subsystem allows configuring the detail level at which the activity of *Agent of Control* is recorded.

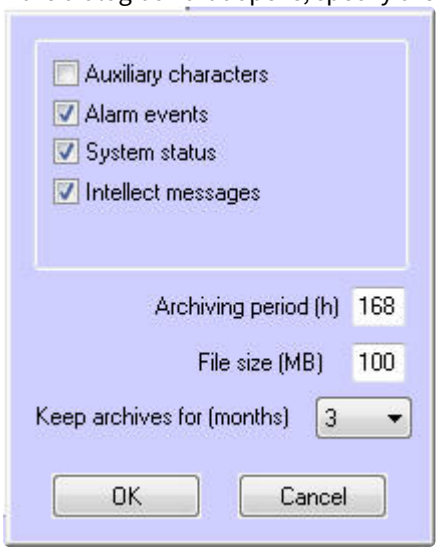
To configure the logging subsystem:

1. Go to the configuration panel for an **Agent of Control** object.



2. Click the **Logging subsystem...** button.

3. In the dialog box that opens, specify the following parameters:



   a. **Auxiliary characters**: To log transport-level auxiliary characters, select this check box.
   b. **Alarm events**: To log alarms (activation of vibration sensor, temperature sensor, or forcible entry sensor), select this check box.
   c. **System status**: To log events related to the system state, select this check box.
   d. **Intellect messages**: To log messages from Intellect, select this check box. Information is saved in the folder to which the software was installed, in the file video.log.
   e. **Archiving period (h)**: Allows archiving the log file at the specified interval (in hours). Archives are saved in the DATA subfolder, with the following name format: namelog_yymmddhhmmss.gz, where
      i. namelog is the name of the log file being archived;
      ii. yy is the year of archive creation;
      iii. mm is the month of archive creation;
      iv. dd is the day of archive creation;
      v. hh is the hour of archive creation;
      vi. mm is the minute of archive creation;
      vii. ss is the second of archive creation.
   f. **File size (MB)**: Sets the threshold size (in megabytes) for the log file after which the file is archived. This setting overrides the value in the **Archive period (h)** field.
   g. **Keep archives for (months)**: Sets the length of time for which to store the log file archive, in months (between 1 and 24). Archives that are older than the specified number of months are deleted.

The main log file is located in the installation folder, in the file vsrvYYMMDD.log, where YY is the year, MM the month, and DD the day.

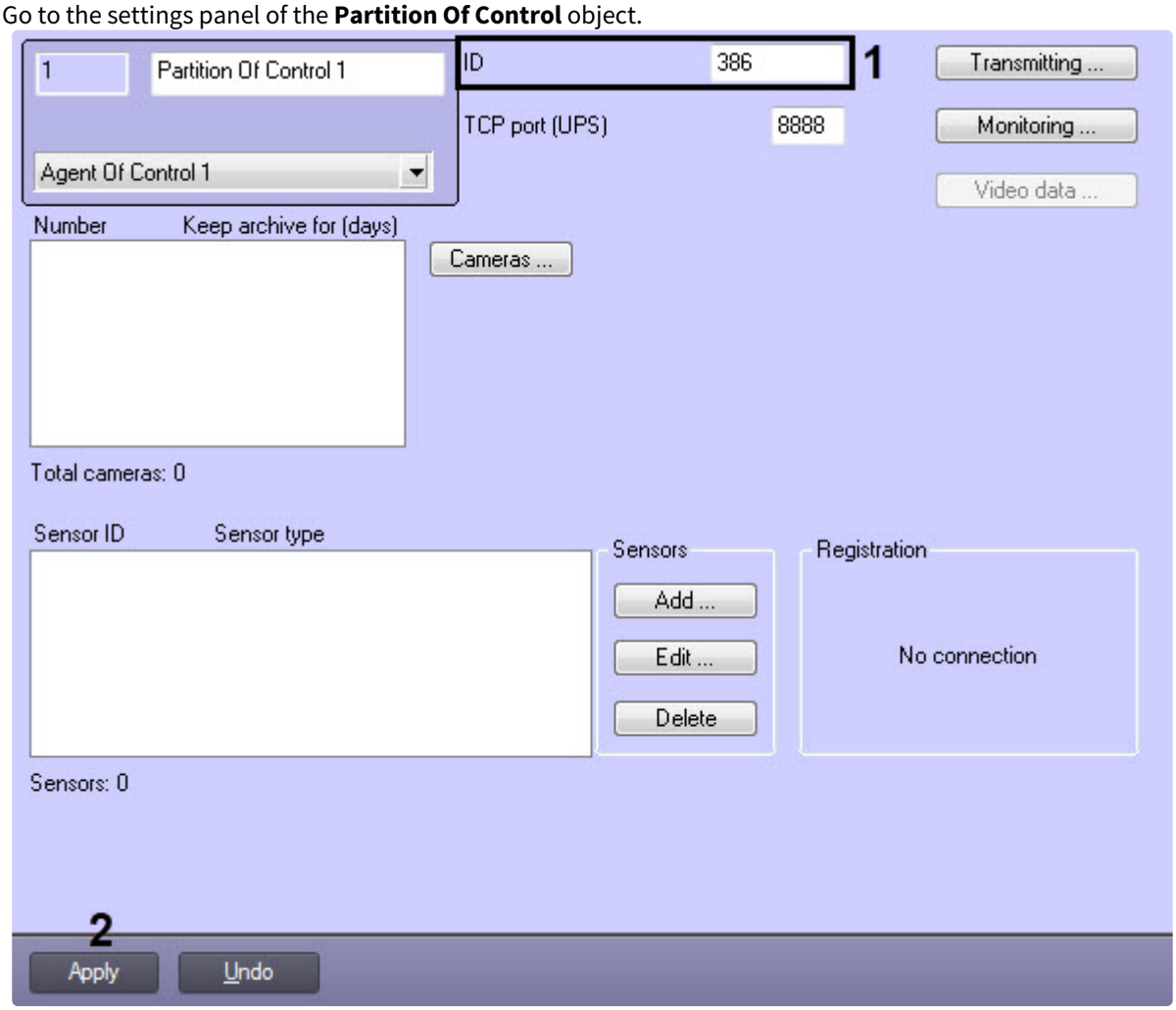
Configuration of the logging subsystem is now complete.

5.3 Configuring the Partition Of Control object

5.3.1 Configuring the Partition Of Control unique ID

To configure the unique ID number for a **Partition Of Control** object:

1. Go to the settings panel of the **Partition Of Control** object.



2. In the **ID** field (**1**), enter a unique number for the object on which *Agent Of Control* is being installed. The number can be from 1 to 9 characters long.

> **Note**
>
> The ID cannot contain the following characters: space " ", underscore "_", backslash "\" and single quote "'".

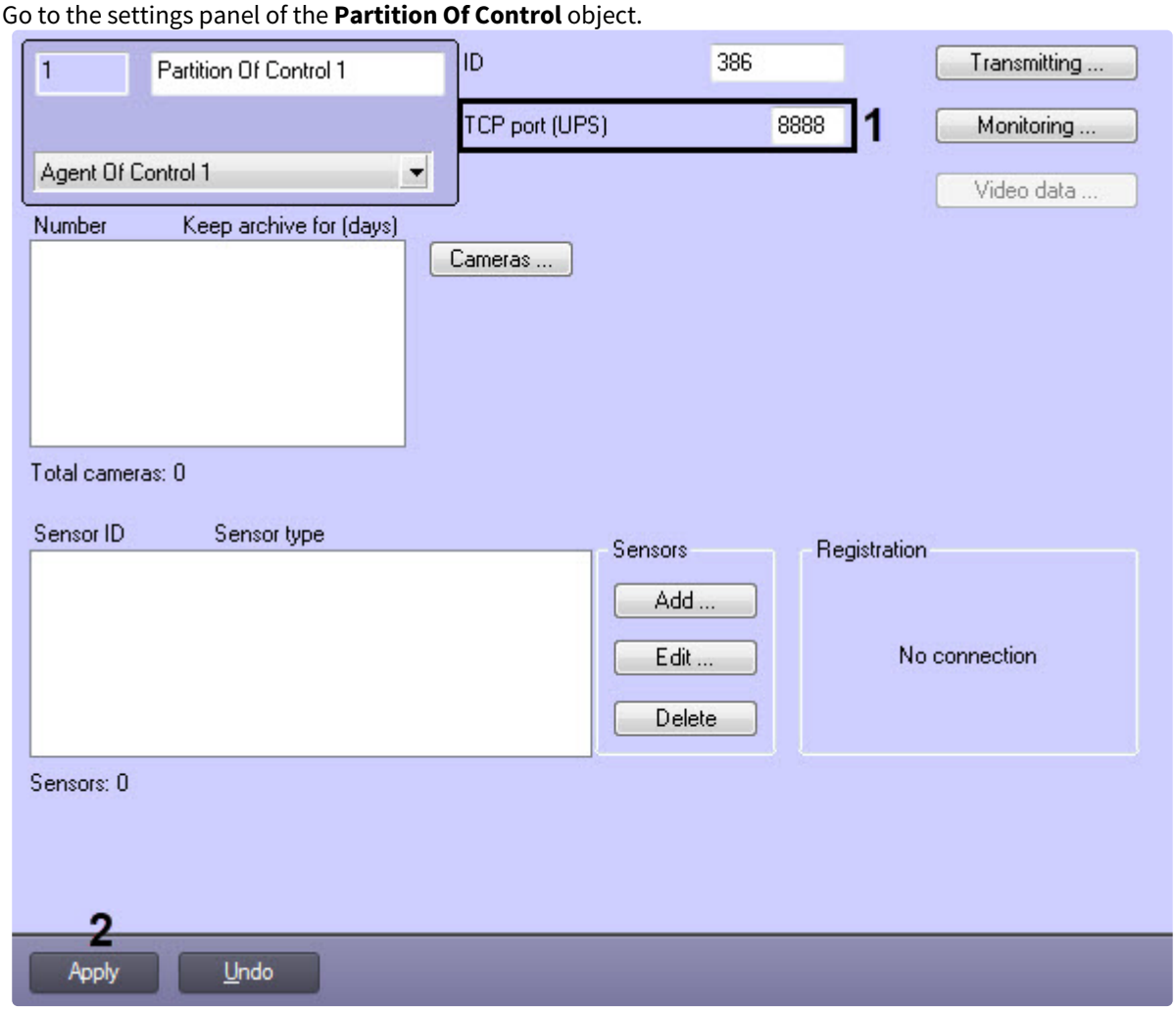
3. To save settings, click the **Apply** button (**2**).

Configuration of a unique **Partition Of Control** ID number is now complete.

5.3.2 Configuring a port for incoming UPS messages

To configure a port for accepting messages from an uninterrupted power supply unit, do the following:

1. Go to the settings panel of the **Partition Of Control** object.



2. In the **TCP port (UPS)** field (**1**), enter the number of the port on which to "listen" for UPS messages.
3. To save the settings, click the **Apply** button (**2**).

Configuration of a port for accepting messages from a UPS is now complete.

5.3.3 Configuring communication between Agent Of Control and Server Of Control

Note

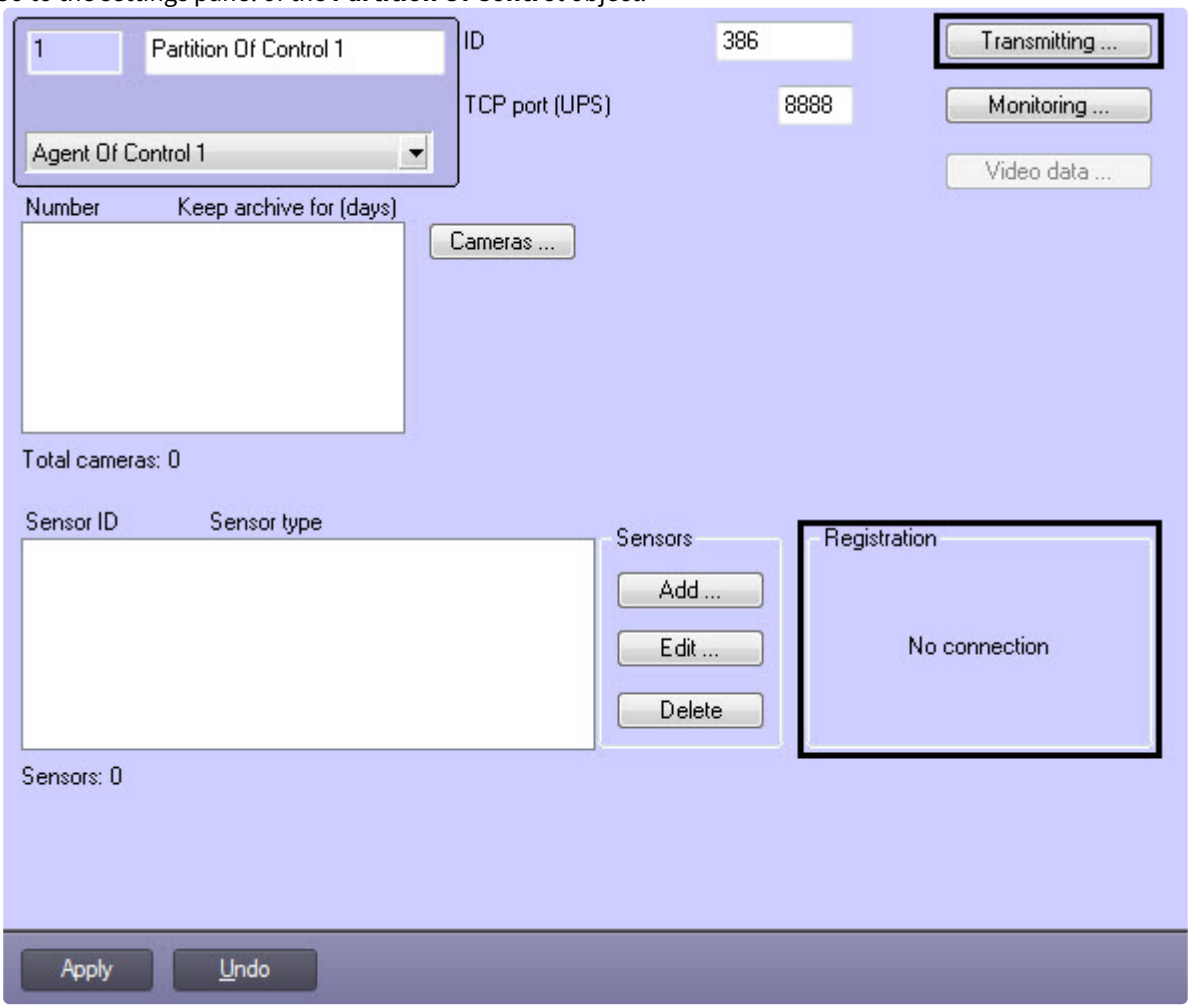
Before you configure the interaction between the *Agent Of Control* and the *Server Of Control*, it is recommended to make sure that the name and identifier of the **Partition Of Control** object being configured are specified correctly, since upon the successful connection to the *Server Of Control*, if an object with this identifier is absent, the **Partition Of Control** object with the name and identifier of the object being configured will be automatically created on it. If the interaction between the *Agent Of Control* and the *Server Of Control* is configured successfully, the **Registration completed** message will be displayed in the **Registration** area. This means that the *Agent Of Control* can transmit alarms and data on the technical state of this *Partition Of Control* to the *Server Of Control*.
If the **Partition Of Control** object could not be created on the *Server Of Control*, the reason will be indicated in the **Registration** area, for example:

- **The base software is not loaded**;

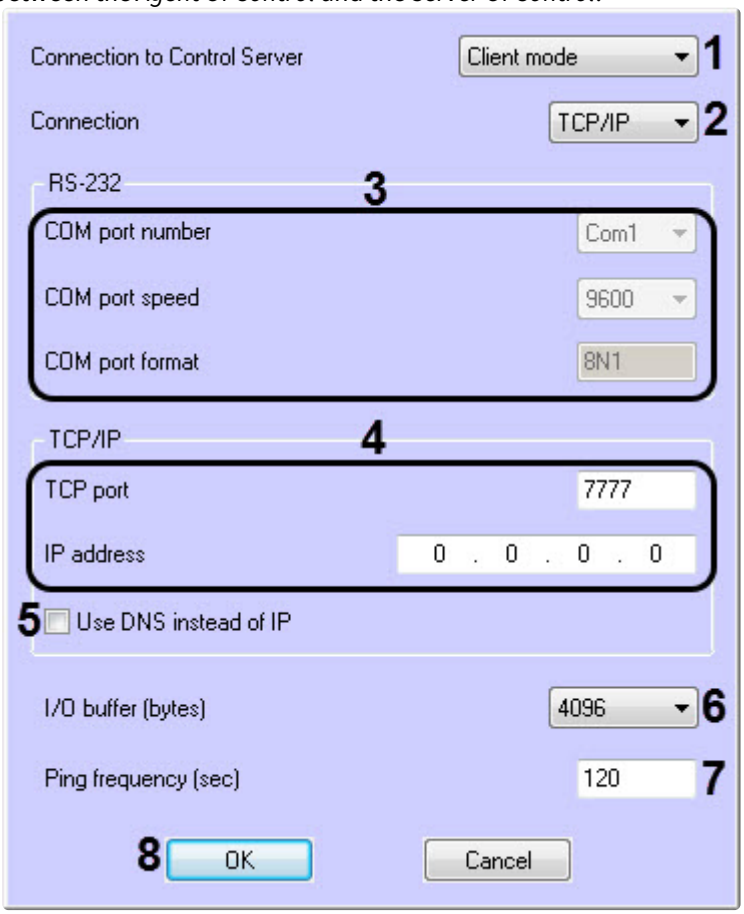
- **Change the object name** (an object with the same name already exists on the *Server Of Control*);
- An object on the *Server Of Control* will also not be created if the user does not have rights to administer the *Server Of Control* object (see Rights administration).

To configure the communication between the *Agent Of Control* and the *Server Of Control,* do the following:

1. Go to the settings panel of the **Partition Of Control** object.



2. Click the **Transmitting** button. A dialog box opens with settings for configuring the communication method between the *Agent Of Control* and the *Server Of Control*.

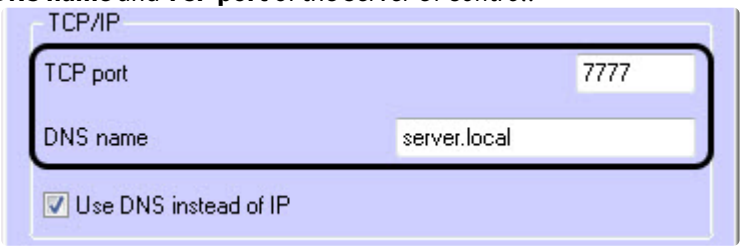


3. In the **Connection to Control Server** drop-down list, select the **Client mode** as the methods for connecting the *Agent Of Control* to the *Server Of Control* (**1**).

> **Note**
>
> The **Server mode** is not used.

4. From the **Connection** drop-down list, select the value for the transport level. Possible values are **TCP/IP** or **RS232** (**2**).
5. If the **RS232** connection type is selected, then specify the **COM port number, COM port speed**, and **COM port format** parameters (**3**).
6. If the **TCP/IP** connection type is selected, then indicate the parameters for connection to the *Server Of Control* in this dialog box:
    a. If an IP address is used for connection, make sure that the **Use DNS instead of IP** checkbox is not set (**5**) and indicate the **IP address** and **TCP port** of the *Server Of Control* (**4**).

b. If a domain name is used for connection, set the **Use DNS instead of IP** checkbox (**5**) and indicate the **DNS name** and **TCP port** of the *Server Of Control*.



> **Note**
>
> The use of domain name for connection allows you to avoid the *Agent Of Control* resetting in case of *Server Of Control* IP address change.

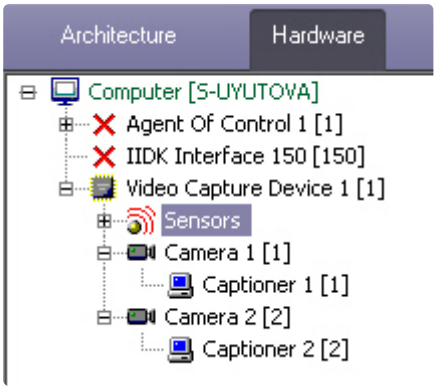
7. When still frames or video is sent to the *Server Of Control*, the data is transferred in packets. The packet size is specified by the **I/O buffer (bytes)** parameter (**6**). For maximum data transfer speed, it is recommended to use the value 4096. For poor connections, such as if a GSM modem is used, it is recommended to use the value 800.
8. If **Client mode** is selected, in the **Ping frequency (sec)** field (**7**), enter the time interval at which the *Agent Of Control* will send messages about its technical state to the *Server Of Control*. Minimum possible value is 10 sec. This value does not affect short-term alarms. Messages about short-term alarms are transmitted from the *Agent Of Control* to the *Server Of Control* immediately after corresponding sensors triggering. Some long-term alarms can also be an exception: for more information, see Appendix 1. Data update periods summary.
9. Click the **OK** button (**8**).
10. Click the **Apply** button to save the changes.

Configuration of communication between the *Agent Of Control* and the *Server Of Control* is now complete.

5.3.4 Configuring captions

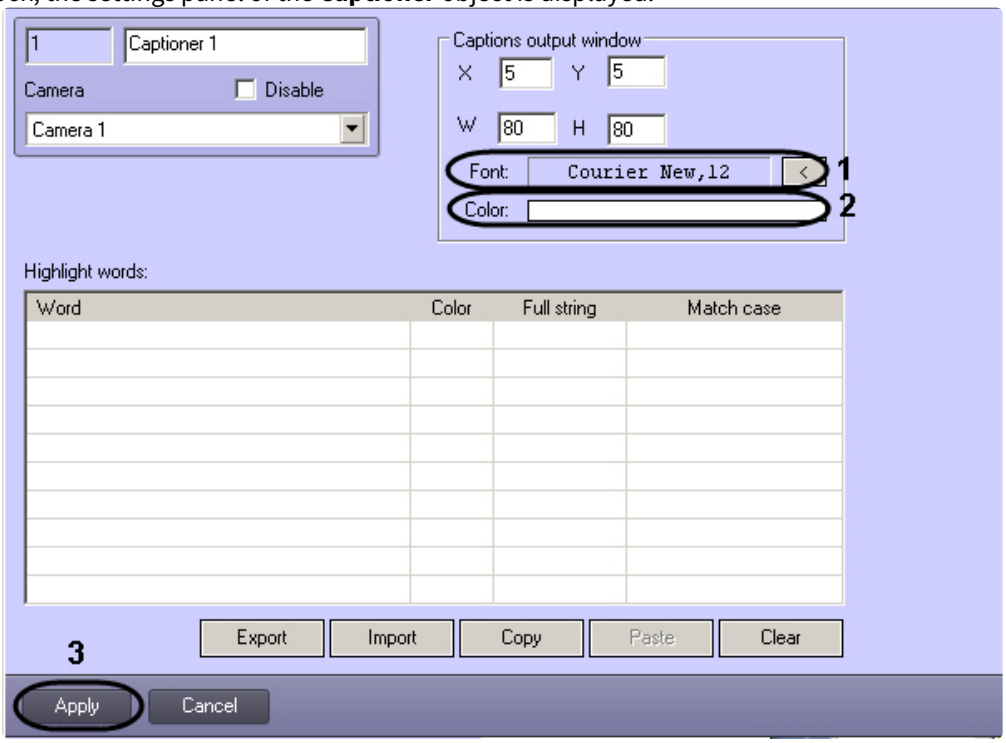
To use and configure captions, for each camera on which you want to use captions, you must create a **Captioner** object.

> **Attention!**
>
> If multiple captioners have been created for a single camera, the *Agent Of Control* uses the captioner with the lowest ID number.

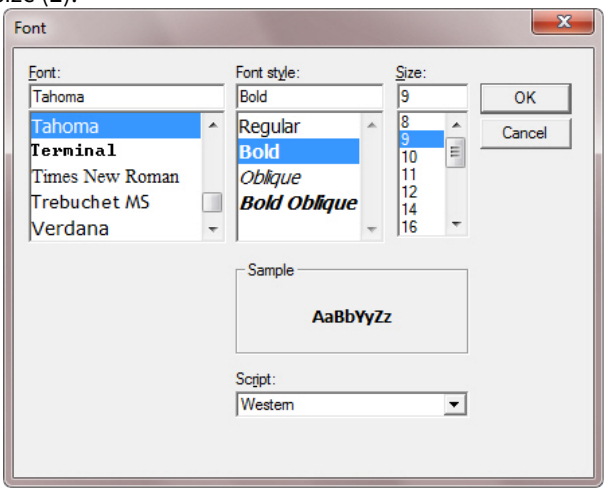


To configure the font and display area used for captions:

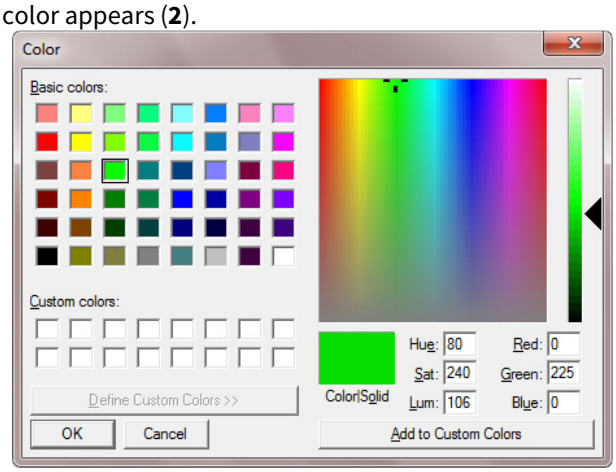
1. In the hardware tree, click the relevant **Captioner** object. On the right side of the **System settings** dialog box, the settings panel of the **Captioner** object is displayed.



2. If you click the button to the right of **Font**, a dialog box appears in which you can configure the font face and size (**1**).



3. To configure the color of captions, double-click the area to the right of **Color**. A dialog box for configuring color appears (**2**).



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

5.3.5 Configuring the camera list

The list of cameras specified in the configuration panel for the **Partition Of Control** object determines the cameras whose archive and video can be accessed through the *Monitoring* interface object (see Monitoring Software Package: Operator's Guide). In addition, this list determines the cameras whose state and archives are monitored by *Agent Of Control*.

Depending on whether the list of cameras has been specified or not, the following situations are possible:

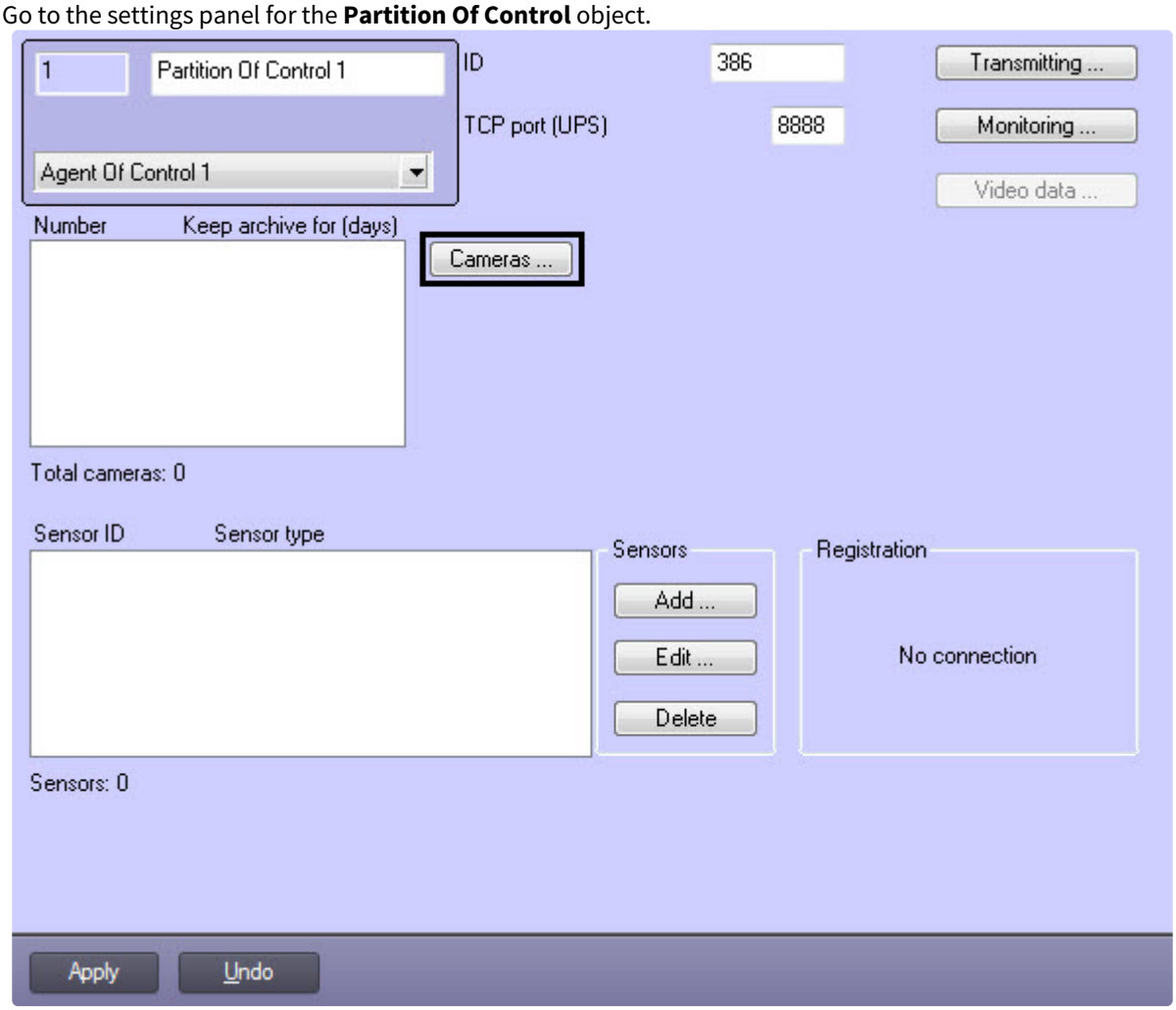
1. If cameras are specified in the list, *Agent Of Control* works in normal mode: it monitors the state of cameras and their archives. *Server Of Control* receives information about the number of cameras, disks, disk volume, etc.
2. If no cameras are specified in the list, *Agent Of Control* checks the presence of a **Backup archive** object in the system and gets information about disks from this object. In this case, *Server Of Control* will receive information only about the disks marked in the **Backup archive** object. Access to the archive is not performed from the **Search in Archive** interface object during this process.
3. If no cameras are specified in *Agent Of Control* settings and there is no **Backup archive** object in the configuration, information about disks is taken from the **Computer** object; the disks specified for storage of the main archive are taken into account. Access to the archive is not performed from the **Search in Archive** interface object during this process.

In the second and third cases, monitoring is performed of the state of the system (network functioning, restarts, etc.) and disks (their number and free space). The state of cameras and their archives is not available for monitoring.

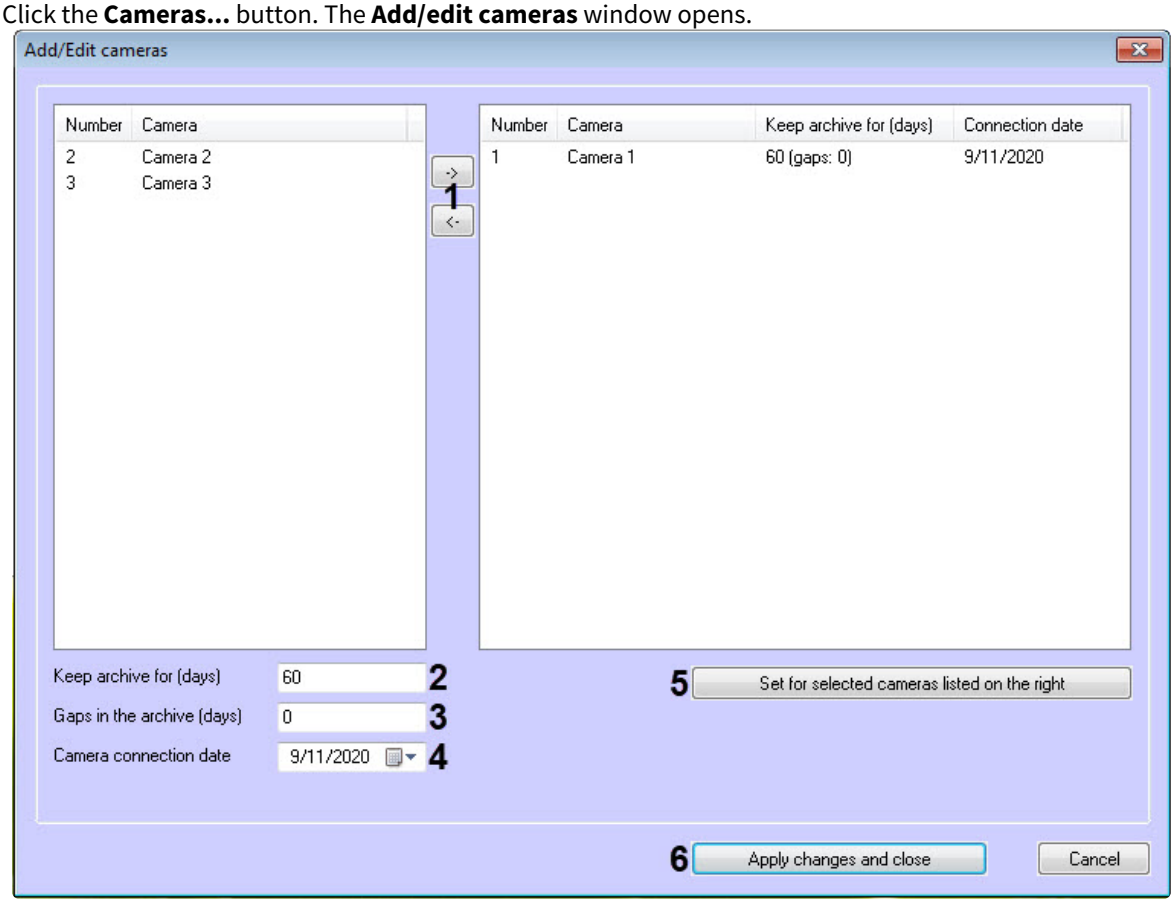
> **Note**
>
> Creation and configuration of the **Backup archive** object is described in Intellect Software Package: Administrator's Guide.

To configure the list of cameras in use, do the following:

1. Go to the settings panel for the **Partition Of Control** object.



2. Click the **Cameras...** button. The **Add/edit cameras** window opens.



3. Move the necessary cameras from the left list to the right list by clicking the -> and <- buttons (**1**).
4. Select cameras in the list on the right.
5. In the **Keep archive for (days)** field, specify the storage time of the video archive in days (**2**) in the range from 0 to 999. If the value of the parameter is 0, the size of the archive will not be monitored.
6. In the **Gaps in the archive (days)** field, specify the number of days on which the video archive is not recorded, because non-working days are taken into account in the working schedule (**3**).
7. In the **Camera connection date** field, specify the date the camera was connected to the system (**4**).
8. Click the **Set for selected cameras listed on the right** button (**5**).
9. Click the **Apply changes and close** button (**6**). The selected cameras will be added to the list on the settings panel of the **Partition Of Control** object.
10. Click the **Apply** button on the settings panel of the **Partition Of Control** object.

Note

The ID numbers of cameras and captioners must be whole numbers.

Note

Cameras will be automatically removed from the list in the following cases:

- The **Camera** object or its **Video Capture Device** parent object is removed from the *Intellect* hardware list;
- The **Camera** object or its **Video Capture Device** parent object is set to **Disabled** mode;

- In a distributed configuration, the **Camera** object is moved to a **Video Capture Device** object located on another computer;
- In a distributed configuration, the **Video Capture Device** object, to which the **Camera** object belongs, is moved to another computer.

Configuration of the camera list is now complete.

5.3.6 Configuring sensors

The system supports use of four fixed sensors (vibration sensor, lock sensor, temperature sensor, and additional sensor) as well as 12 expansion sensors.

Note.

Before configuring a list of sensors for a protected site, you must create and configure the necessary **Sensor** objects in *Intellect* first. Creation and configuration of these objects is described in the document Installing and configuring security system components guide.

Attention!

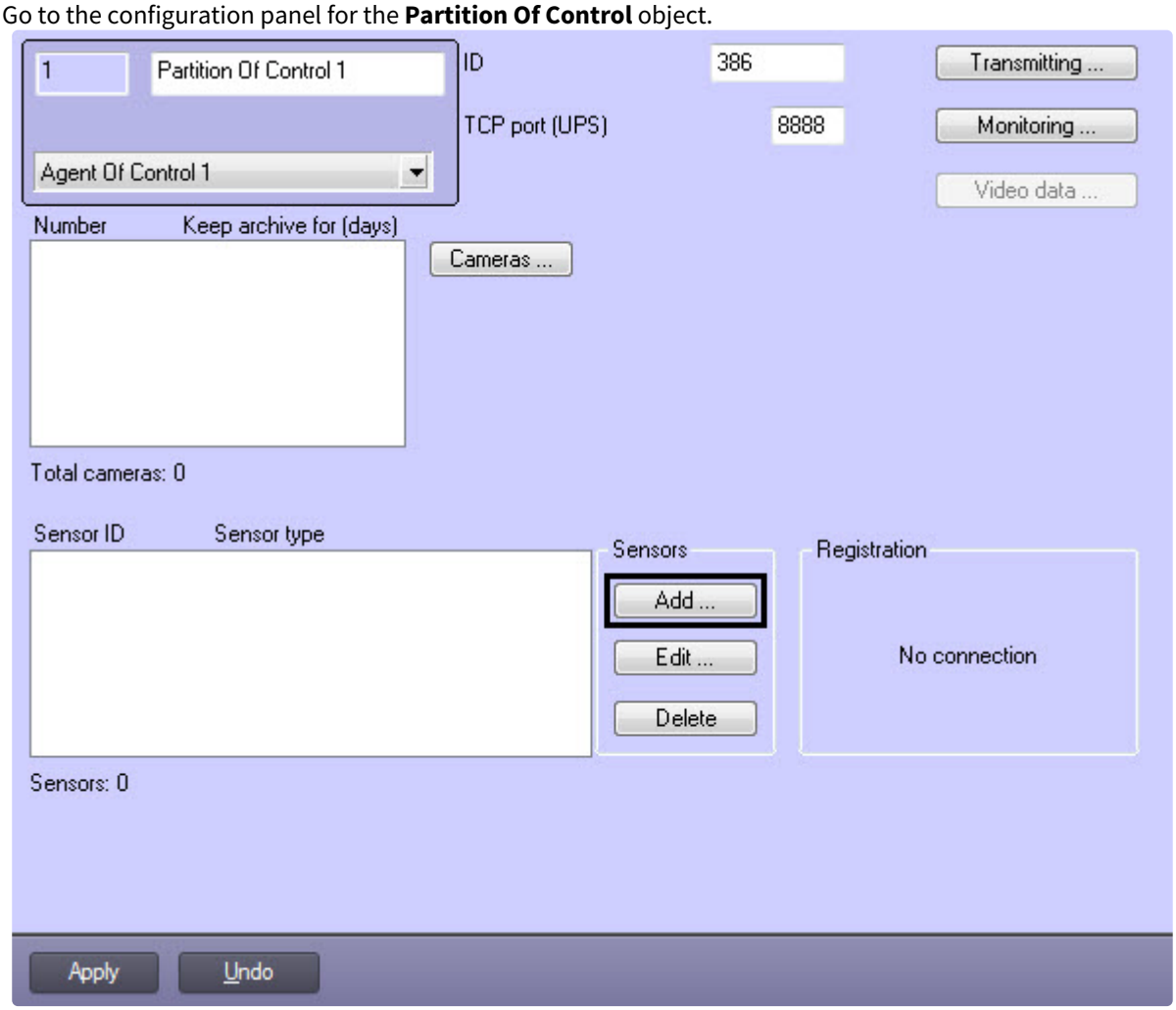
Sensor IDs must be whole numbers.

Note

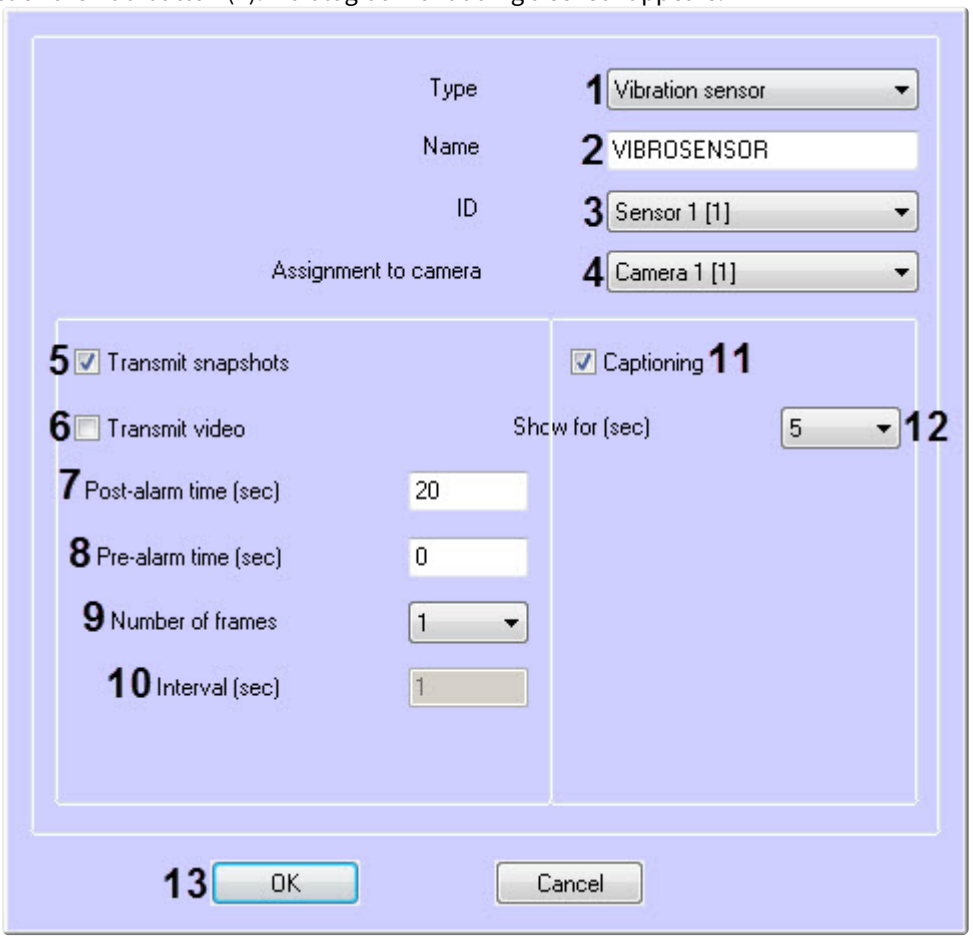
If video data (i.e. clips or snapshots) are attached to the alarms, it is necessary to create a script for stopping recording on camera (see Sample script for stopping camera recording).

To configure the list of sensors in use:

1. Go to the configuration panel for the **Partition Of Control** object.



2. Click the **Add** button (**1**). A dialog box for adding a sensor appears.



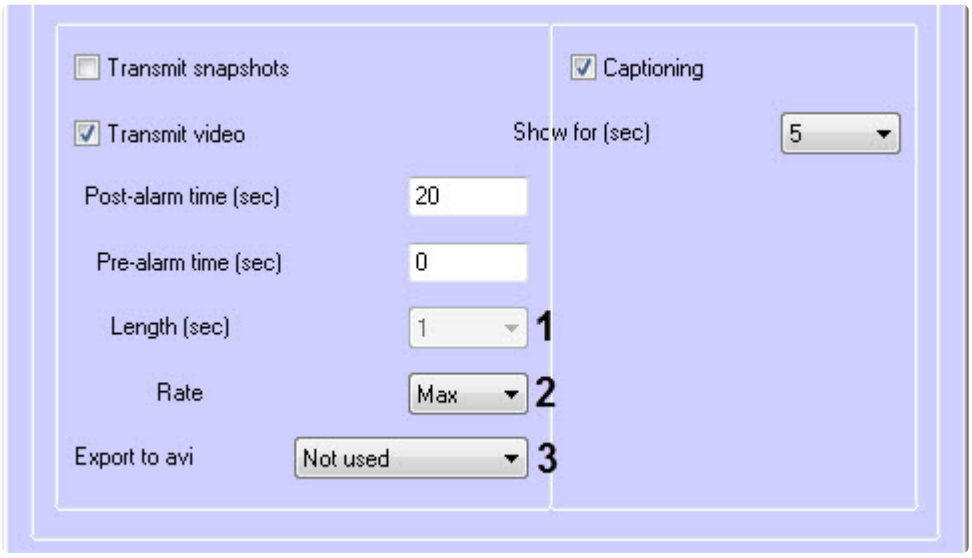
3. In the **Type** drop-down list, select the type of sensor from the sixteen types described previously (**1**).
4. In the **Name** field (**2**), enter the text that will be sent to *Server of Control* together with the alarm message. This text will be overlaid on the video during the captioning process.
5. In the **ID** drop-down list, select a **Sensor** object that has been previously created in the Intellect device tree (**3**).
6. In the **Assignment to camera** drop-down list, select a video camera from which the video frames or video clips should be requested (**4**).
7. To enable sending video frames to *Server of Control* when a sensor is activated, select the **Transmit snapshots** check box (**5**).
8. If you want for a video fragment to be sent to *Server of Control* when a sensor is triggered, select the **Transmit video** check box (**6**).
9. In the **Post-alarm time (sec.)** field, enter the time delay between when a sensor is triggered and the time of access to the video archives, in seconds (**7**). The default value is 20 seconds. This parameter is necessary for guaranteed recording on camera.
10. In the **Pre-alarm time (sec.)** field, specify the amount of time for which you want to pre-record before sensor triggering, in seconds (**8**). This allows obtaining video frames depicting not only the very moment at which an alarm occurs, but a short time before.
11. If the **Transmit snapshots** check box was selected:
    a. In the **Number of frames** drop-down list, select the quantity of video frames to be transferred when a sensor is triggered (**9**).
    b. In the **Interval (sec.)** field, enter the length of time, in seconds, between video frames if more than one frame is to be sent (**10**). Thus when an alarm occurs, it is possible to send to *Server of Control* an

entire sequence of frames that represent different points in time, which increases the chance of viewing the most valuable frames.

> **Attention!**
>
> For snapshots transmitting more, as well as for video clips transmitting, it is necessary to create a script for stopping video recording on camera (see Sample script for stopping camera recording).

> **Attention!**
>
> When specifying the **Pre-alarm time**, **Number of frames**, and **Interval** settings, keep an eye on the configuration of the camera from which video frames are to be sent, and particularly on the **Pre-alarm record** setting. **Pre-alarm record** time on camera have to be greater or equal to **Pre-alarm time** value in sensor settings.

12. If the **Transmit video** check box was selected:
    a. In the **Length (sec.)** field (**1**), specify the length of the video fragment to send.



Attention!

If the **Not used** value is selected in the **Export to avi** parameter (**3**), then the **Length (sec.)** parameter will be unavailable. In this case, the length will be determined by the size of the video fragment file in the video archive. To limit the length of the video fragment to be sent, use a script to stop recording on the camera (a sample script is found in the Sample script for stopping camera recording).

b. In the **Rate** field, enter the transmission rate for the video fragment (**2**).
c. The **Export to avi** parameter (**3**) allows you to select the format and codec of the requested video clip:
   - **Not used** - the video clip will be exported as an archive with a set of directories and files from the VIDEO folder.
   - **Original** - the video clip will be exported to an avi-file without transcoding.
   - **Xvid** - the video clip will be exported to an avi-file with the Xvid codec.
   - **DivX** - the video clip will be exported to an avi-file with the DivX codec.
   - **x264** - the video clip will be exported to an avi-file with the x264 codec.

Attention!

The export to an avi-file with the specified codec is performed on the *Agent Of Control* side using the **AviExport.run** module. The **AviExport.run** module version used on the *Agent Of Control* should be no lower than 4.10.5.3776, and the required codec should be installed. Otherwise, an error **Frame or video clip is not found (archive export error)** will be received.

Note

If the *Agent Of Control* version is lower than 11.0.1520, then the value of the **Export to avi** parameter will be automatically set to **Not used** without the possibility of changing it.

13. If it is necessary to overlay captions on video when a sensor is triggered, select the **Captioning** check box (**11**). In the **Assignment to camera** field, specify the camera on whose video you want to overlay captions (**4**).

14. In the **Show for (sec.)** drop-down list, select the amount of time for which you want captions to be displayed on video, in seconds (**12**).
15. Click **OK** (**13**).

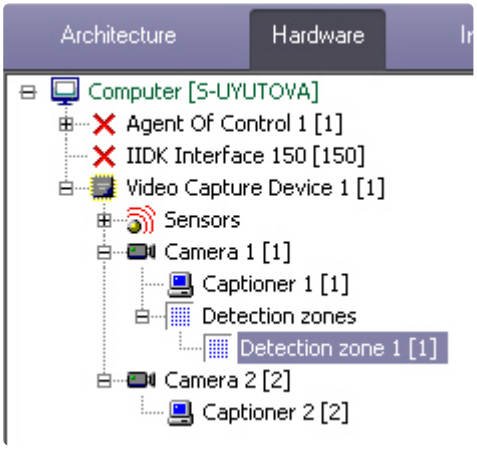
Configuration of the list of used sensors is now complete.

5.3.7 Configuring alarm groups

Configuration for associating events with certain alarm groups

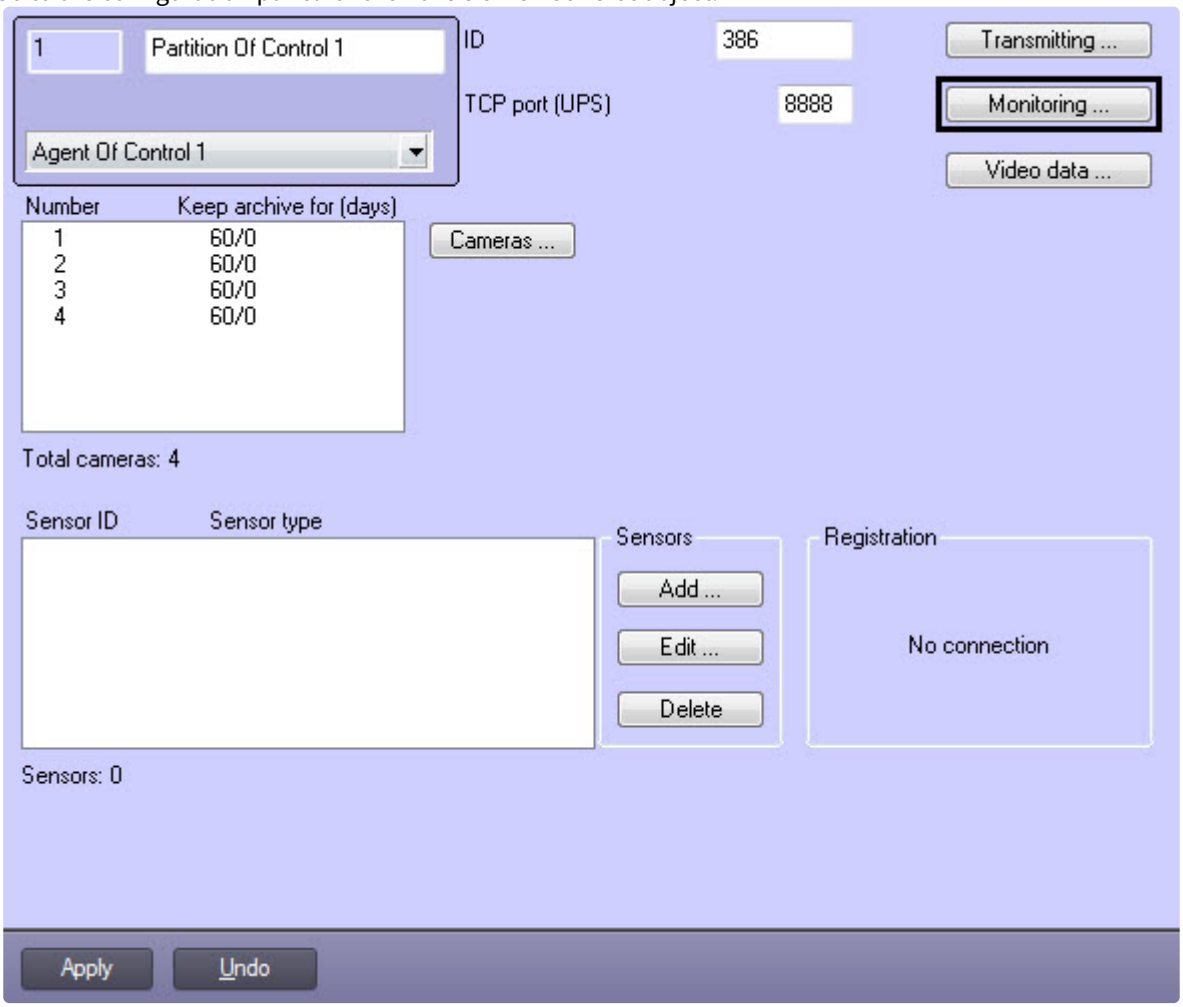
By default, for the **Access Control** and **Detection Tools** alarm groups, no data is sent from *Agent Of Control*. These alarm groups, as well as **Hardware** and **Fire/Security System**, can be used for designating their respective alarm types.

To classify events of an object as belonging to a particular alarm group, create an object (if it does not exist already) in the device tree. For example, if you want for the signal from the **Abandoned Object Detection Tool** to be displayed in *Monitoring* in the **Detection Tools** alarm group, create a **Detector Zone** object and configure it (select the **Abandoned Object Detection Tool** type, specify the detection area and sensitivity, etc.; for more details, see Intellect Software Package: Administrator's Guide).



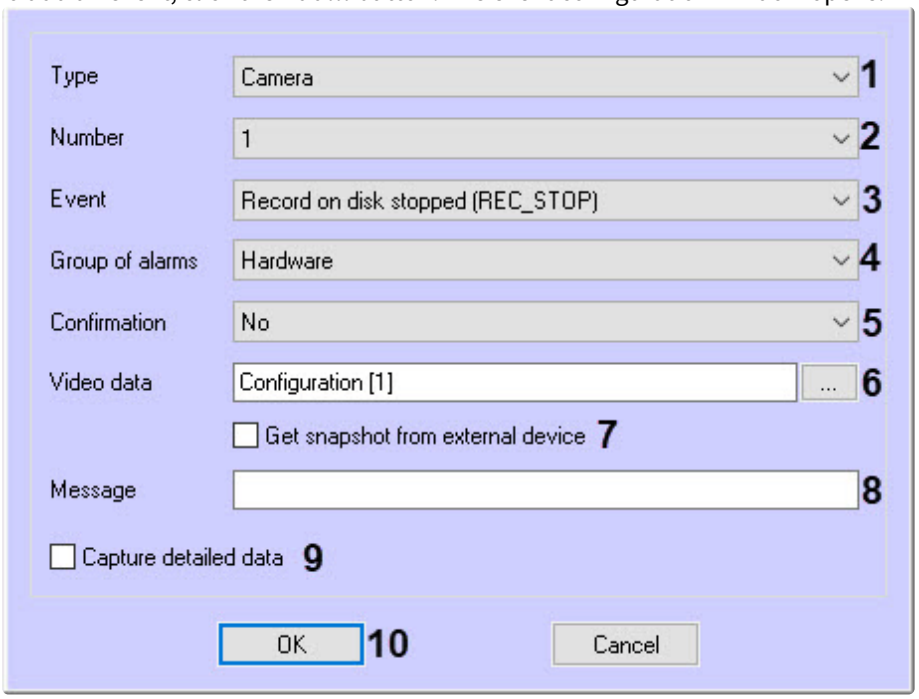
To associate the events with particular alarm groups, do the following:

1. Go to the configuration panel for the **Partition Of Control** object.



2. Click the **Monitoring...** button. The **Add/Edit events for Monitoring** window opens.

3. To add an event, click the **Add...** button. The event configuration window opens.



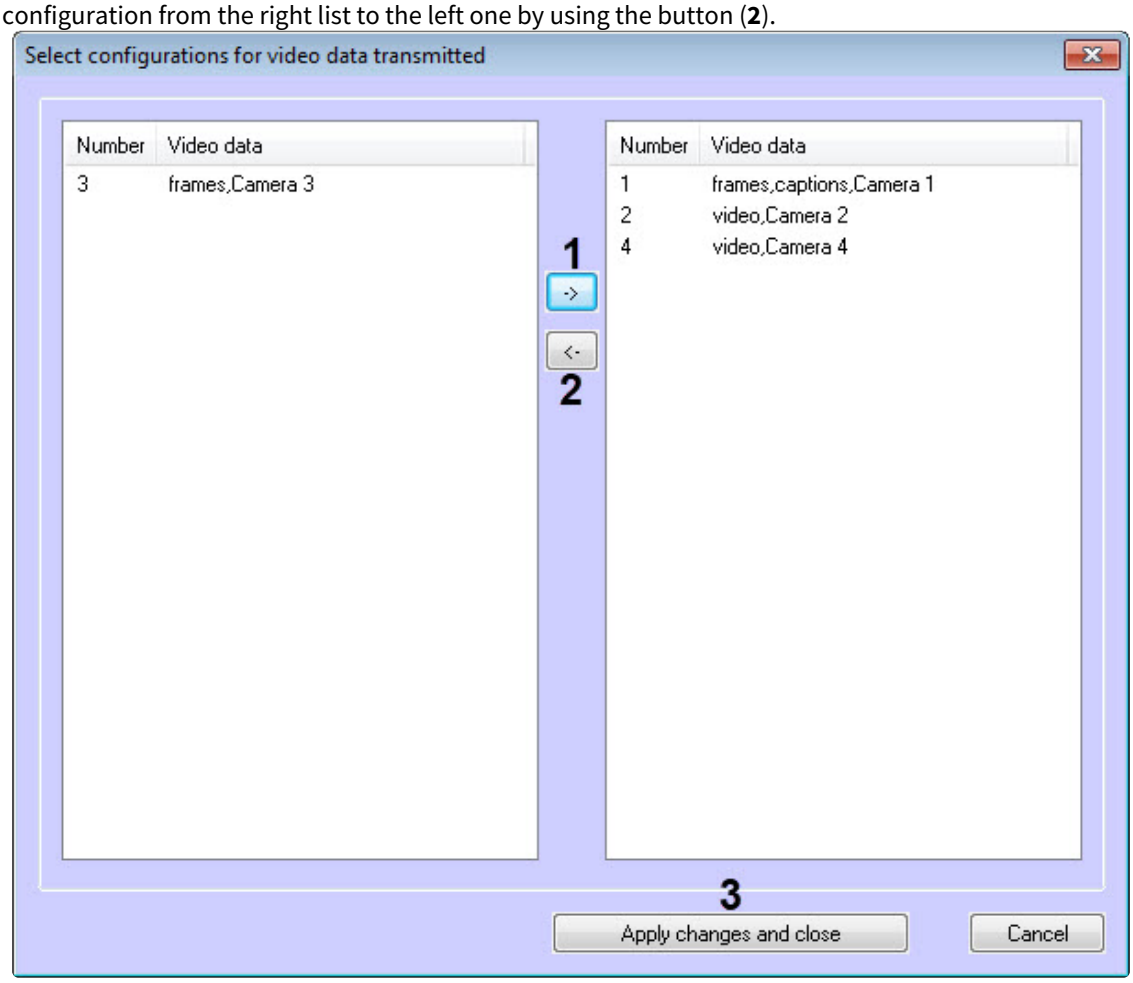
4. In the form that appears, from the **Type** drop-down list (**1**), select the type of device. This list contains the types of all objects created on the **Hardware** tab of the **System settings** window that have recorded events. Example: In the case of the Abandoned Object Detection Tool, select the **Detector Zone** type.
5. From the **Number** drop-down list (**2**), select an ID number for the object of the selected type from which you want to get events. If you want to get events from all devices of this type, leave this field blank.
6. From the **Event** drop-down list (**3**), select the event type. The available event types depend on the selected object type. System type of the event in brackets is used in scripts and programs (see Guide for creating scripts (programming) and The Script object. Programming using the JScript language).
   For example, for the Abandoned Object Detection Tool triggering event, select **Alarm in the zone (MD_START)**.
7. From the **Group of alarms** drop-down list (**4**), select an alarm group and indicate in which alarm group you want for *Monitoring* to display alarms for this event.
8. It is possible to get confirmation of alarm acceptance from the *Server Of Control*. To do this, from the **Confirmation** drop-down list (**5**), select the type of confirmation:
   a. **No**—no confirmation is sent.
   b. **Simple**—*Agent Of Control* sends confirmation when an alarm is confirmed by the operator.
   a. **Complex**—when accepting an alarm the operator must confirm it in the confirm box and after that the confirmation is sent.

> **Note**
>
> - The *Agent Of Control* sends the "Confirmed: Monitoring event" message to *Intellect* core when there is the confirmation of alarm acceptance on the *Server Of Control*. Scripts that use this event can be created in *Intellect*—see Sample scripts for processing alarm confirmations.
> - Confirmation sending can be disabled on the side of the *Server Of Control*—see Sending confirmations of alarm acceptance.

9. If it is necessary to attach video data to alarms, click the **Video data** button (**6**). As a result, the **Select configurations for video data transmitted** window will open.

> **Note**
>
> Configuration of the transmitted video data is described in Setting up the configurations for transferred video data.

a. Move the required configurations using the button (**1**) from the left list to the right. Remove a configuration from the right list to the left one by using the button (**2**).



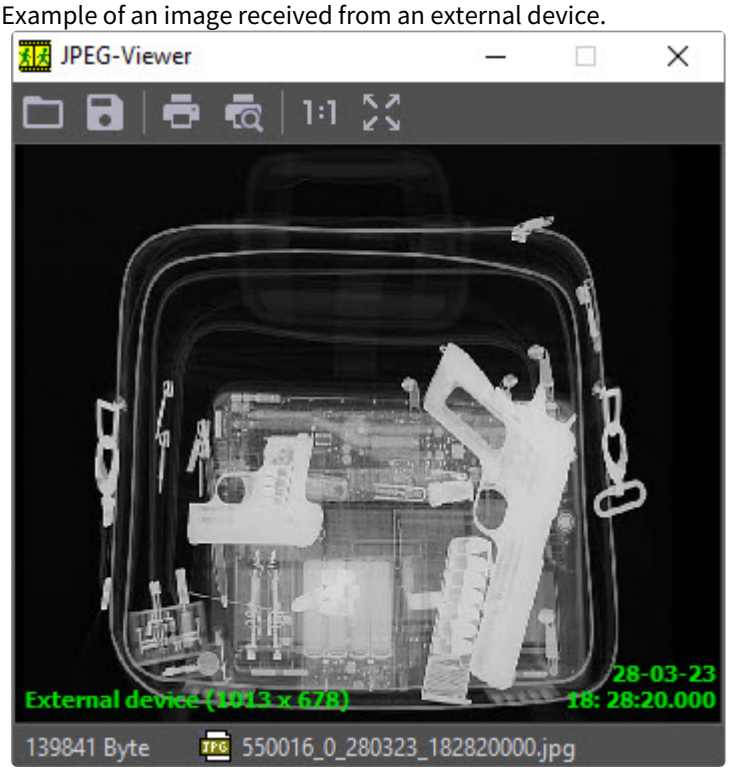
> **Attention!**
>
> Multiple configurations cannot be used for the same camera.

b. Click the **Apply changes and close** button (**3**). The selected configurations will be listed in the non-editable **Video data** field.

10. To add the possibility of attaching a snapshot not associated with the camera to an event, set the **Get snapshot from external device** checkbox (**7**). This way you can transmit, for example, a JPG snapshot received from an X-ray apparatus.

> **Attention!**
>
> To enable the **Get snapshot from external device** setting, the imageBase64<> substring with an image encoded in it must be present in the monitored event.

Example of an image received from an external device.

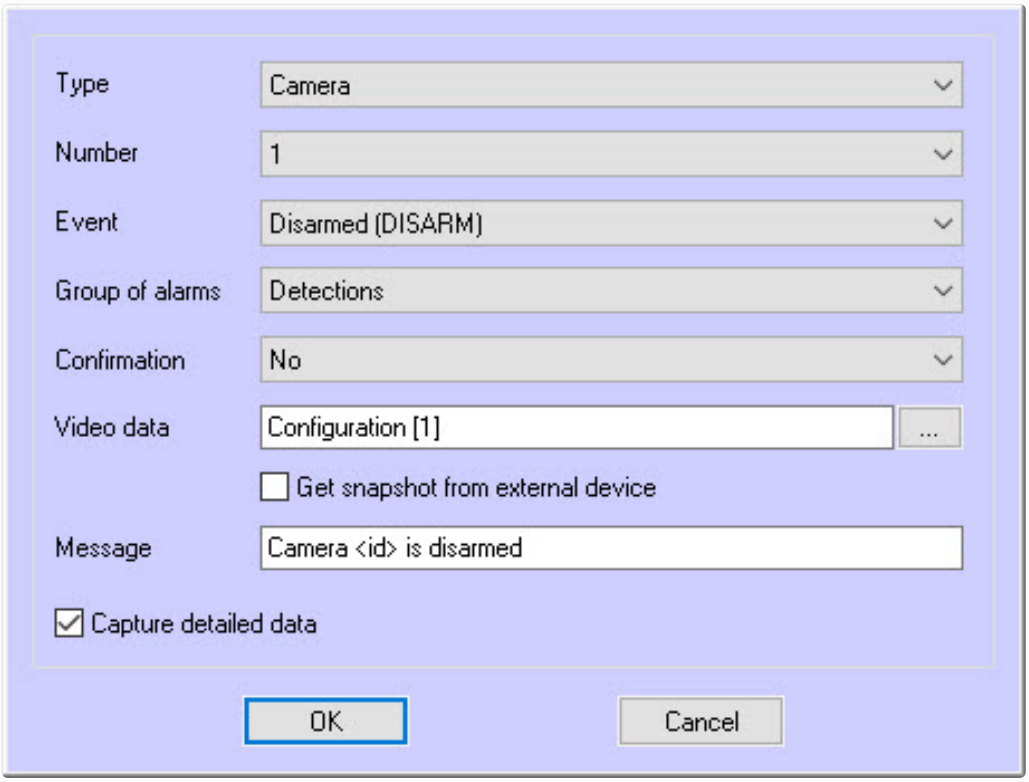


11. In the **Message** field (**8**), enter the text message, that will appear in the **Device** column of the **Alarm Reaction** dialog form (see Monitoring Software Package: Operator's Guide).
    If the object identifier is not specified, the following variables can be used in the **Message** field to detail the message:
    a. <id>—identifier of the object from which the event came.
    b. <name>—the object name.

> **Attention!**
>
> <id> and <name> are to be in lower case.
> After substitution of variables values the message must not be longer than 60 characters. If the resulting message is longer, extra characters will be dropped.

> **Example**

When the **Disarmed** event appears at the **Camera 1**, the “Camera 1 disarmed” message is sent.



12. To search for additional information in messages from a device of this type (for the substring "param0<>"), set the **Capture detailed data** checkbox (**9**).
13. Click the **OK** button to save the changes (**10**).

This means that when integrating a new device into *Intellect*, if a developer wants to be able to send more detailed information to *Monitoring*, when generating an event from the device, the developer should add detail in the param0<> parameter. For example, if there is a Motherboard Control module that has the Alarm event, the following values could be included in param0<>: "processor cooler", "BIOS battery", etc. If you enter "Motherboard" in the **Message** field and select **Capture detailed data**, the following text may appear in the **Device** column of the **Alarm Reaction** dialog form: "Motherboard (CPU cooler)".

Similarly, it is possible to monitor messages from other objects created in the *Intellect* hardware tree, on the **Hardware** tab.

Configuration for associating events with certain alarm groups is now complete.

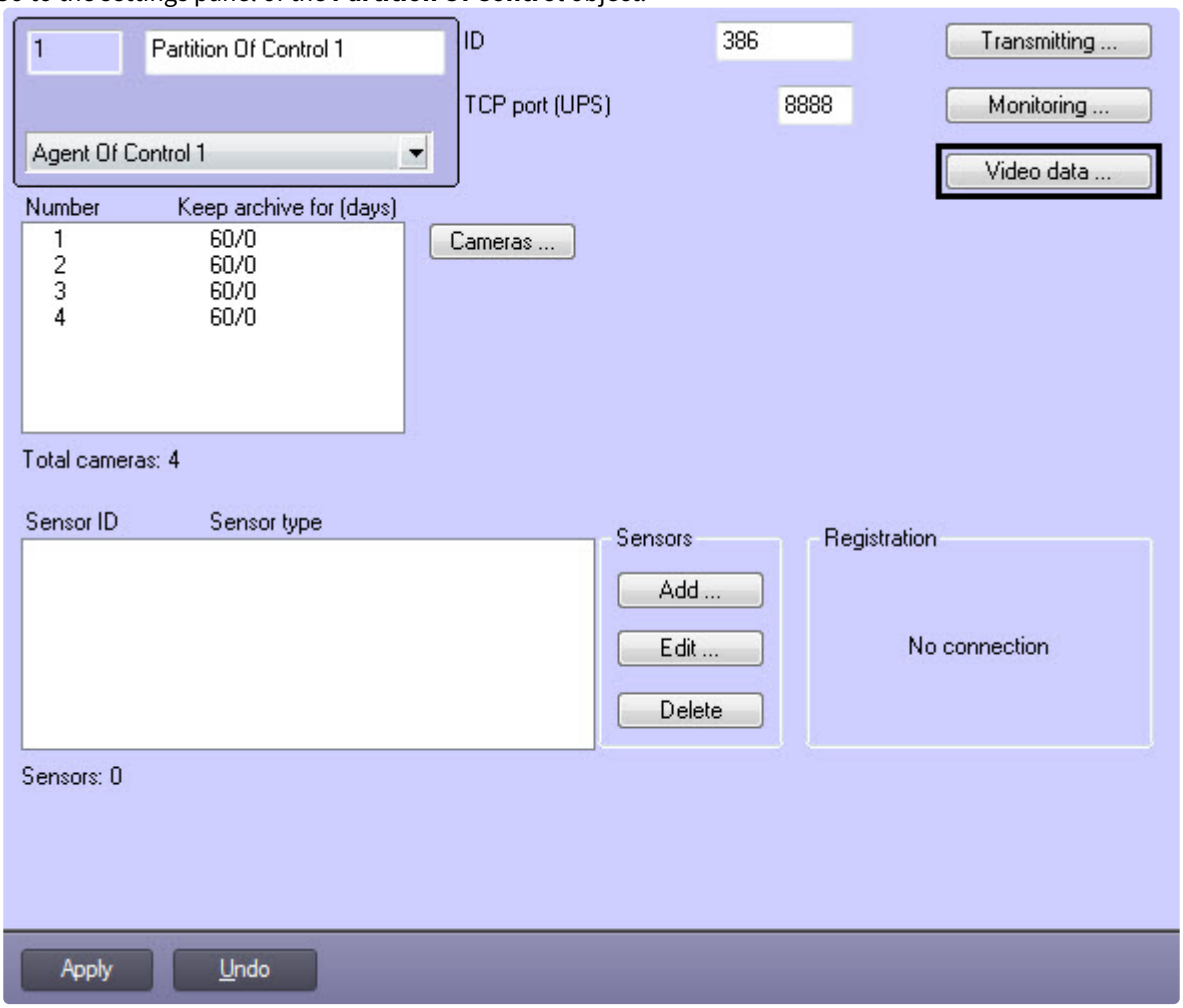
Setting up the configurations for transferred video data

If the transmission of user alarms (see Configuration for associating events with certain alarm groups section) to the *Server of Control* is configured, then video data can be added to these alarms. The video data transmission configurations can be created in *Monitoring* software in order to be added to any events when configuring alarm groups.

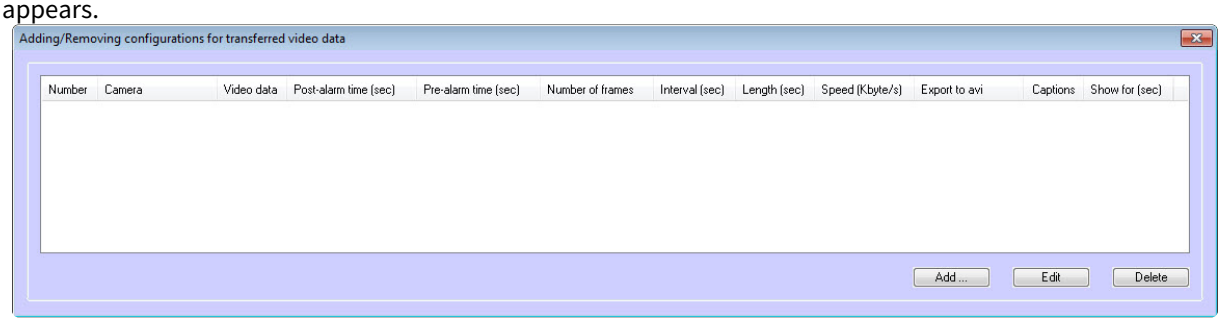
> **Important!**
>
> If video data (snapshots or videos) is added to an alarm, then the script for stopping camera recording is to be created (see Sample script for stopping camera recording section).

Set up the configurations for transferred video data as follows:

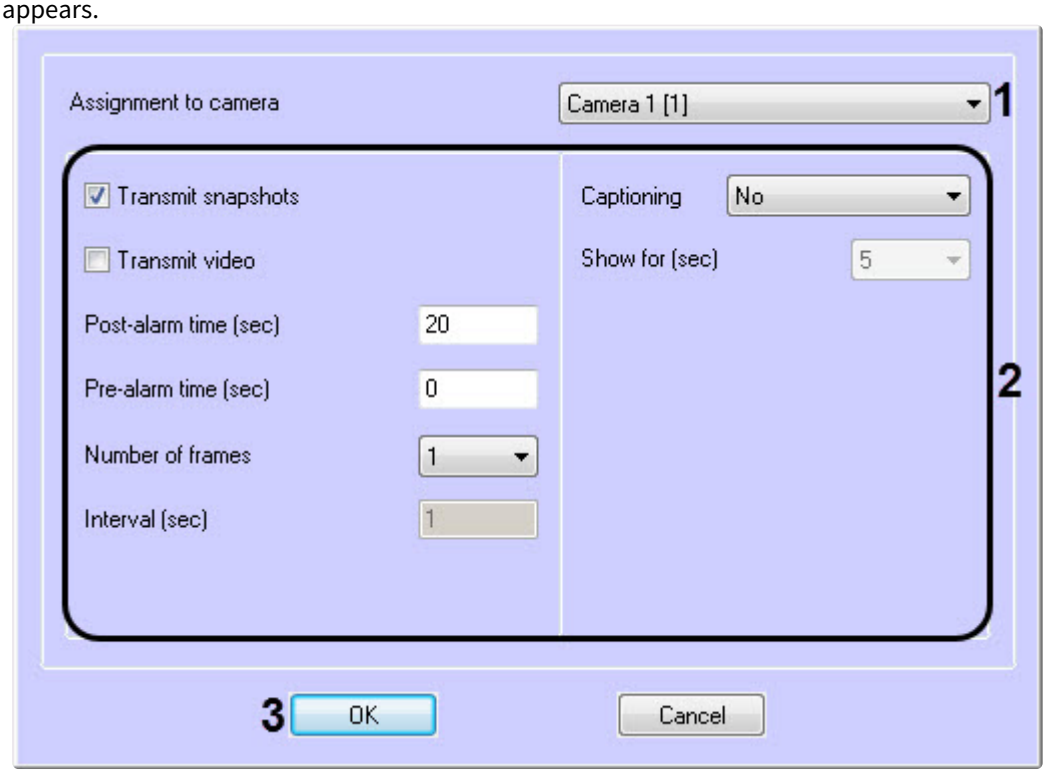
1. Go to the settings panel of the **Partition Of Control** object.



2. Click the **Video data…** button. The **Adding/Removing configurations for transferred video data** box appears.



3. To add a new video data transmission configuration click the **Add...** button. The configuration settings box appears.



4. From the **Assignment to camera** drop-down list (**1**) select the **Camera** object that will be used for getting video data.
5. Configure the data transmission parameters (**2**). The data transmission parameters are the same as those for video data transmitted along with sensor alarms (see Configuring sensors section, steps 7-17).
6. Click the **OK** button (**3**). The created configuration is added to the list.
7. Click the **Apply** button.

Setting up the configurations for transferred video data is complete.

Changing the description of short alarms and long alarm Object disarmed

To change the description of a long alarm **Object disarmed** in the **Monitoring** and **Monitoring Reports** interface objects, it is necessary to specify the required description for the **CustomizedLongAlarmName** registry key on the *Server Of Control* and *Central Server Of Control* side (for details, see Registry keys reference guide, for more information about working with the registry, see Working with Windows OS registry).

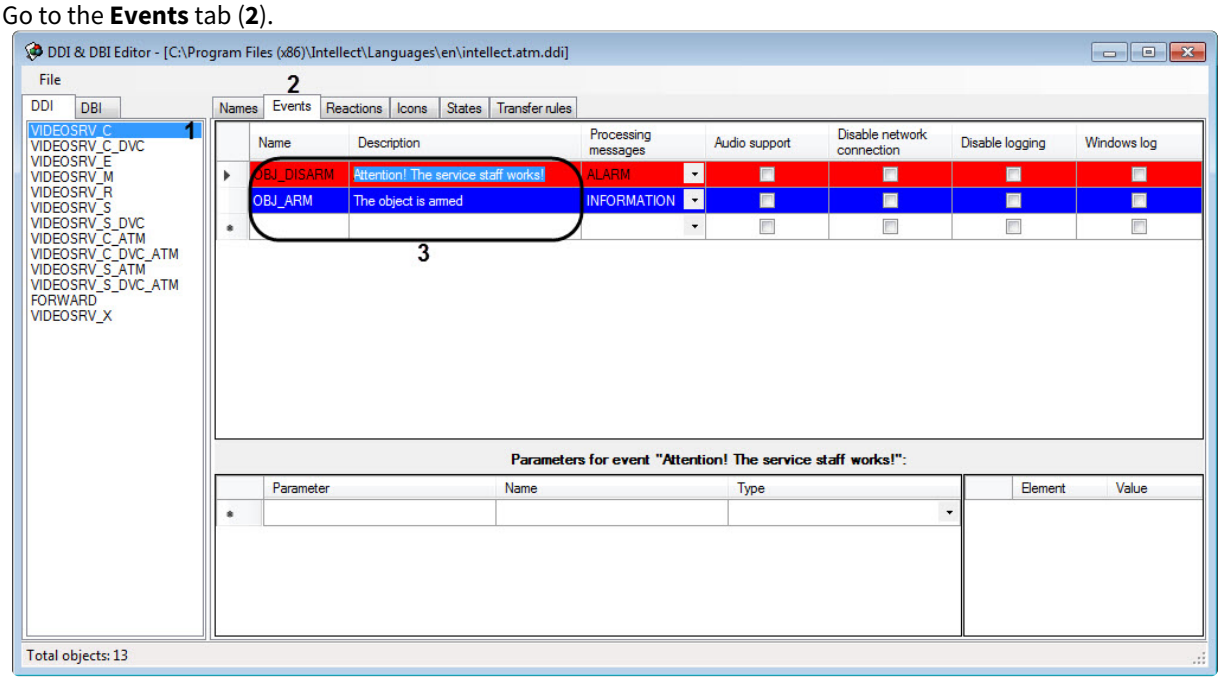
To change the description of short alarms that occur with the **OBJ_ARM** and **OBJ_DISARM** events, do the following:

1. Run the *ddi.exe* utility on the *Agent Of Control* side.

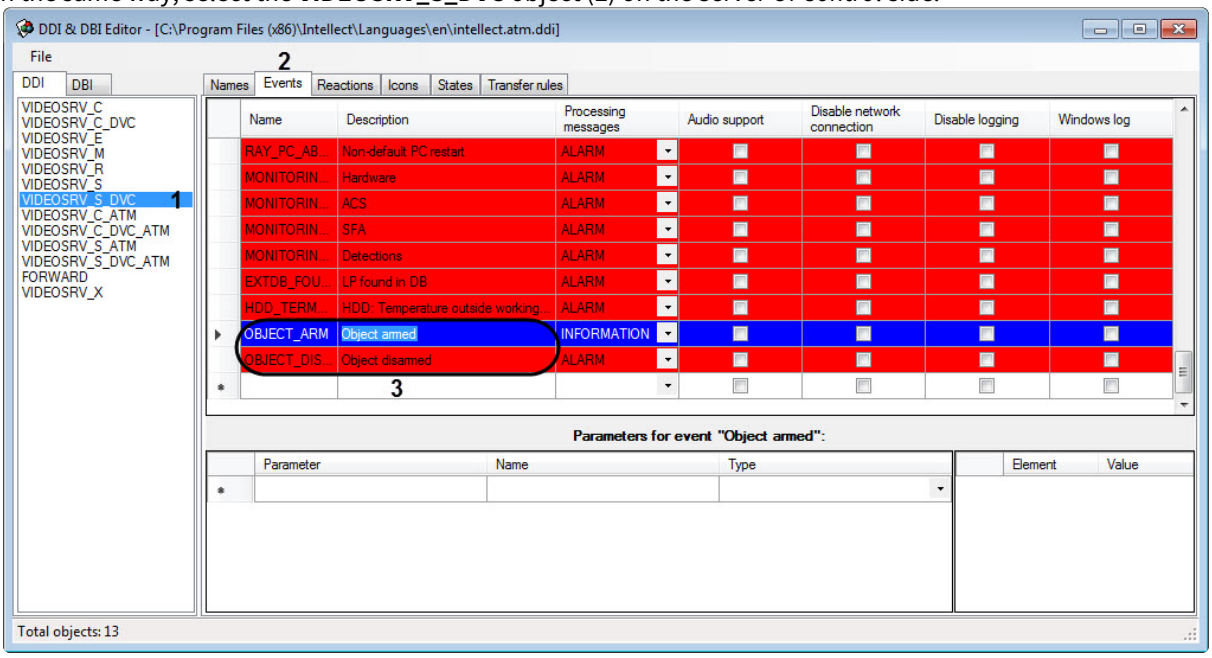
> **Note**
>
> For detailed information about working with this utility, see Intellect integration guide (HTTP API, IIDK, ActiveX, HTTP Server, Axxon Next).

2. Open the **intellect.atm.ddi** file, which is located in the <*Intellect installation directory*>*Languages**ru*.
3. Select the **VIDEOSRV_C** object (**1**).

4. Go to the **Events** tab (**2**).



5. In the **Description** column, specify the necessary text for the **OBJ_ARM** and **OBJ_DISARM** events (**3**).
6. Save the changes to the file and restart the *Monitoring*.
7. In the same way, select the **VIDEOSRV_S_DVC** object (**1**) on the *Server Of Control* side.



8. Go to the **Events** tab (**2**).
9. In the **Description** column, specify the necessary text for the **OBJECT_ARM** and **OBJECT_DISARM** events (**3**).
10. Save the changes to the file and restart the *Monitoring*.

Changing the description of short alarms and long alarm **Object disarmed** is complete.

Configuring alarms for monitoring the object state on the Agent Of Control side

On this page:

General information about the alarms for monitoring of the object state on the Agent Of Control side

To monitor the object state on the *Agent Of Control* side, create an **AccessByCardEnable** string registry key and set **1** as its value (for details, see Registry keys reference guide, for more information about working with the registry, see Working with Windows OS registry).

By default, the following alarms will become available in the **Detection Tools** alarm group:

Alarm group	Event name	Alarm type (default alarm description)	Alarm length
Detection Tools	-	Object disarmed	Long alarm
	OBJ_DISARM	Attention! The service staff works!	Short alarm

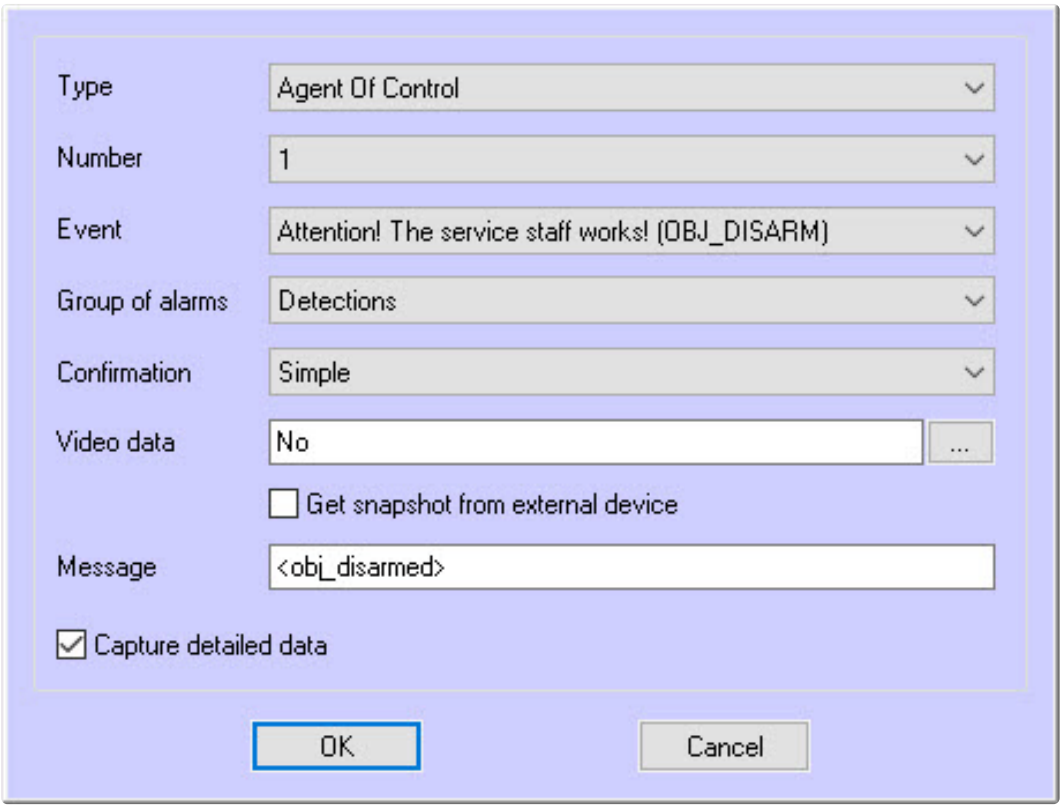
	OBJ_ARM	Armed object	Short alarm

These alarms are designed for the special mode of *Monitoring* operation with *ACFA Intellect* (see Configuring the special mode of Monitoring operation with ACFA Intellect). However, these alarms can be used to monitor the state of the relay, for example, to generate a short and long alarm when the relay switches from the **Relay on** to the **Relay off** state, and another short alarm when the relay switches from the **Relay off** to the **Relay on** state.

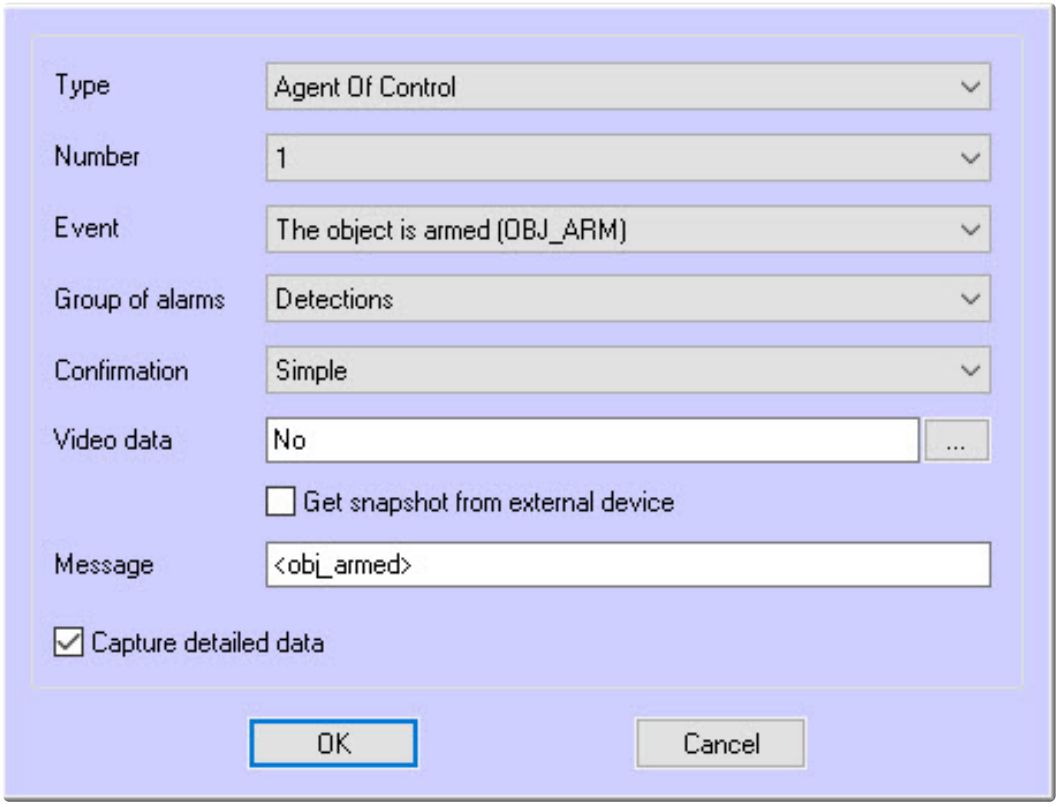
Configuring the alarms for monitoring the object state on the Agent Of Control side

You can change the description of alarms for the **OBJ_ARM** and **OBJ_DISARM** events, and the long alarm **Object disarmed** (for details, see Changing the description of short alarms and long alarm Object disarmed).

To receive the short alarms **Attention! The service staff works!** it is necessary to set up an alarm group as shown below.



To receive the short alarms **The object is armed**, it is necessary to set up an alarm group as shown below.

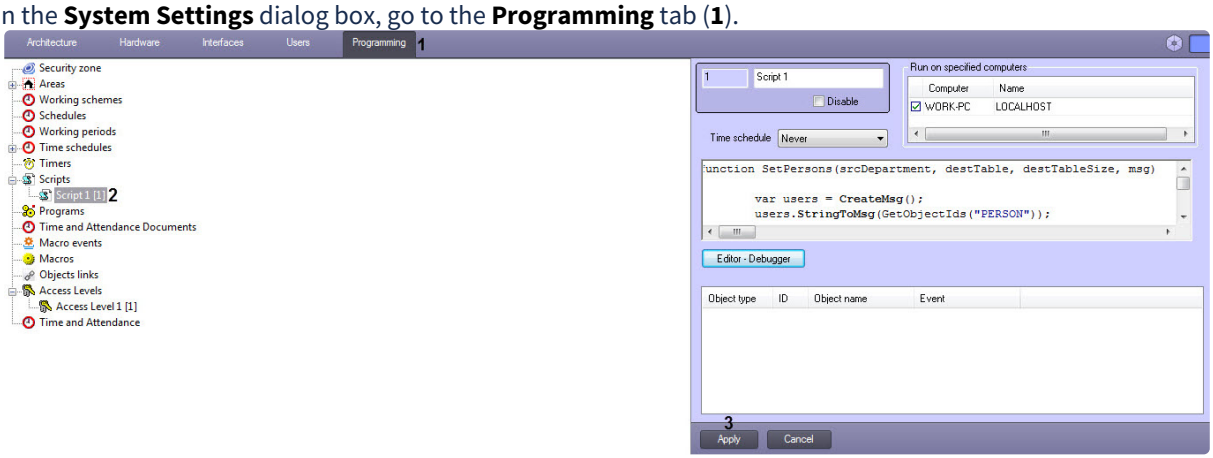


Note

It is necessary to enter the **<obj_disarmed>** and **<obj_armed>** messages in the lower case.

To monitor the object state on the *Agent Of Control* side, do the following:

1. In the **System Settings** dialog box, go to the **Programming** tab (**1**).



2. Create the **Script** object (**2**) on the basis of the **Scripts** object in the objects tree.
3. If you are configuring the special mode of *Monitoring* operation with *ACFA Intellect*, it is necessary to copy the contents of a sample script from the page Sample scripts for determining the current state of the zones of the Rovalant (A6, A16) object on the Agent of Control side.
4. If you are configuring the monitoring of the relay state, it is necessary to copy the contents of a sample script from the page Sample scripts for determining the current state of the relay on the Agent of Control side.

5. Click the **Apply** button (**3**).

Operating procedure

At startup, and then every 15 minutes, *Agent Of Control* sends a **GET_OBJECT_STATE** event to the *Intellect* core. This event is processed in a script, which then generates an **OBJECT_STATE_INFO** event with the object status in the **state** field and the additional information in the **card** field. When the state of the relay changes, this script generates the **OBJ_ARM** or **OBJ_DISARM** event a long alarm **Object disarmed**.

Configuring alarms for monitoring the object state on the *Agent Of Control* side is complete.

5.4 Connecting to uninterrupted power supplies

If your computer has a Smart-UPS uninterrupted power supply unit made by APS, messages from the UPS can be sent to *Server of Control*.

Configuration of a UPS is performed in the following order:

1. Install the StateUPS utility.
2. Configure the PowerChute plus utility.

5.4.1 Configuring StateUPS

StateUPS utility (exe-file and ini-file) is installed with *Agent of Control* and placed to the <*Intellect* software installation>/Vhost/UPS/.

> **Note**
>
> Files from the <*Intellect* software installation>/Vhost/UPS/Ext directory will look for the ini settings file in the same directory as the StateUPS utility.

Configure the file StateUPS.ini in this directory:

1. Address – address of the machine on which *Agent of Control* is running. The default value of this parameter is 127.0.0.1. If you install StateUPS on the same computer on which *Agent of Control* is installed, it is not necessary to change this parameter.
2. Port – TCP port to which StateUPS sends messages from the UPS. The value of this parameter must match the corresponding setting of *Agent of Control*, TCP port (UPS) (see the section Configuring a port for incoming UPS messages).

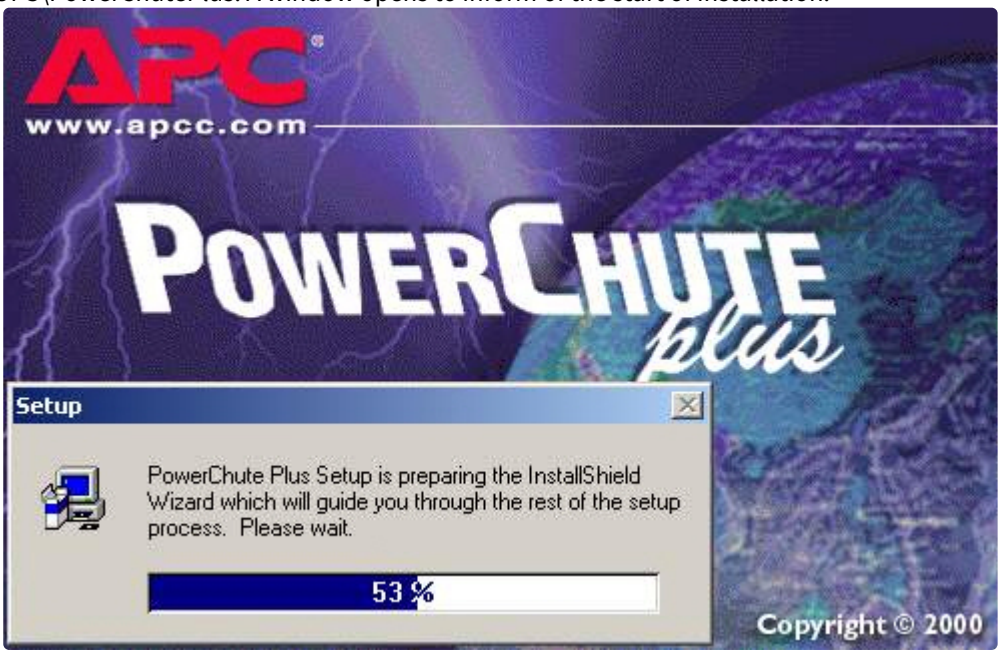
If the StateUPS utility is to be used on another computer, do the following:

1. Create "HKLM\SOFTWARE\BitSoft\VHOST\VHostService" section in the registry for 32-bit OS ("HKLM\SOFTWARE\Wow6432Node\BitSoft\VHOST\VHostService" for 64-bit) on this computer.
2. In this section, create the "FolderLog" parameter. In the "FolderLog" parameter specify the path where the UPS folder will be created containing ini-file. For example, if the folder is C:\EVUPS, then "FolderLog" = "C:\EVUPS\"
3. In the specified folder, for example, C:\EVUPS, create the UPS sub-folder and copy the StateUPS.ini into it.

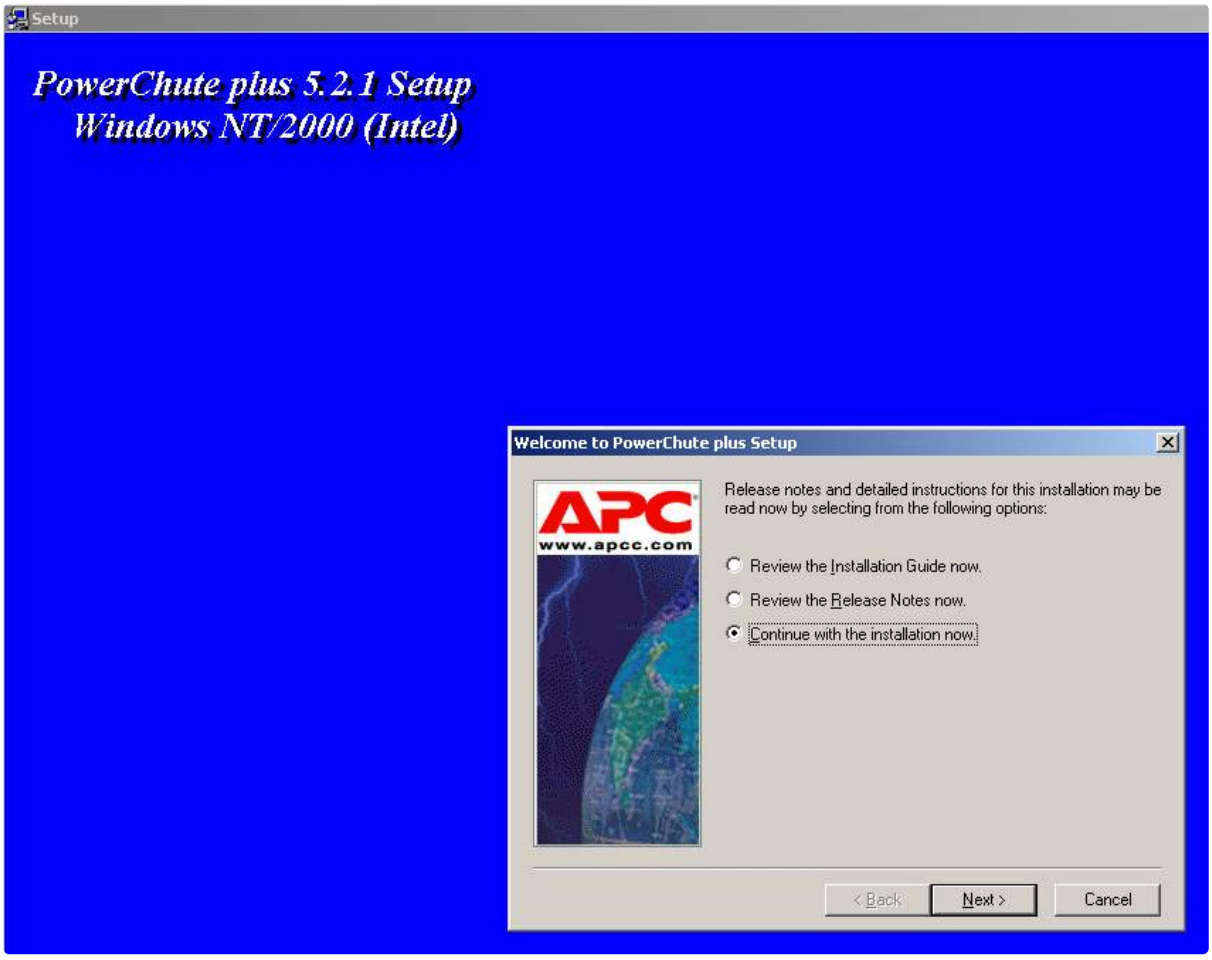
5.4.2 Installing the software from the UPS vendor

After the StateUPS is configured, install the software from the UPS vendor. Before starting installation, make sure that the interface cable is connected to the UPS.

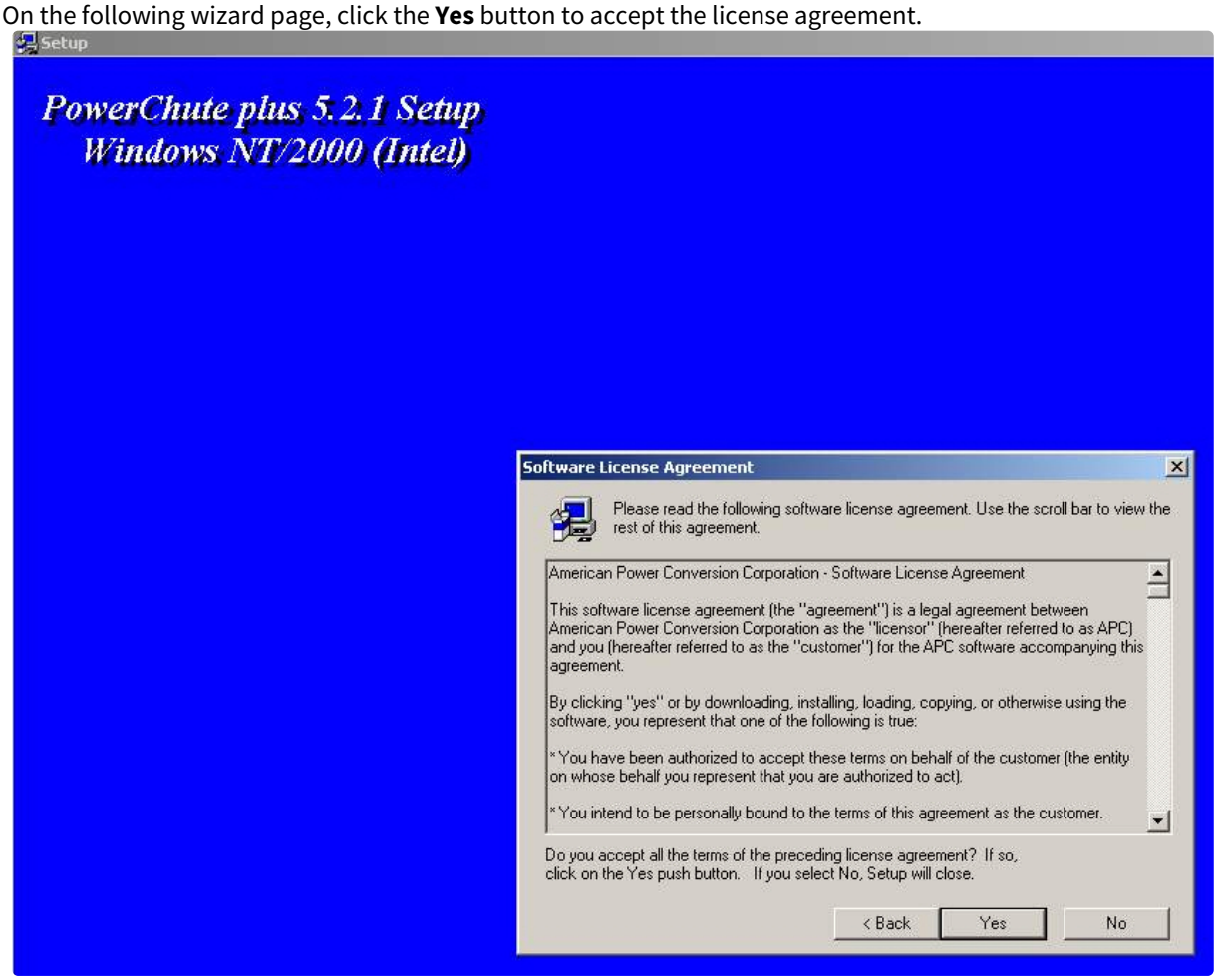
1. To start the installation process, start the executable file pc521.exe in the installation folder UPS\PowerChutePlus. A window opens to inform of the start of installation.



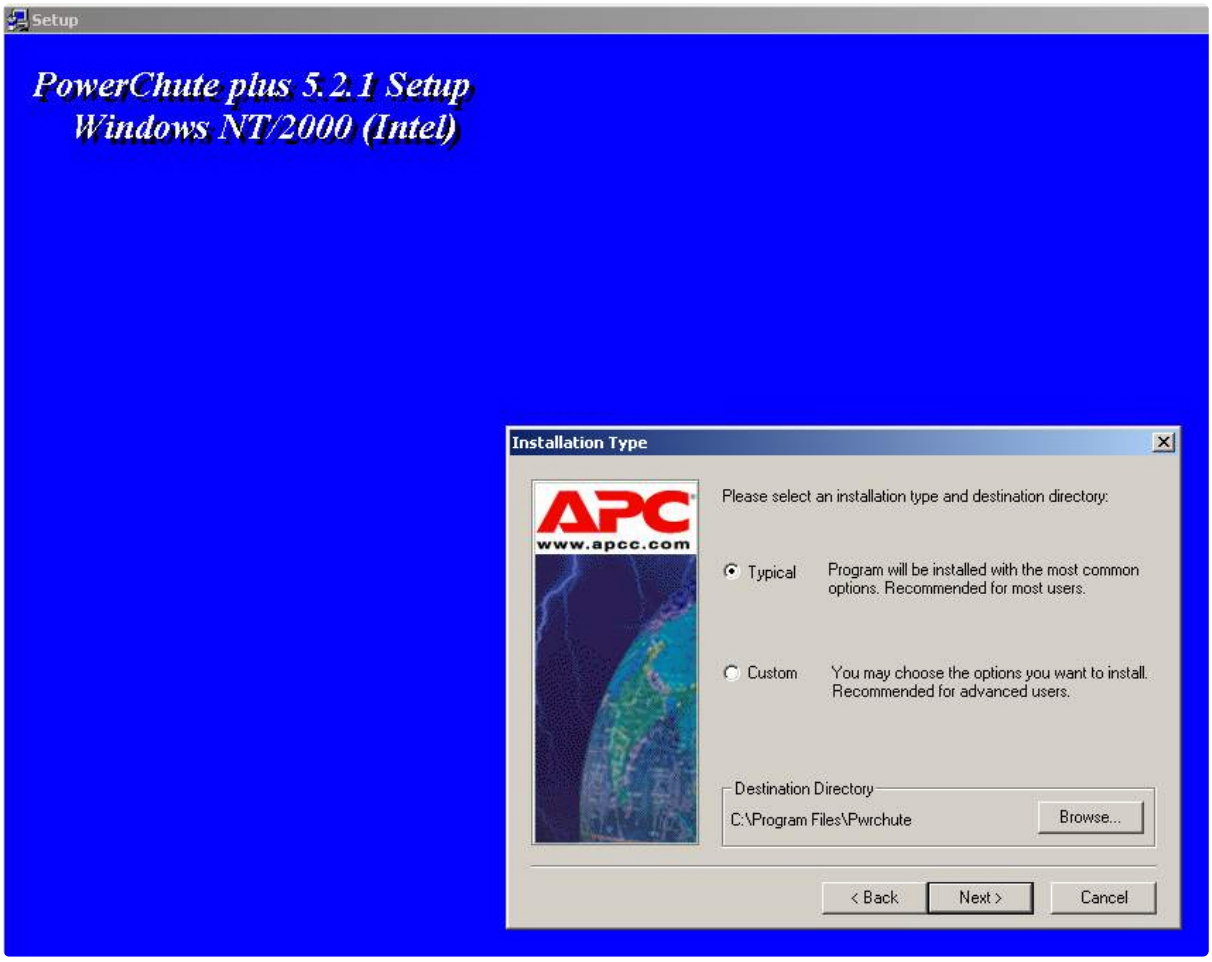
2. On the following wizard page, select the option **Continue with the installation now** and click the **Next** button.



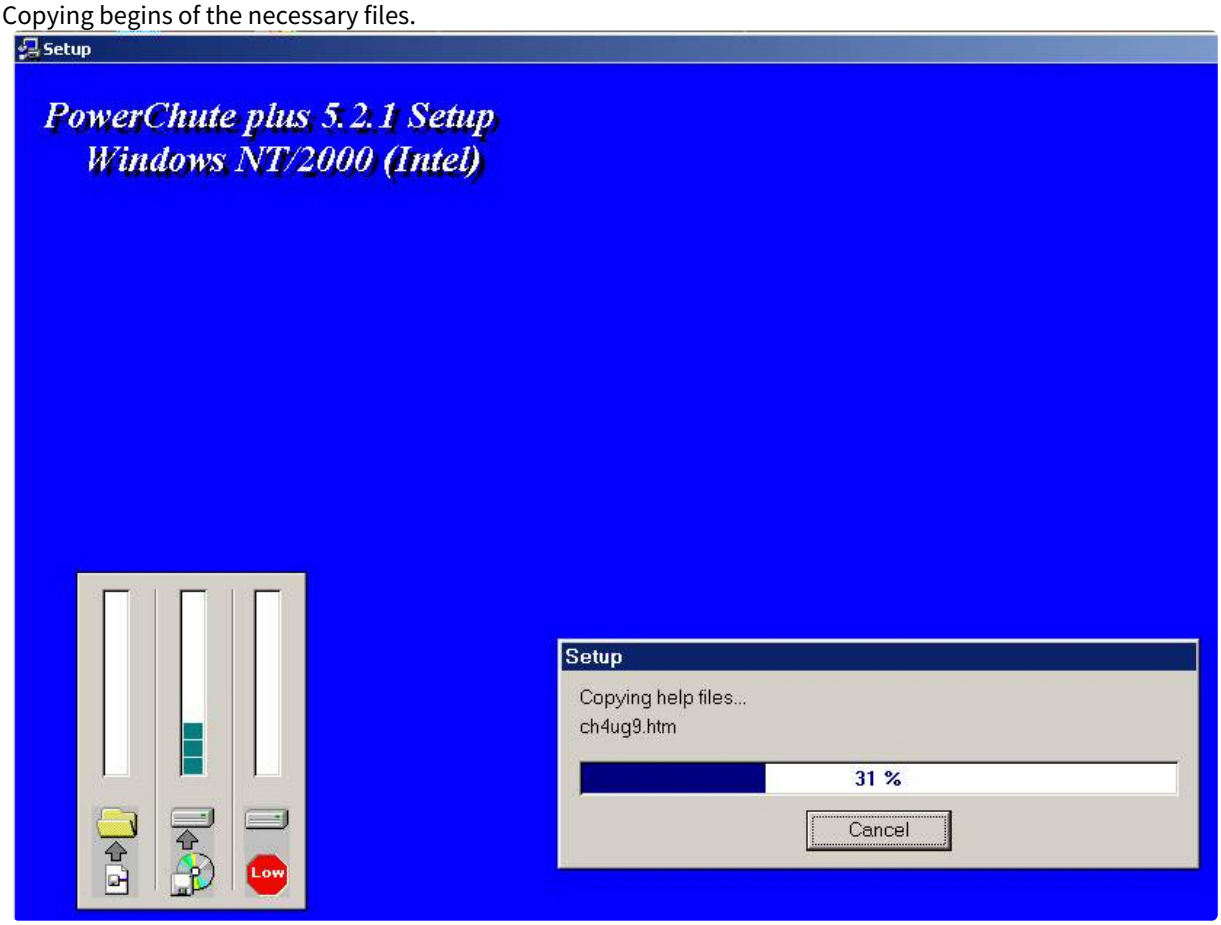
3. On the following wizard page, click the **Yes** button to accept the license agreement.



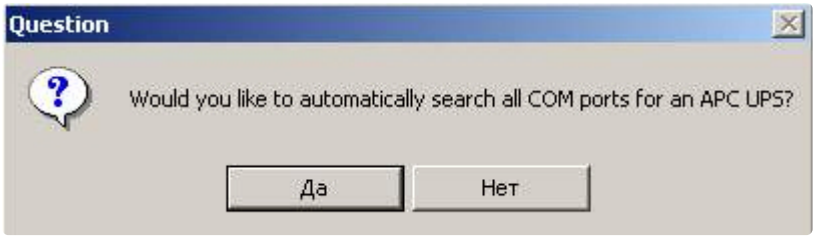
4. On the following wizard page, select the **Typical** installation type and indicate the path at which you want to install the software.



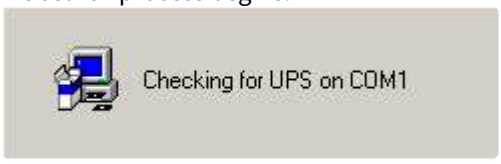
5. Copying begins of the necessary files.



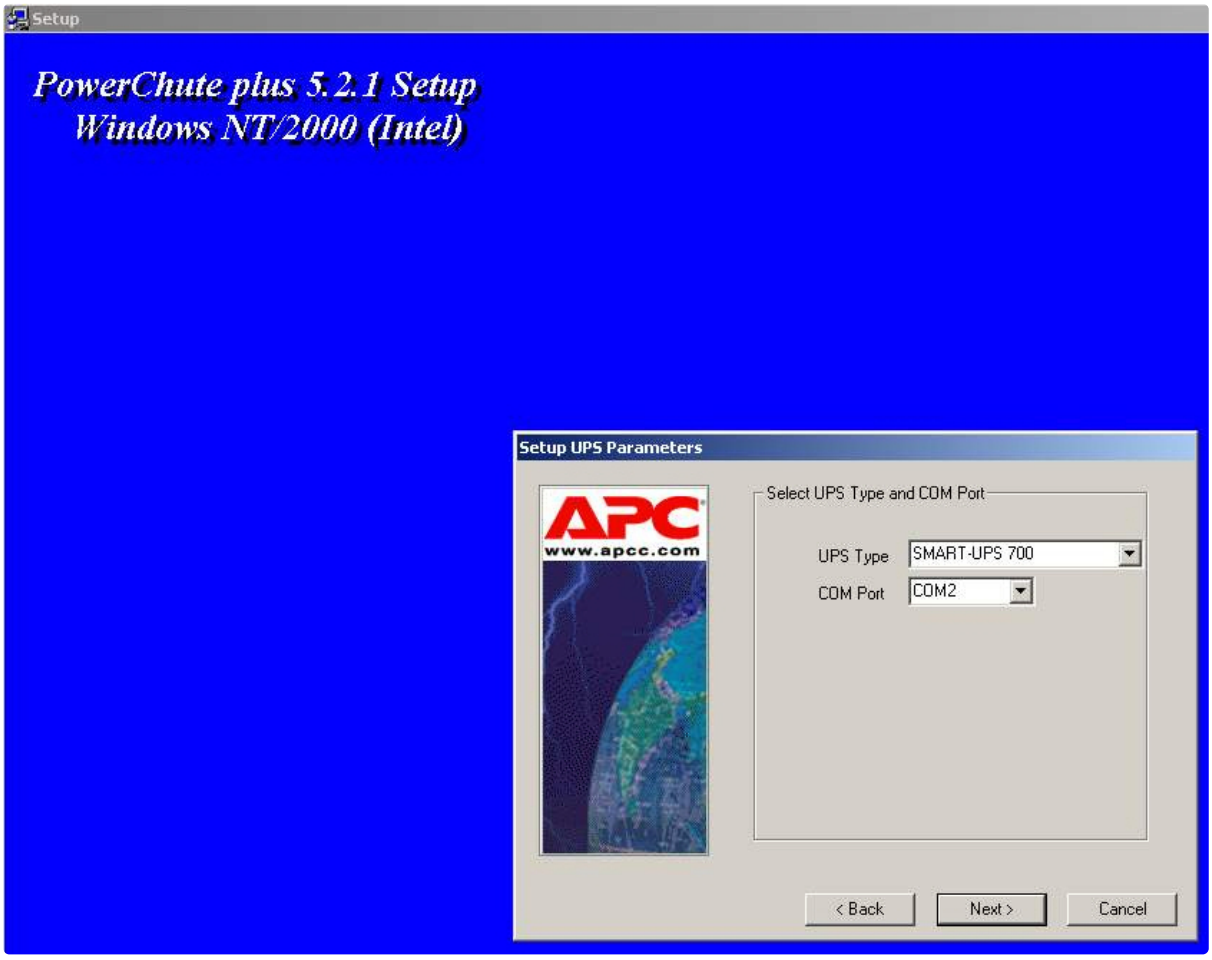
6. When copying is complete, a dialog box appears with a request to automatically determine the COM port on which the UPS is located. Click the **Yes** button.



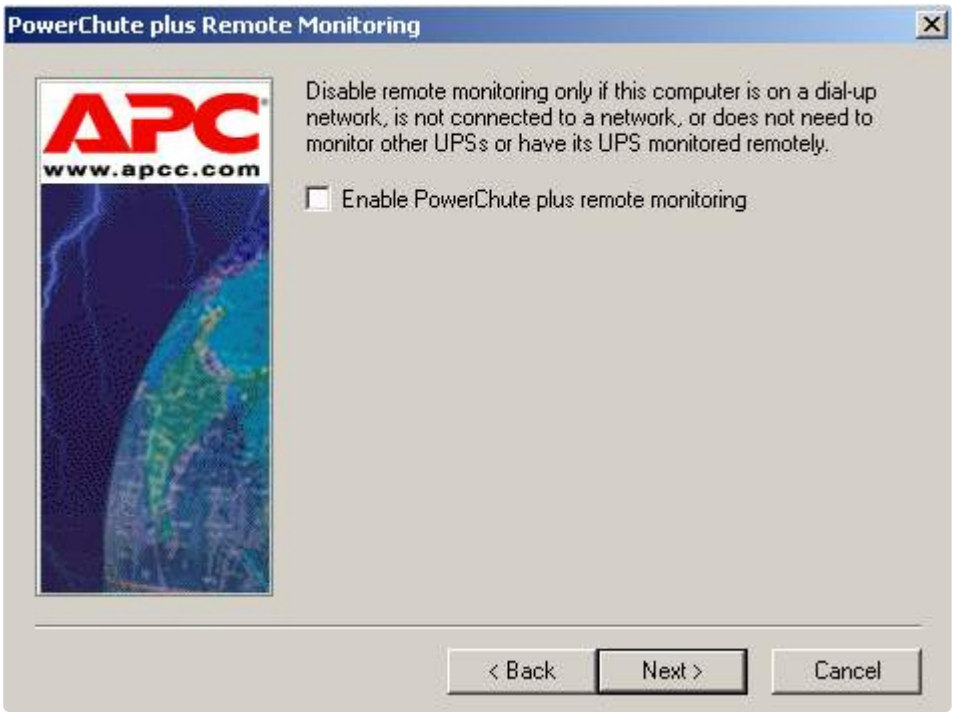
7. The search process begins.



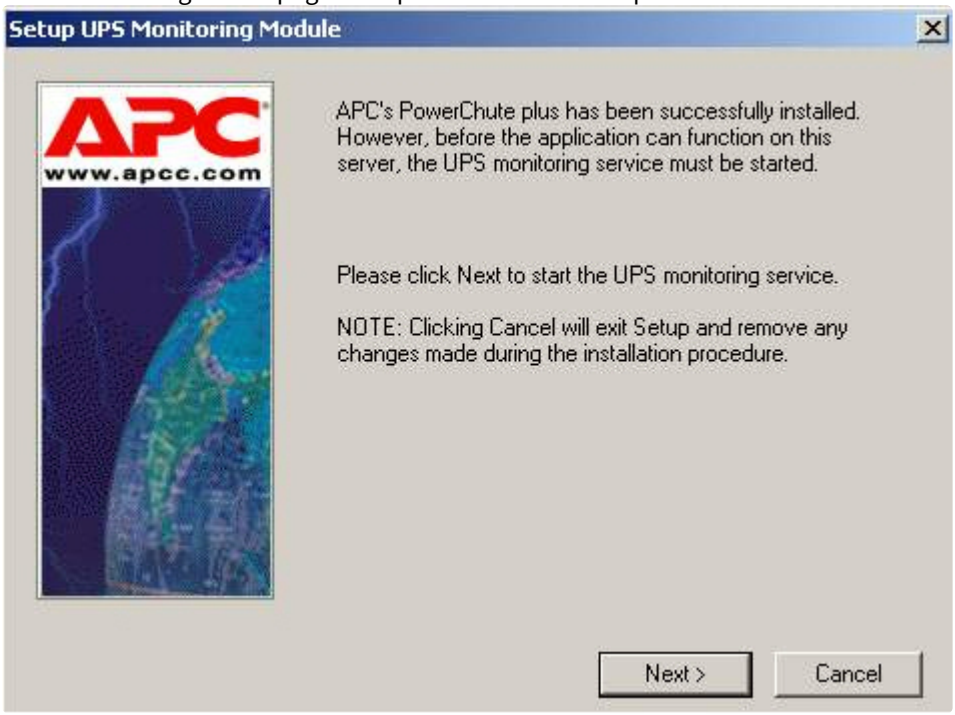
8. When the search is complete, the program will show what type of UPS it found and on which COM port. Click the **Next** button.



9. On the next wizard page, clear the **Enable PowerChuteplus remote monitoring** check box and click the **Next** button.



10. The two following wizard pages complete the installation process.



Dialog box to confirm installation completion.

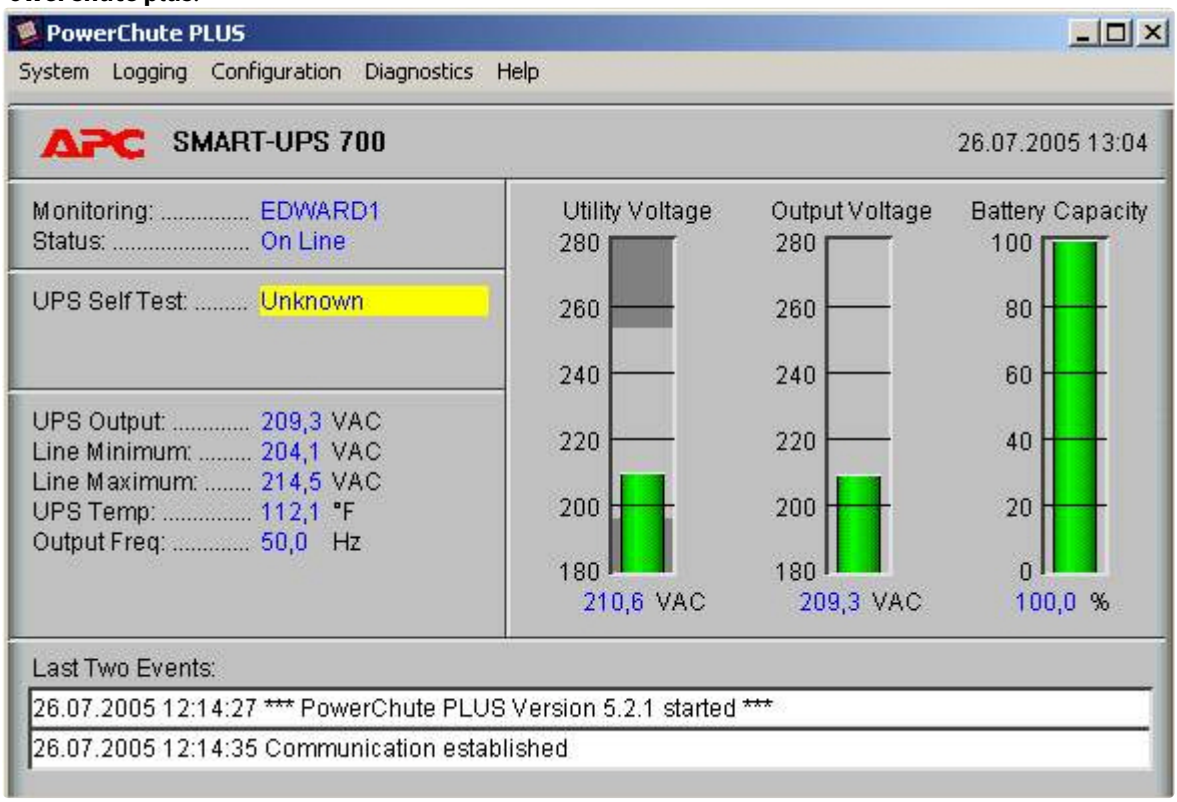
Installation of the StateUPS utility is now complete.

5.4.3 Configuring the PowerChute plus utility

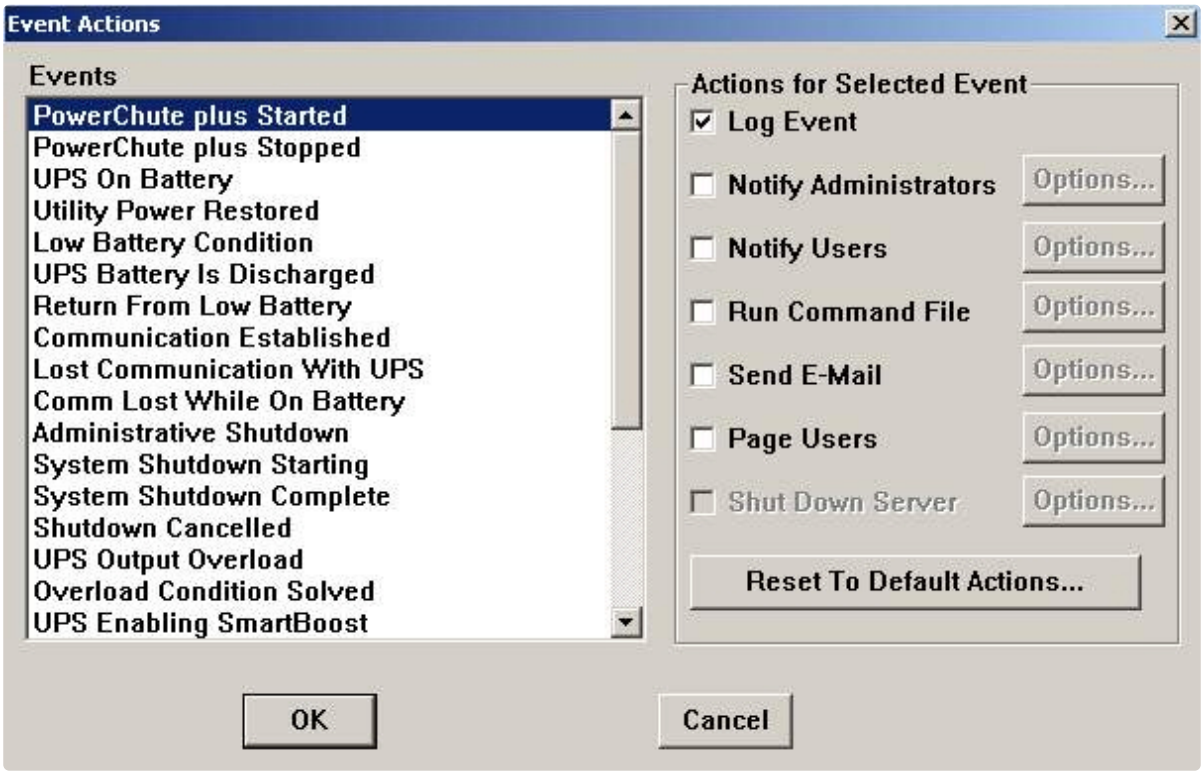
> **Note.**
>
> The PowerChute utility configuring process is given in this document as an example. Alternative software can have different settings.
> Alternative software must allow binding certain reactions with UPS events.

To set up the PowerChute plus utility:

1. Start the PowerChute plus configuration program, by selecting **Start -> Programs** -> **PowerChute plus** -> **PowerChute plus**.



2. Select the menu item **Configuration -> Event Actions...** A dialog box appears, in the left part of which there is a list of events for which different reactions can be assigned (right part of the window). It is recommended to disable the **Notify Users** option for all events unless there is a need for it; otherwise, messages are sent to the entire domain on which the computer is located.



A more detailed list of events is given in the table.

ID Code	Event Name	Description
1000	PowerChute Started	PowerChute service started
1001	PowerChute Stopped	PowerChute service stopped
1002	Communication Established	Communication restored
1003	Utility Power Restored	Electricity restored
1004	UPS Self-Test Passed	Self-Test passed
1005	Administrative Shutdown	Administrative shutdown
1006	Shutdown Cancelled	Shutdown cancelled
1007	Returned From Low Battery	Battey charged
1009	UPS Battery Replaced	Battery replaced

1013	Overload Condition Solved	Overload is back to normal
1014	Runtime Calibration Started	Runtime Calibration Started
1015	Runtime Calibration Finished	Runtime Calibration Finished
1016	System Shutdown Starting	System is shutting down
1102	UPS Internal Temperature In Bounds	Internal temperature is in bounds
2000	UPS On Battery	Electricity turned off
2001	System Shutdown Complete	System performed shutdown
2002	UPS Enabling SmartBoost	Low-voltage mode
2003	Low Battery Condition	Battery is running low
2004	Runtime Calibration Aborted	Runtime Calibration Aborted
2007	UPS Enabling SmartTrim	High-voltage mode
3000	Lost Communication With UPS	Communication lost
3001	UPS Output Overload	Overload
3002	UPS Self-Test Failed	Self-Test failed
3003	UPS Battery Is Discharged	Battery discharged
3004	Comm Lost While On Battery	Comm Lost While On Battery
3016	Battery Needs Replacing	Must replace battery
3107	Maximum Internal Temperature Exceeded	High internal temperature

PowerChute plus can be configured so that any of the events listed previously can be sent to the *Server* of Control.

Events marked in green are highly recommended for sending to *Server of Control*.

The <*Intellect* installation>\Vhost\UPS\Ext\ folder also includes three executables that have been created for specific events:

- PowerOff.exe (electricity is off)

- PowerOn.exe (electricity is restored)
- BatDisch.exe (battery is discharged)

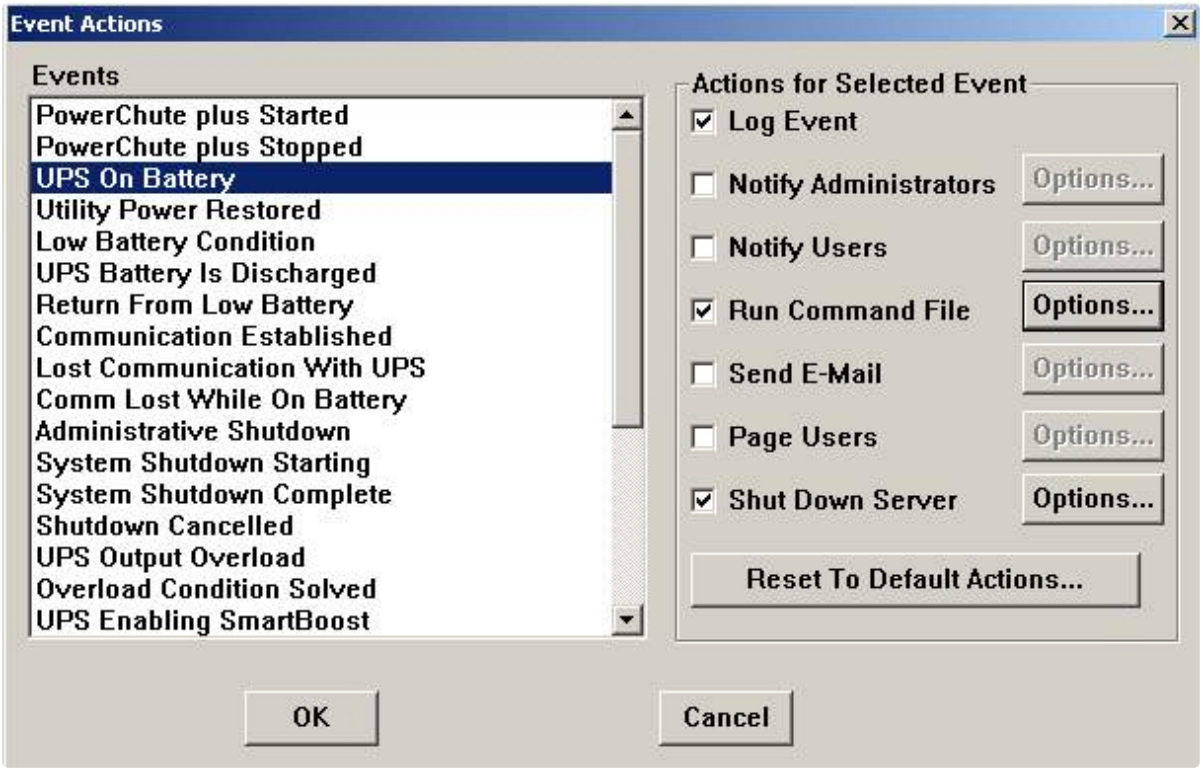
This minimal set can be used with different series of Back-UPS that do not support calling third-party subprograms with the command line.

5.4.4 Example of configuration of event distribution

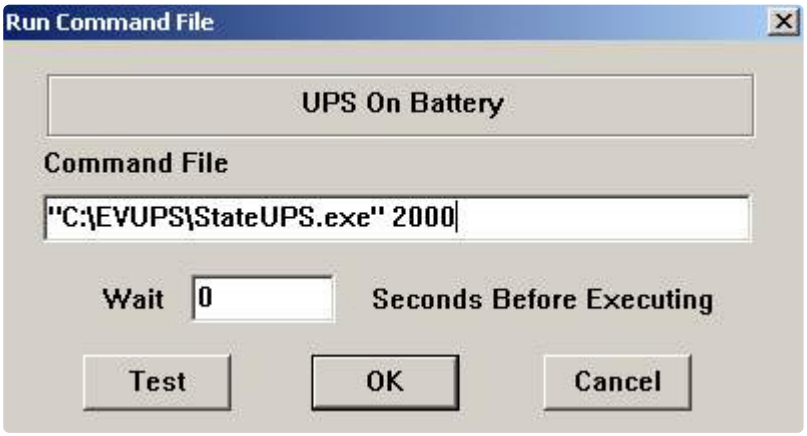
Let us consider the following situation: electricity has turned off and the UPS began to work in battery mode (ID Code = 2000), and after a time electrical supply was restored (ID Code = 1003).

In this case to configure events notifying do the following:

1. In the list of events, select the event **UPS On Battery** and, for this event, select the **Run Command File** check box.

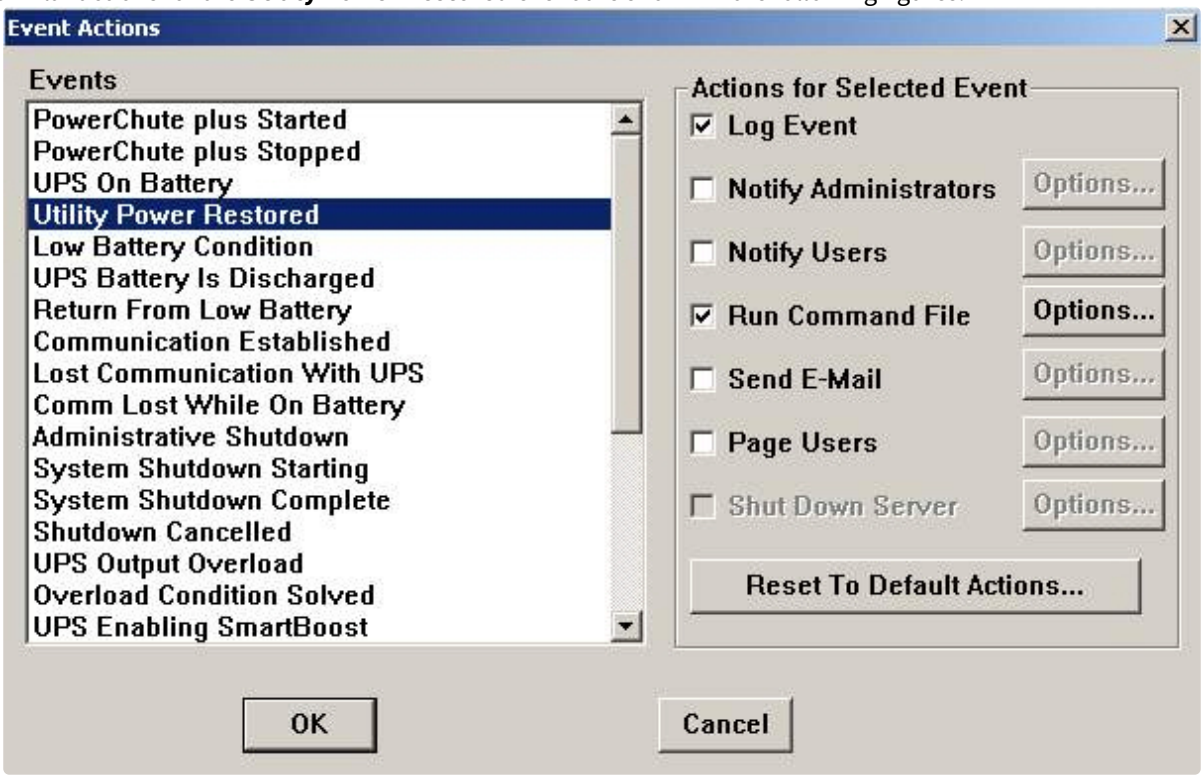


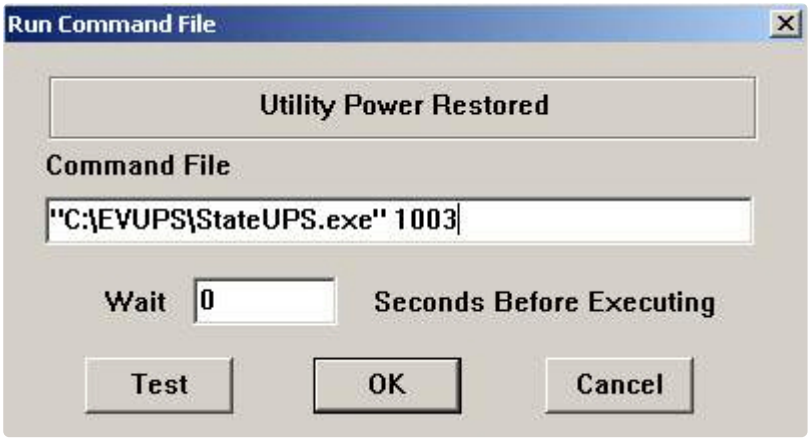
2. To the right of **Run Command File**, click the **Options...** button.
3. In the dialog box that opens, indicate the full path to the StateUPS utility that you want to be started when the event occurs.



This path should be surrounded by double quotation marks (one at the beginning of the path and one at the end). Leave a space and then indicate the ID code; for the **UPS On Battery** event, the ID code is 2000.

4. Similar actions for the **Utility Power Restored** event are shown in the following figures.





You should also remember that after utility power is restored, the UPS does not always generate the **Utility Power Restored** event; sometimes, it generates the **UPS Enabling SmartBoost** or **UPS Enabling SmartTrim** events. In order to not "miss" the moment at which utility power is restored, it is advisable to also handle the **UPS Enabling SmartBoost** and **UPS Enabling SmartTrim** events.

Each time the StateUPS utility is called, a log file is created in the <*Intellect* installation>\Vhost\UPS folder with a name of the following format:

upslog_<state><*date*><time>.log

5.5 Working with Agent of Control without Windows administration rights

To allow the user not added to the Administrators group in the Windows operating system to work correctly with *Agent of Control*, make sure the following conditions are fulfilled:

1. The user must have full access to the *Agent of Control* registry section: HKEY_LOCAL_MACHINE\Software\BitSoft for 32-bit system (HKEY_LOCAL_MACHINE\Software\Wow6432Node\BitSoft for 64-bit).
2. The user must have full rights for the folder <DISK>:\Backup, where <DISK> is the logical disc where Intellect software is installed.

6 Configuring Server of Control

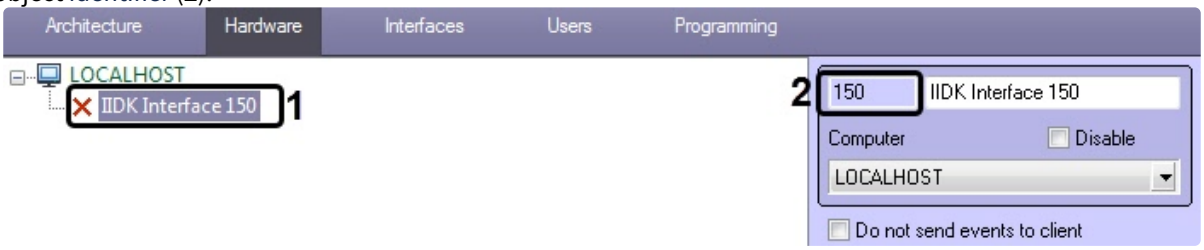
To configure *Server of Control*, go to the **System settings** window. Use of this window is described in Intellect Software Package: Administrator's Guide.

6.1 Creating necessary Server Of Control objects

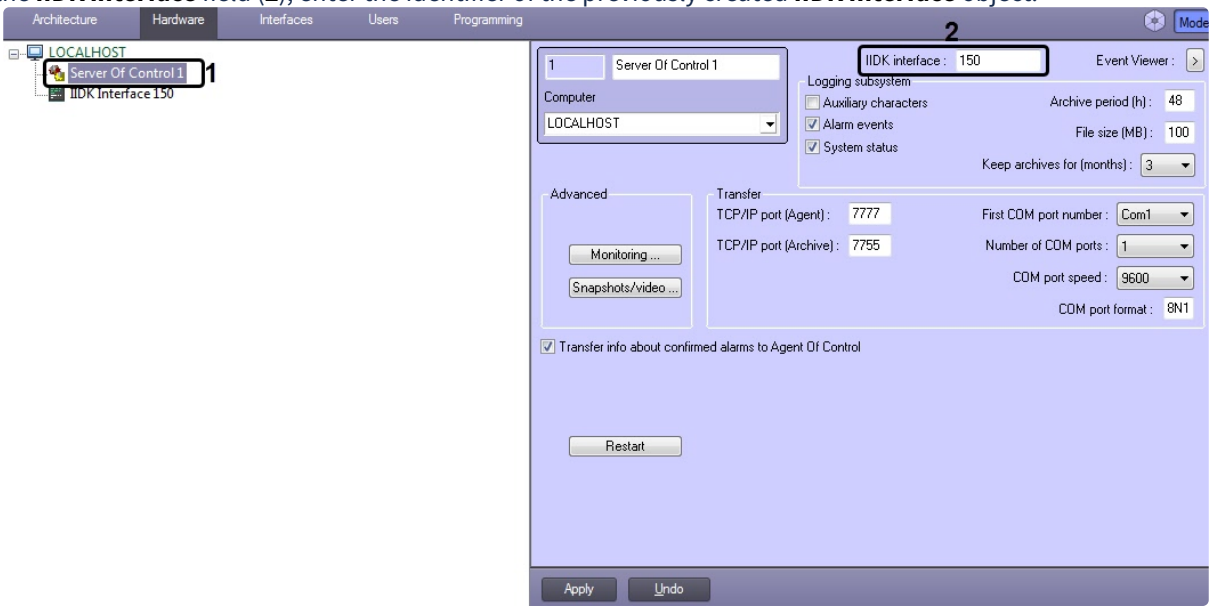
> **Note**
>
> *Agent Of Control*, like *Server Of Control*, can operate in a distributed configuration, while *Agents Of Control*, *Servers Of Control* and *Central Servers Of Control* can see where each of them is installed and can be configured.

To create necessary *Server Of Control* objects, do the following:

1. Go to **Hardware** tab in the **System settings** dialog box.
2. Create an **IIDK interface** object on the basis of the **Computer** object (**1**). Set the **IIDK Interface** object identifier (**2**).

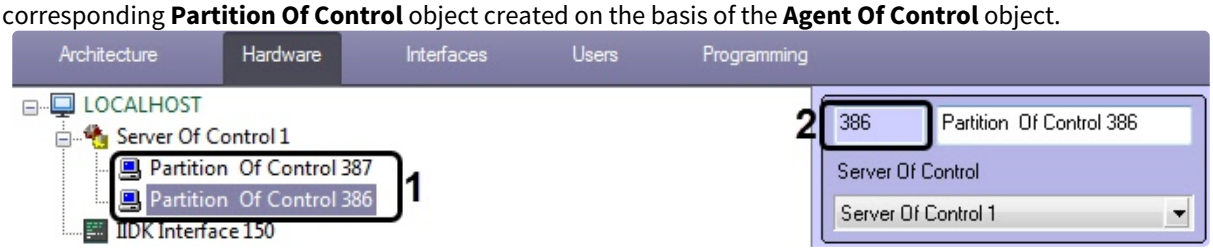


3. Create a **Server Of Control** object on the basis of a **Computer** object. On the settings panel of this object, in the **IIDK interface** field (**2**), enter the identifier of the previously created **IIDK Interface** object.



4. Create the required number of **Partition Of Control** child objects on the basis of the **Server Of Control** object. When you create these objects, specify the same ID (**2**) as in the **ID** field on the settings panel of the

corresponding **Partition Of Control** object created on the basis of the **Agent Of Control** object.



> **Note**
>
> It is not necessary to manually create the **Partition Of Control** objects on the basis of the **Server Of Control** object. They will be created automatically upon successful configuration of the communication between the *Agent Of Control* and the *Server Of Control* with the name and identifier specified on the *Agent Of Control* side (see Configuring communication between Agent Of Control and Server Of Control).

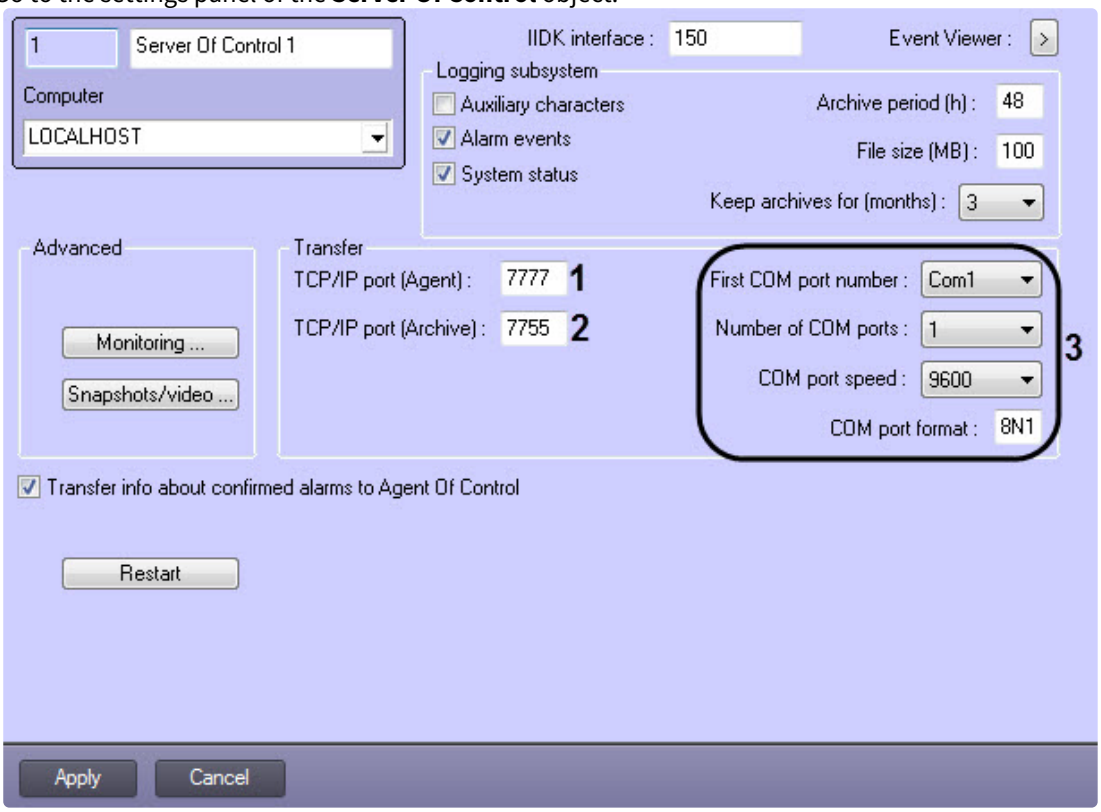
The required objects are now created.

6.2 Configuring a connection

A *Server Of Control* can simultaneously operate with objects over both the TCP/IP and RS232 protocols.

To configure a connection between *Server Of Control* and *Agent Of Control*/Archive, do the following:

1. Go to the settings panel of the **Server Of Control** object.



2. In the **TCP/IP port (Agent)** field, enter the port number for TCP/IP communication with remote objects (**1**).
3. In the **TCP/IP port (Archive)** field, enter the port number for TCP/IP communication with the *Search in archive* module (**2**).

> **Note**
>
> The default value of the **TCP/IP port (Archive)** is **7755**. After you change the port number, it is necessary to also change the **IPPort** registry key value to the new port number (for details, see Registry keys reference guide. For more information about working with the registry, see Working with Windows OS registry).

4. For the RS232 protocol, configure the following parameters: **First COM port number, Number of COM ports, COM port speed,** and **COM port format** (**3**).
5. Click the **Apply** button.

Configuring a connection is complete.

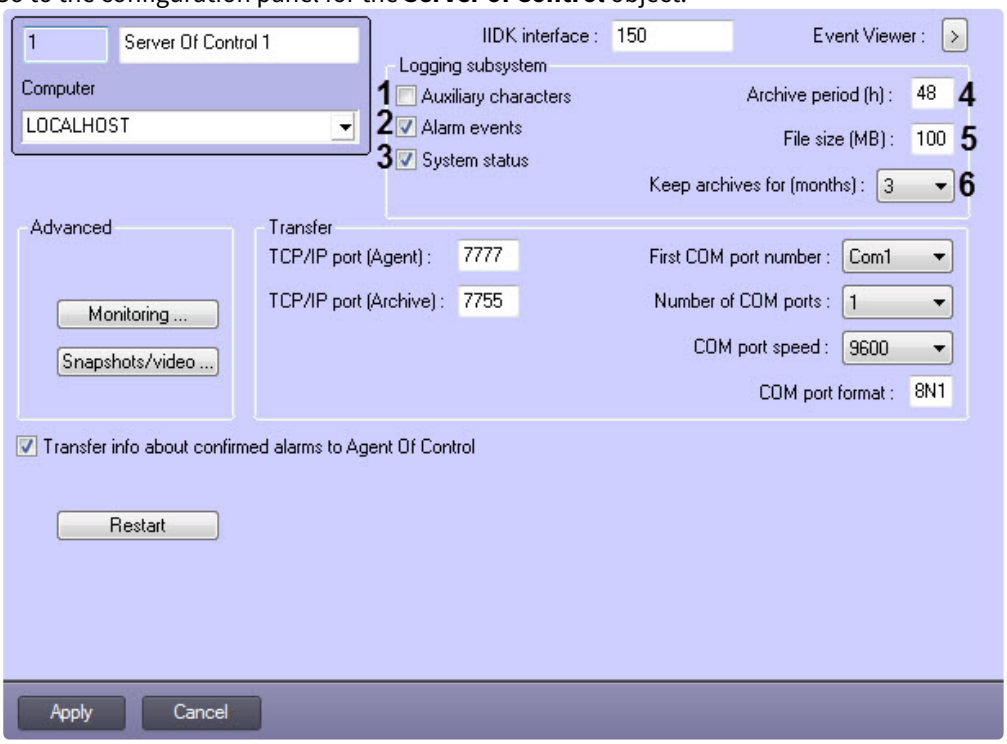
6.3 Configuring logging subsystem

The logging subsystem allows configuring the detail level at which *Server of Control* activities are logged.

The main log file is located in the <*Intellect* software installation folder>\VHost folder, in the file vsrvYYMMDD.log, where YY is the year, MM the month, and DD the day.

To configure the logging subsystem:

1. Go to the configuration panel for the **Server of Control** object.



2. To log auxiliary characters at the transport level, select the **Auxiliary characters** check box (**1**).
3. To log alarms (activation of a vibration sensor, temperature sensor, or Door-Forced-Open (DFO) sensor), select the **Alarm events** check box (**2**).
4. To log events related to system status, select the **System status** check box (**3**).
5. In the **Archive period (h)** field, enter the frequency, in hours, at which the log file is to be archived (**4**). Archives are saved in the DATA subfolder, with the following name format: namelog_yymmddhhmmss.gz, where
   a. namelog is the name of the log file being archived;

b. yy is the year of archive creation;
c. mm is the month of archive creation;
d. dd is the day of archive creation;
e. hh is the hour of archive creation;
f. mm is the minute of archive creation;
g. ss is the second of archive creation.

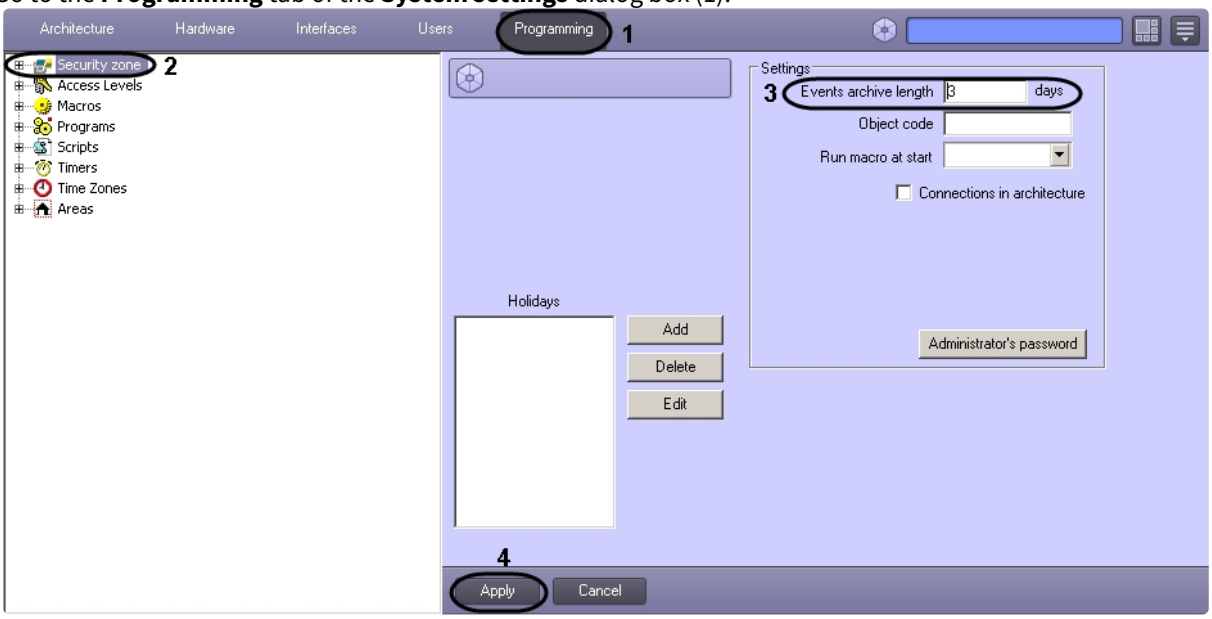
6. In the **File size (MB)** field, enter the file size threshold, in megabytes, upon which the log file is archived (**5**). This setting overrides the value in the **Archive period (h)** field.
7. In the **Keep archives for (months)** drop-down list, select the length of time, in months, for which you want to store archived log files. This value must be between 1 and 24 (**6**). Archives that are older than the specified number of months are deleted.

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

6.3.1 Specifying storage time for event log

To specify the term of keeping the event log in the database do the following:

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



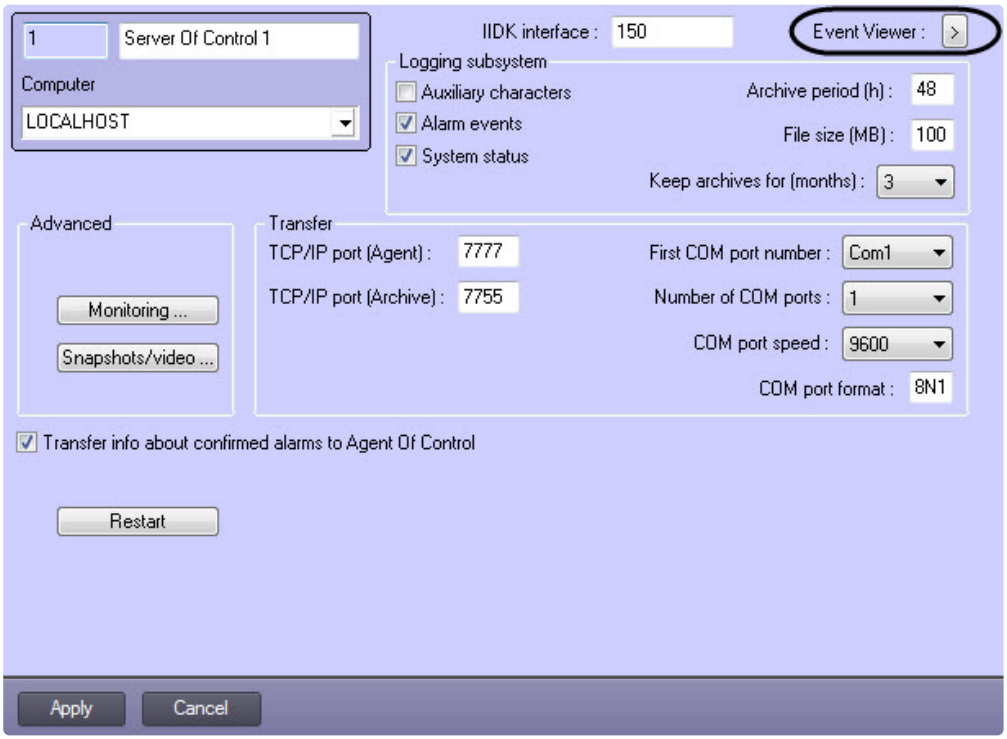
2. Go to the **Security zone** object setting panel (2).
3. Specify the term of keeping the event log in the **Event archive length** parameter (3).
4. Press **Apply** (4).

Specifying the term of keeping the event log is completed.

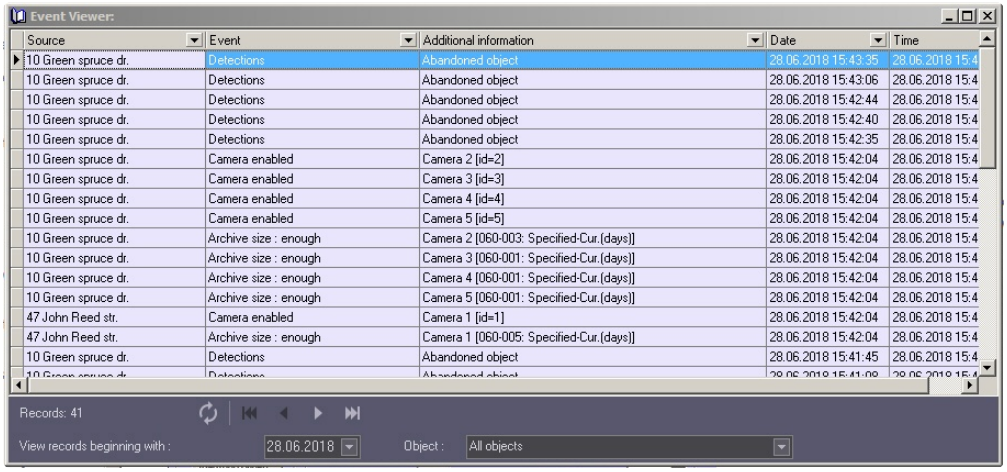
6.3.2 The Event Viewer utility

The disadvantage of viewing information via the *Event Viewer* is clearing the screen on each Intellect restart. It is impossible to see what was on before the system restart. The additional *Event Viewer* utility is required in such cases. This utility operates the database directly and allows to view information from the whole length of time used to keep the event log in the database.

To start the *Event Viewer* utility, click the **Event Viewer** button on the **Server of Control** settings panel.



The *Event Viewer* utility allows to sort and filter data.

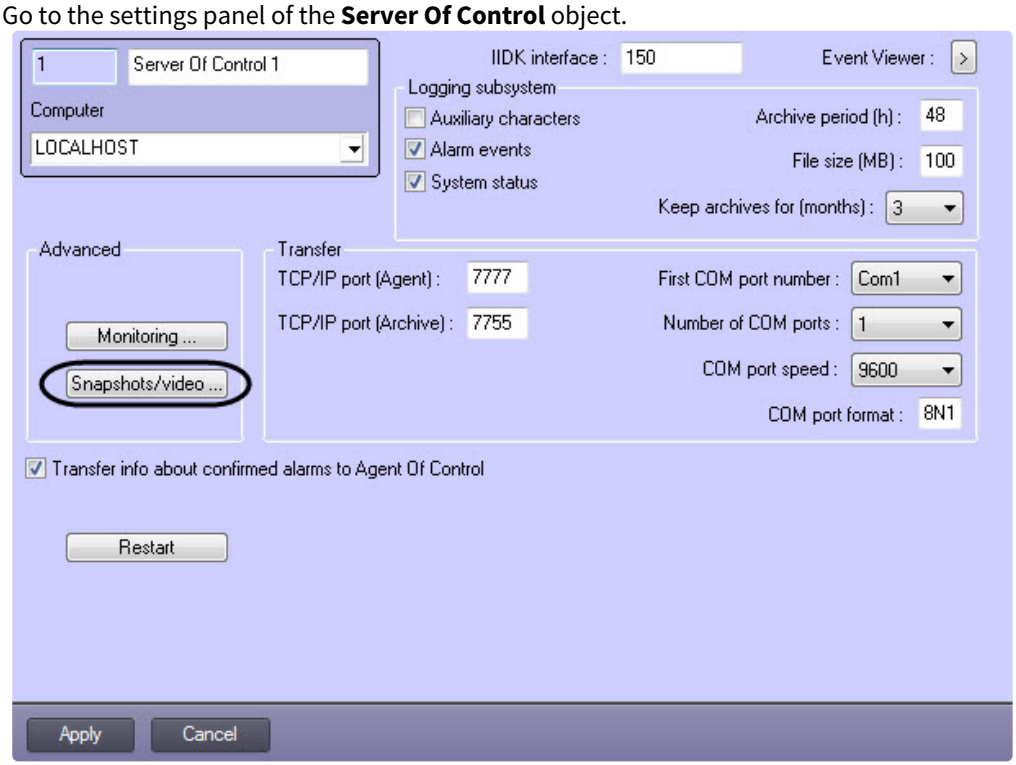


6.4 Configuring reaction to snapshots and videos

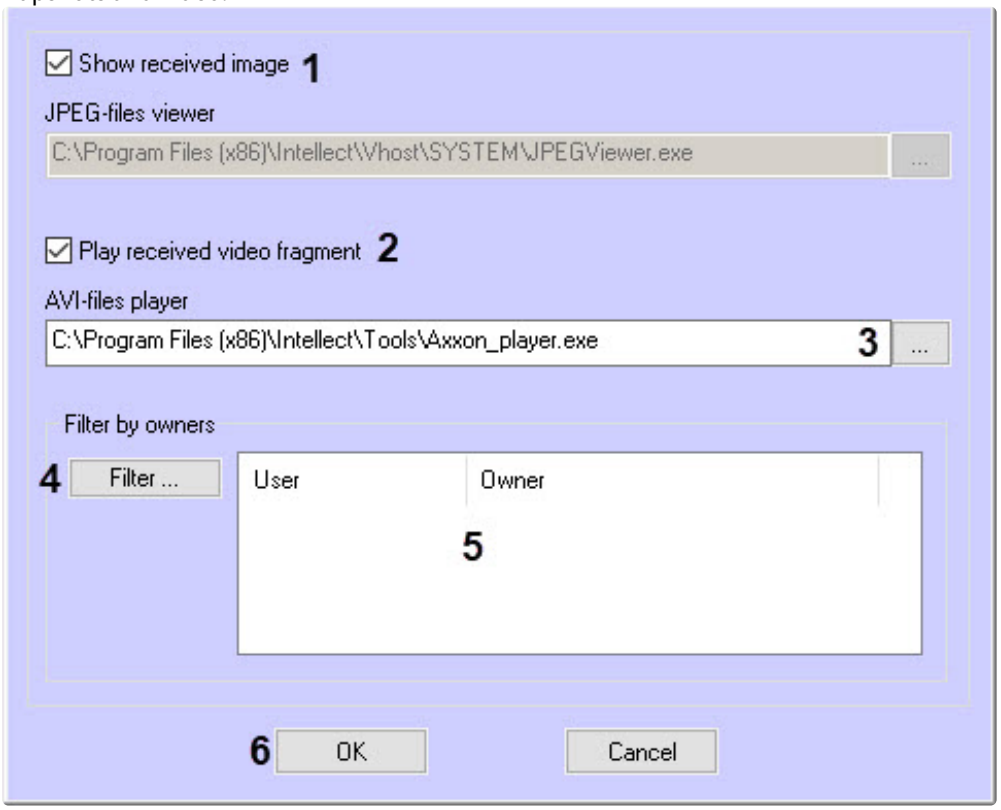
To configure the visualization of video frames and video fragments that are received with alarms (see Viewing video data on alarms), it is necessary to do the following:

> **Note**
>
> This setting doesn't affect the acquisition of video data by the **Search in archive** interface object, except for the **AVI-files player** parameter (see Request for video clips from objects).

1. Go to the settings panel of the **Server Of Control** object.

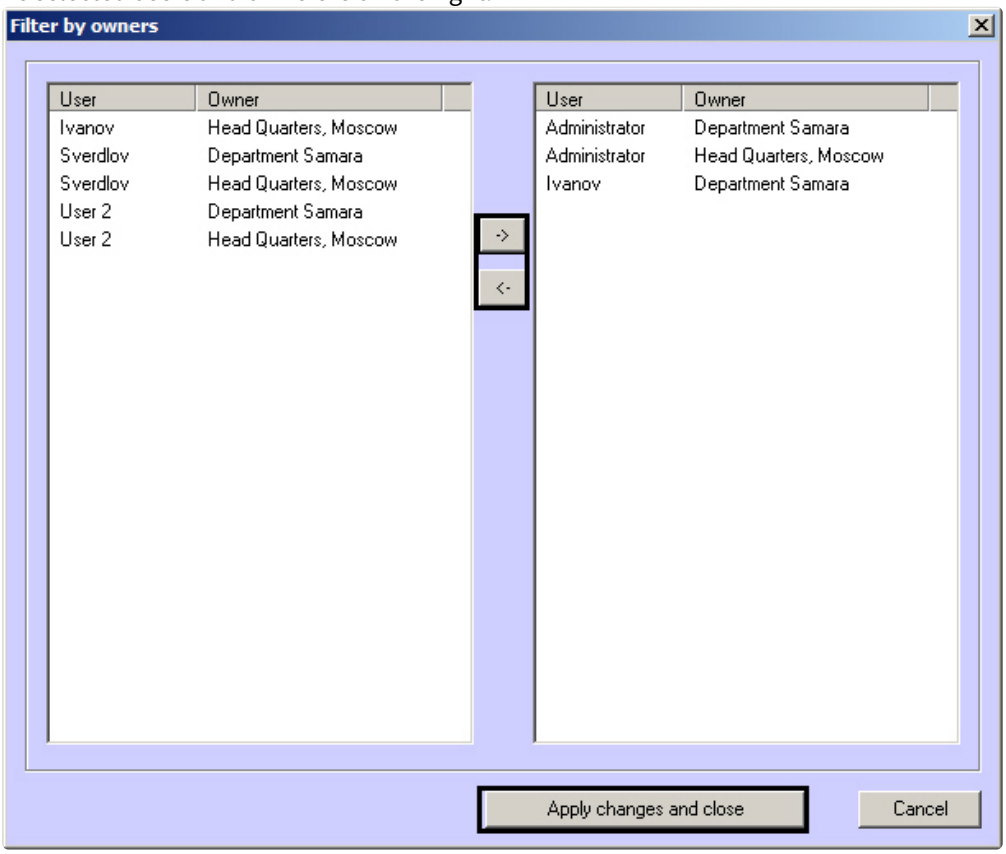


2. Click the **Snapshot/video** button. A window will open where you can configure reactions to receiving snapshots and video.



3. If you want to open the received image:
   a. Set the **Show received image** checkbox (**1**).

4. If you want to playback the received clip:
    a. Set the **Playback received video fragment** checkbox (**2**).
    b. In the **AVI-files player** field, specify the path to the program used to playback the AVI files (**3**).
5. If you want certain users to have access only to snapshots and video fragments received from the objects belonging to specific owners, set a filter by owners:
    a. Click the **Filter** button (**4**).
    b. The **Filter by owners** window will open. The list of available user-owner pairs is on the left, the list of the selected users and owners is on the right.



> **Note**
>
> The list of owners is set on the Control Panel (see Regulatory and reference information). Users and their rights are configured in the **Users** tab of the **System settings** dialog box (see *Intellect. Administrator's Guide*. The latest version of this document is available in AxxonSoft documentation repository).

    c. Move the pairs between the lists using the <- and -> buttons.
    d. When the list of users and owners is formed, click the **Apply changes and close** button.
6. Selected pairs of users and owners will be displayed in the table (**5**).
7. Click the **OK** button (**6**).

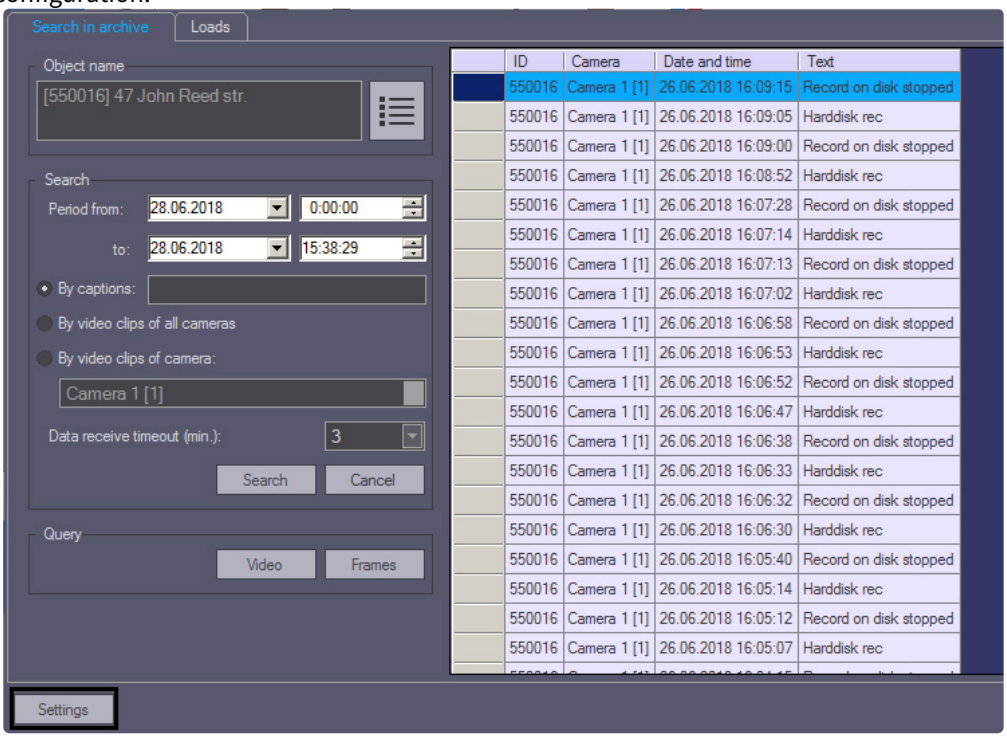
Configuring reactions to receiving snapshots and video fragments is now complete.

6.5 List of Additional workplaces

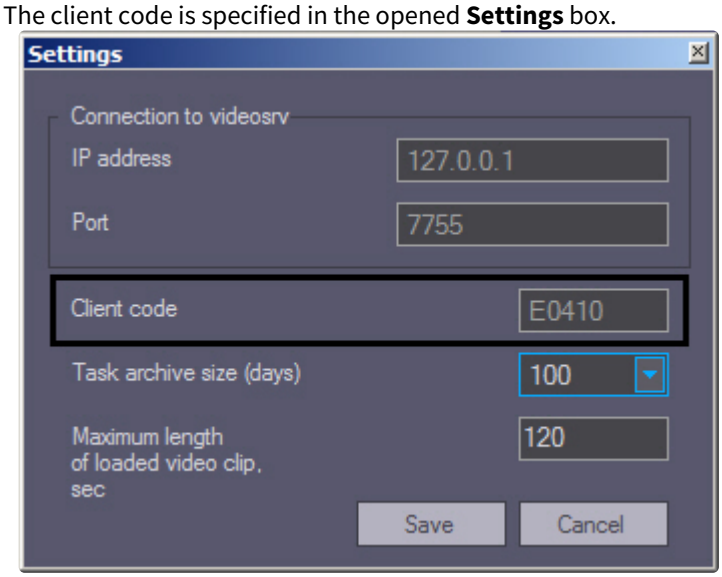
For the *Additional workplaces* software operation, it is necessary to configure the list of additional workplaces on the *Server Of Control*, and specify the computer name and the client code for each of them.

The client code is bound to the computer hardware. You can find it out as follows:

1. On the computer with installed *Monitoring*, open the **Search in archive** interface in the Additional workplace configuration.

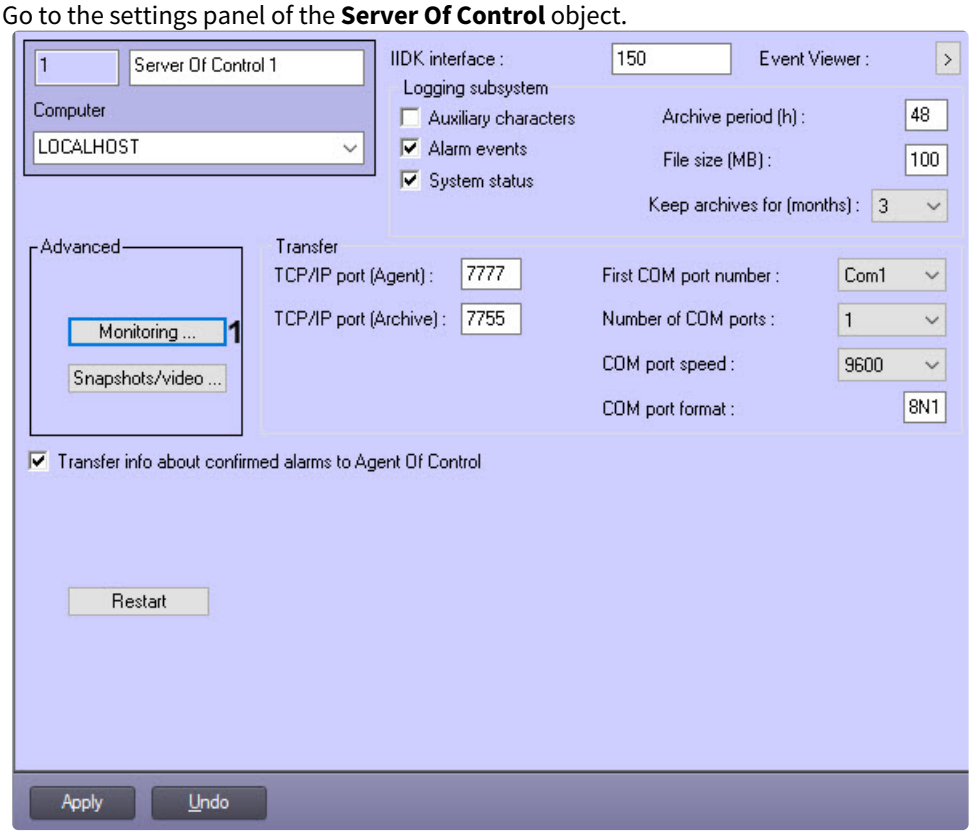


2. Click the **Settings** button in the bottom left corner.
3. The client code is specified in the opened **Settings** box.

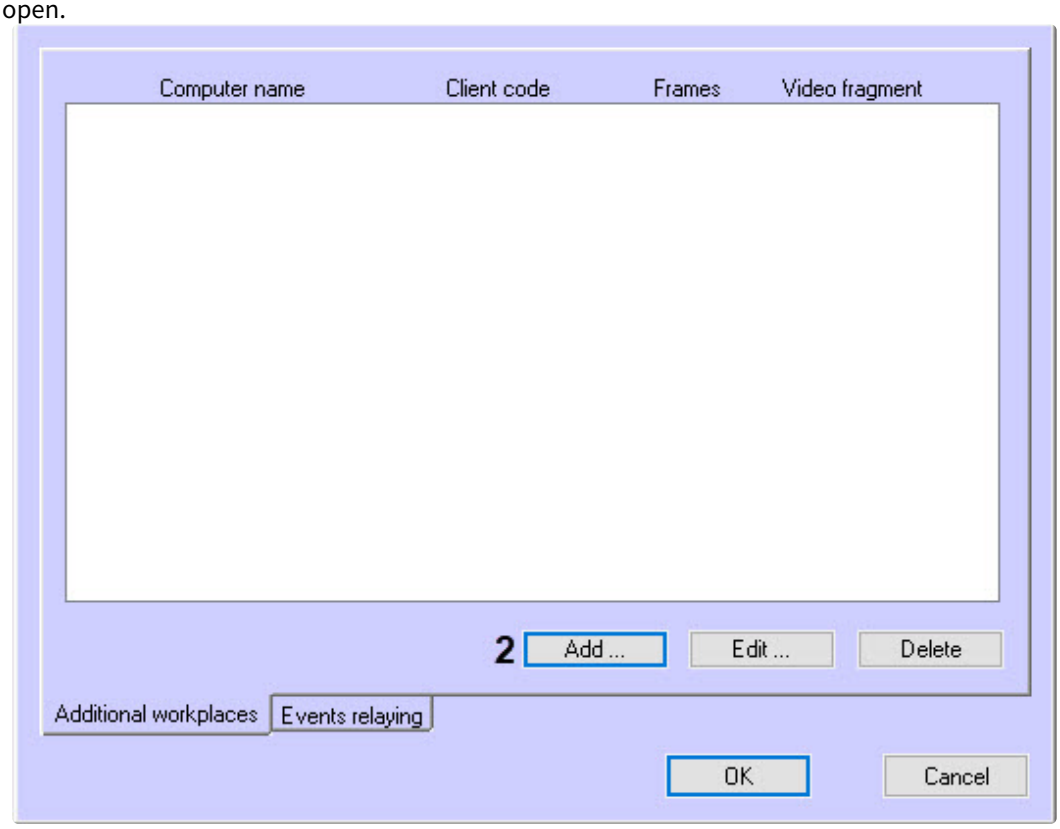


The list of Additional workplaces that can be connected to the *Server Of Control* is configured as follows:

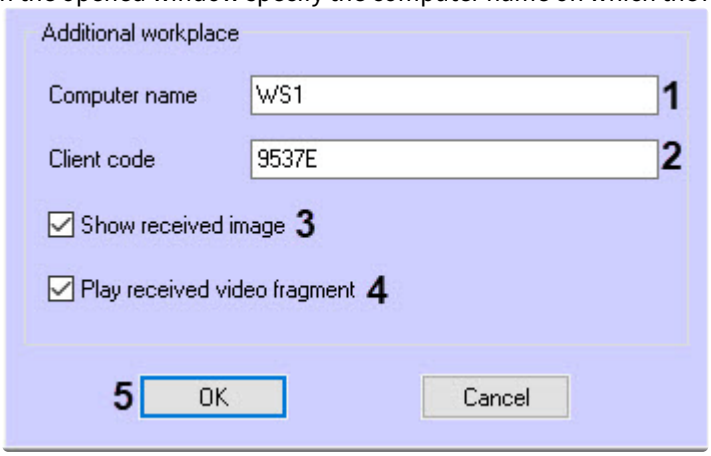
1. Go to the settings panel of the **Server Of Control** object.



2. Click the **Monitoring** button (**1**). As a result, the window for configuring the list of Additional workplaces will open.



3. To add an Additional workplace to the list, click the **Add** button (**2**).
4. In the opened window specify the computer name on which the Additional workplace is installed (**1**).



5. In the **Client code** field (**2**), enter the client code.
   To configure the visualization of video frames and video fragments that are received with alarms (see Viewing video data on alarms), it is necessary to do the following;

   > **Note**
   >
   > This setting doesn't affect the acquisition of video data by the **Search in archive** interface object (see Request for video clips from objects).

6. Set the **Show received image** checkbox (**3**) if you want to open the received video frames. The **Filter by owners** setting is taken into account (see Configuring reaction to snapshots and videos).
7. Set the **Play received video fragment** checkbox (**4**) if you want to playback the received video fragments. The **Filter by owners** setting is taken into account (see Configuring reaction to snapshots and videos).
8. Click the **OK** button (**5**).
9. Repeat steps 3-8 for all Additional workplaces that will be connected to this *Server Of Control*.

   > **Note**
   >
   > To edit the specified settings, select the Additional workplace in the list and click the **Edit** button.
   > To delete the Additional workplace in the list, select it in the list and click the **Delete** button.

10. Click the **OK** button.
11. Click the **Apply** button.

The list of Additional workplaces is now configured.

6.6 Sending confirmations of alarm acceptance

In general, the *Agent Of Control* is considered not to have the same core as the *Server Of Control*.

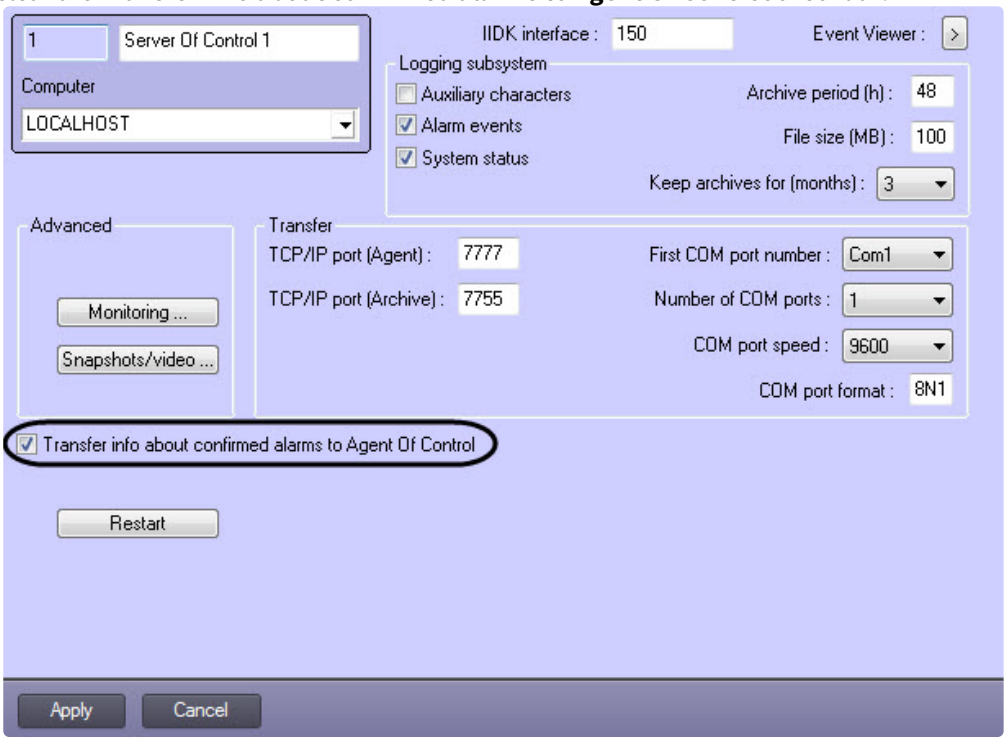
It is possible to configure sending messages to *Agent Of Control* when the operator confirms an alarm on the *Server Of Control*. The *Agent Of Control* then sends these messages to *Intellect* core. Two types of confirmation are available: simple and complex. The confirmation type is selected when configuring alarm transmission to the *Server Of Control* (see Configuration for associating events with certain alarm groups).

When the confirmation is sent, the *Server Of Control* waits for the confirmation from the *Agent Of Control* that the message has been sent to *Intellect* core. If this message is not received, then confirmation packets are sent every 5 minutes.

> **Note**
>
> See also Sample scripts for processing alarm confirmations.

Disable sending confirmations of alarm acceptance as follows:

1. Go to the settings panel of the **Server Of Control** object.
2. Clear the **Transfer info about confirmed alarms to Agent Of Control** checkbox.



3. Click the **Apply** button.

The **Transfer info about confirmed alarms to Agent Of Control** function is now disabled.

6.7 Working with Server of Control without Windows administration rights

To allow the user not added to the Administrators group in the Windows operating system to work correctly with *Server of Control*, make sure the following conditions are fulfilled:

1. The user must be given full access to the registry key:
   - For a 32-bit system: HKEY_LOCAL_MACHINE\Software\BitSoft
   - For a 64-bit system: HKEY_LOCAL_MACHINE\Software\Wow6432Node\BitSoft
2. The user must be granted full rights to the export directory (see Specifying the export directory).

6.8 Configuring sound notification at Server of Control

6.8.1 Configuring sound notification at Server Of Control in a general way

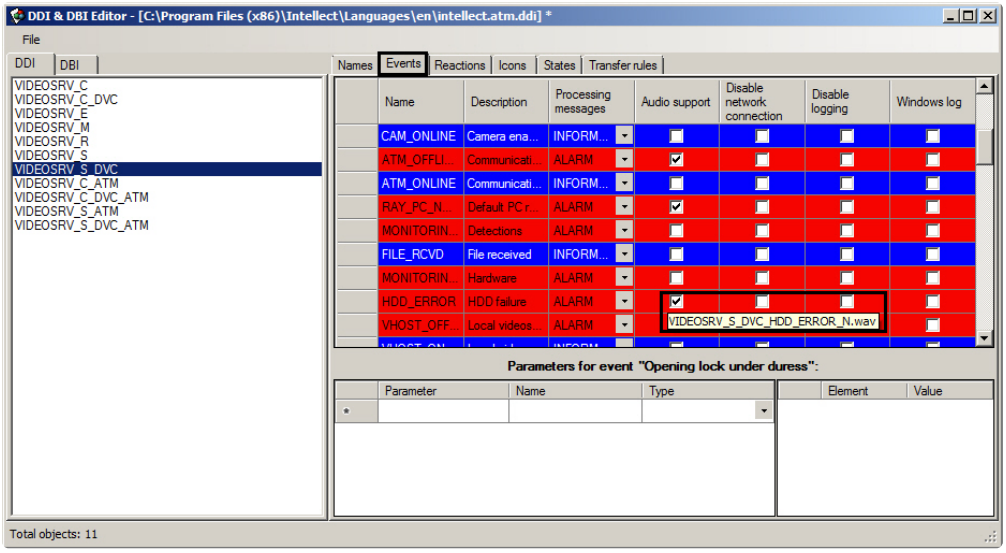
Monitoring allows configuring audio signal that accompanies alarm messages received from *Agents Of Control*. For this, do the following:

> **Note**
>
> This function is not supported for the *Additional Workstation* in non-distributed configuration.

1. Create a **Display** object in the **Interfaces** tab.
2. Create an **Audio player** object on the basis of the **Display** object.
3. Run the *System configuration* utility (ddi.exe).

> **Note**
>
> Detailed information on using this utility is given in the *Intellect software. Administrator's Guide*. The most relevant version of this document is available in AxxonSoft documentation repository.

4. Open the intellect.atm.ddi file.
5. Select the VIDEOSRV_S_DVC (**Partition Of control**) object.
6. Go to the **Events** tab.



7. In the **Audio support** column, set the checkboxes next to all events that have to be accompanied by an audio signal.
   A tooltip shows the required name of the WAV file.
   N is an ID of the VIDEOSRV_S_DVC_ATM object.
8. Create corresponding files and place them into the <*Intellect* installation>\Wav folder.

Configuration of sound notification at *Server Of Control* is completed.

6.8.2 Configuring sound notification at Server Of Control for various alarm groups

There are four alarm groups in *Monitoring*. Several different events can be assigned to them at the *Agent Of Control*. These groups are: **Equipment, ACS, FSA, Detections** (see Configuration for associating events with certain alarm groups).

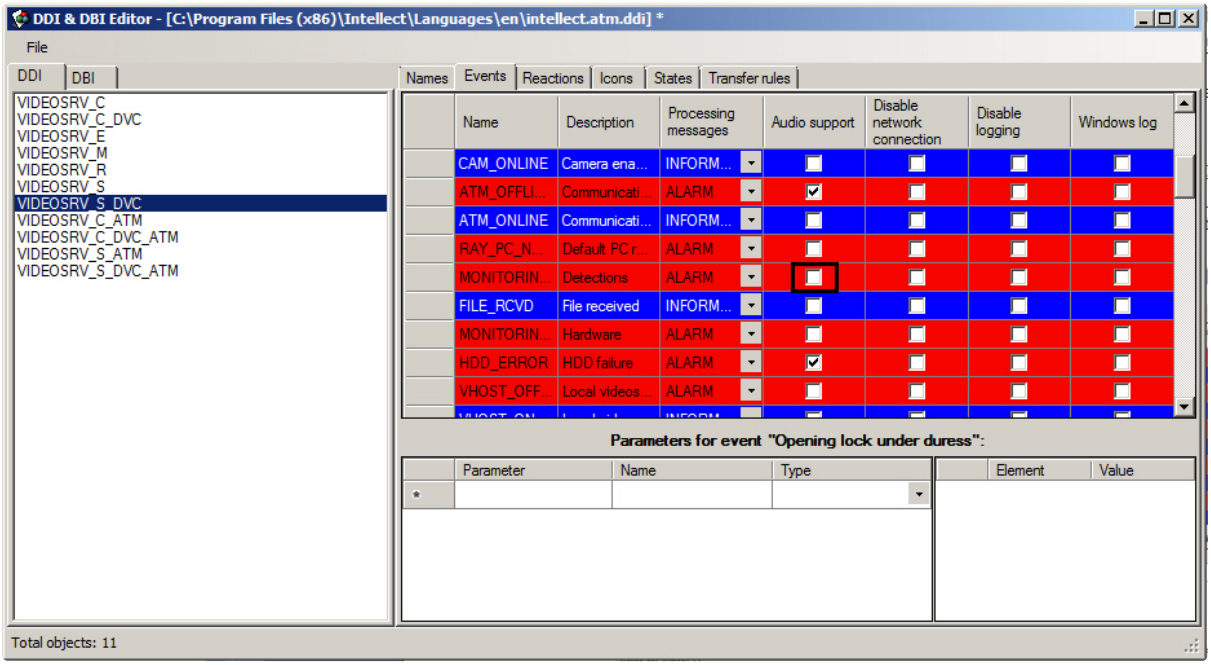
In order to configure sound notification for alarm groups, do the following:

> **Note**
>
> This function is not supported for the *Additional Workstation* in non-distributed configuration.

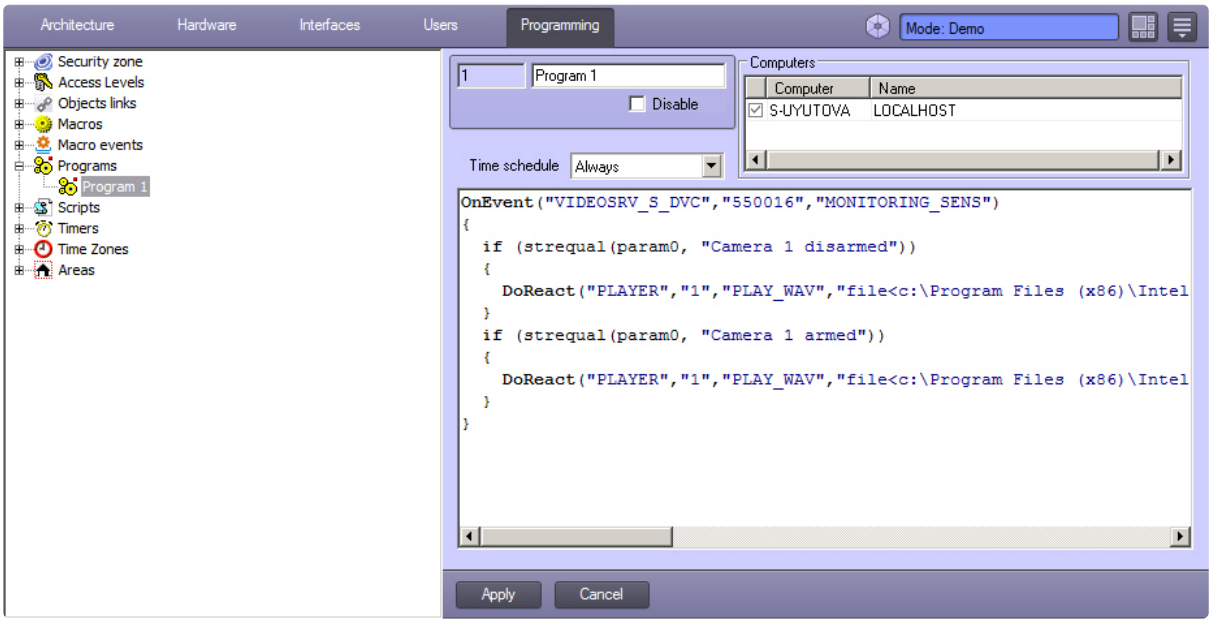
1. Create and configure the **Display** and **Audio player** objects in the **Interfaces** tab of the **System settings** dialog box.
2. Run the *System configuration* utility (ddi.exe).

> **Note**
>
> Detailed information on using this utility is given in the *Intellect software. Administrator's Guide*. The most relevant version of this document is available in AxxonSoft documentation repository.

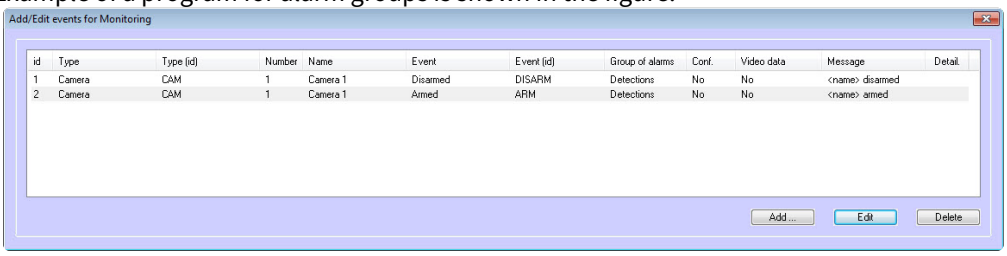
3. Open the intellect.atm.ddi file, select the VIDEOSRV_S_DVC (**Partition Of control**) object.
4. Go to the **Events** tab.



5. Make sure that the **Audio support** is not set for the **Detections** event.
6. Close the *System configuration* utility.
7. Create and configure the **Program** object in the **Programming** tab of the **System settings** dialog box.



Example of a program for alarm groups is shown in the figure:




```
OnEvent("VIDEOSRV_S_DVC","550016","MONITORING_SENS")
{
  if (strequal(param0, "Camera 1 disarmed"))
  {
    DoReact("PLAYER","1","PLAY_WAV","file<c:\Program Files
(x86)\Intellect\Wav\cam_disarm.wav>");
  }
  if (strequal(param0, "Camera 1 armed"))
  {
    DoReact("PLAYER","1","PLAY_WAV","file<c:\Program Files
(x86)\Intellect\Wav\cam_arm.wav>");
  }
}
```

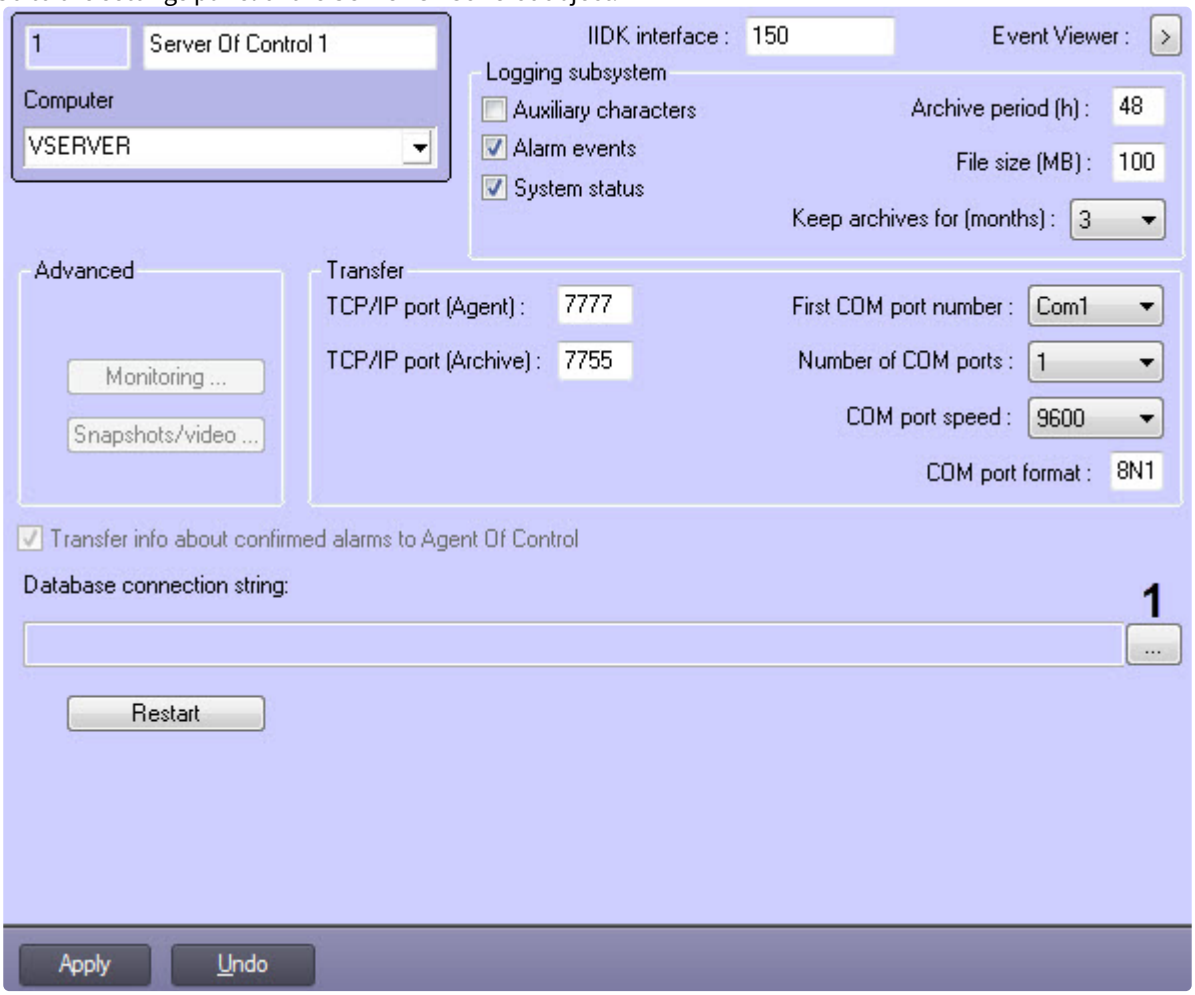
8. Create the corresponding files and place them into the <*Intellect* installation>\Wav folder.

Configuration of sound notification at *Server Of Control* for various alarm groups is completed.

6.9 Configuring the Server of Control from another server in a distributed configuration

To configure the *Server of Control* from another server in a distributed configuration, do the following:

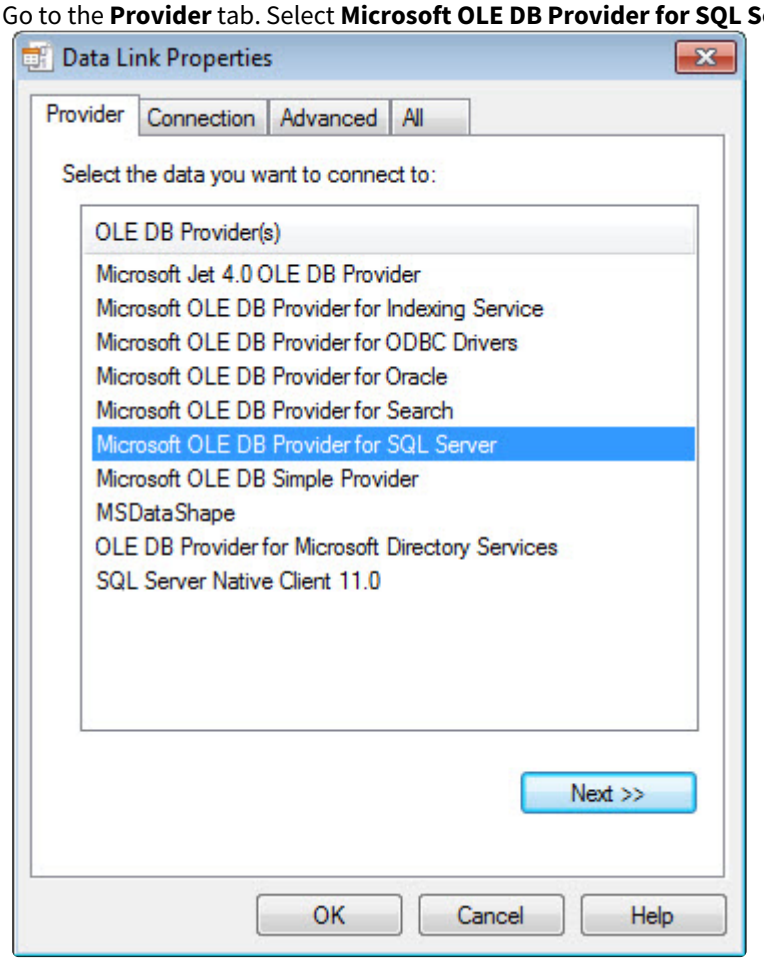
1. Go to the settings panel of the **Server Of Control** object.



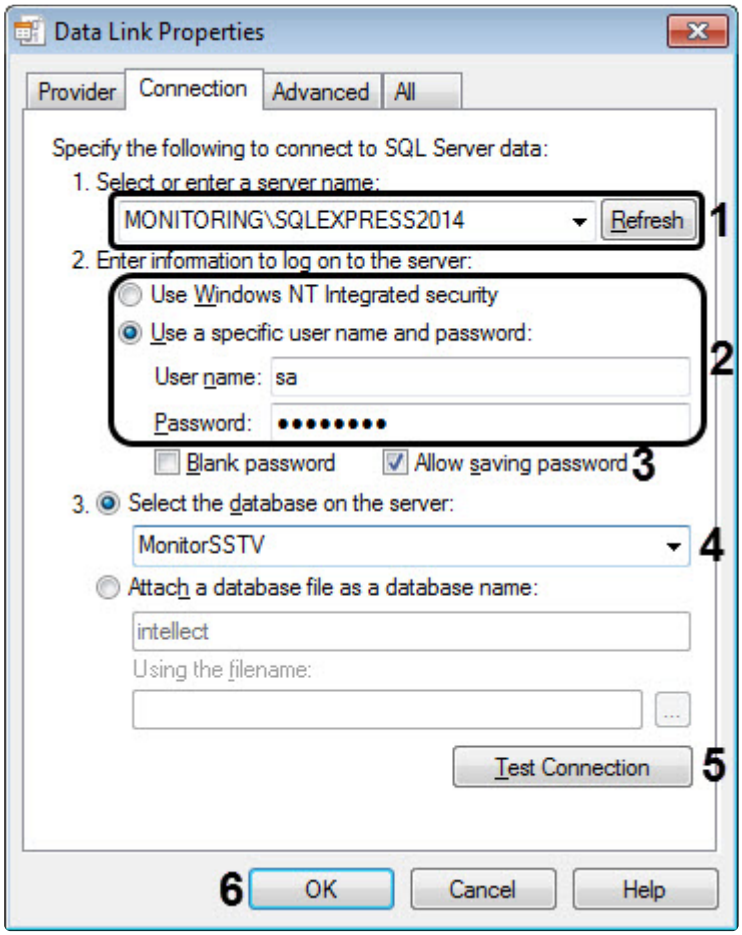
2. Click the ... button (**1**). The **Data Link Properties** window opens. Configure the connection to the remote *Server of Control* database as follows:

> **Note**
>
> The **Database connection string** parameter is displayed only if the *Server of Control* is configured from another server in a distributed configuration.

a. Go to the **Provider** tab. Select **Microsoft OLE DB Provider for SQL Server**.

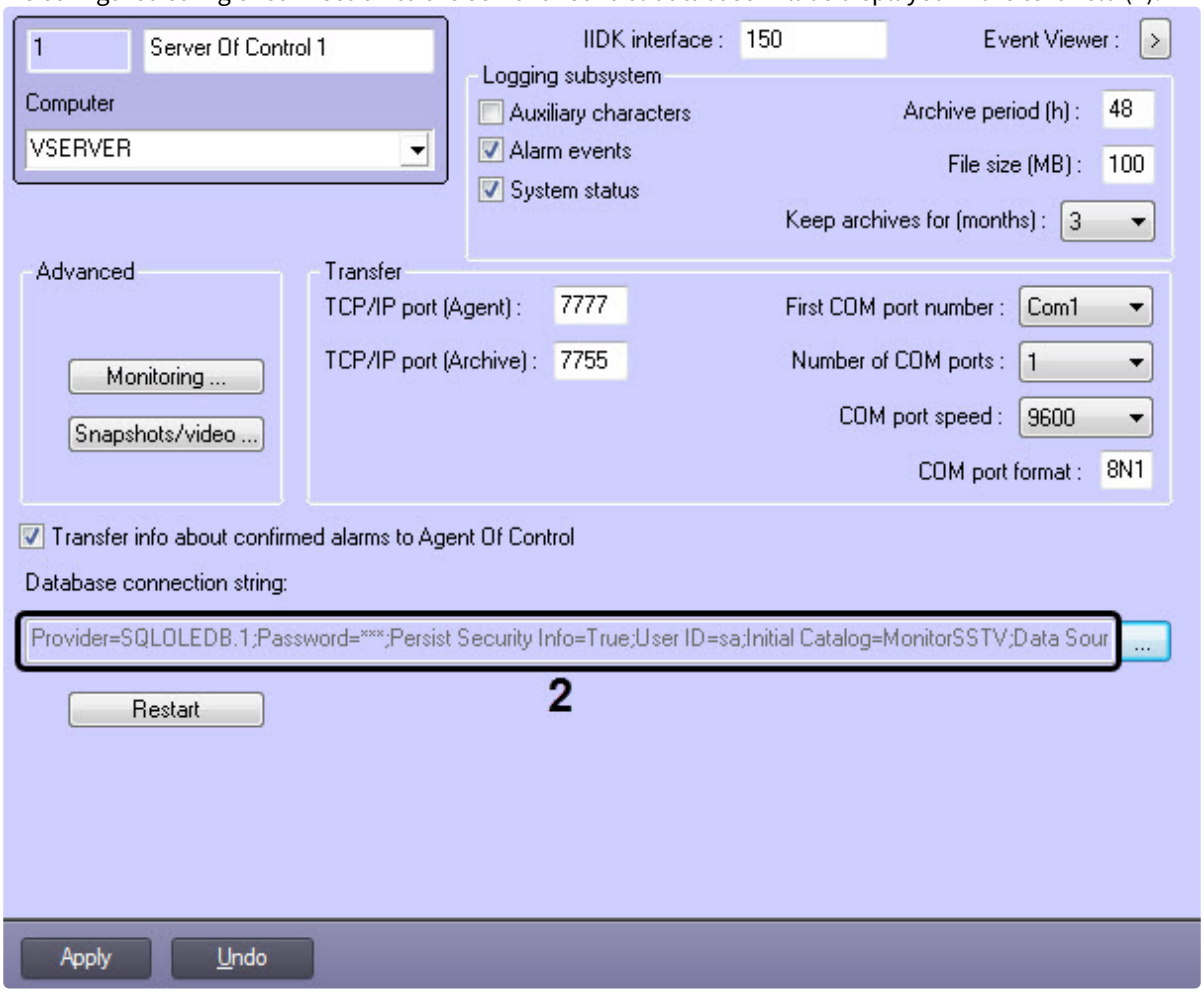


b. Go to the **Connection** tab. From the **1. Select or enter a server name** drop-down list, select the name of the database server that stores the *Server of Control* database (**1**).



c. Set the **2. Enter information to log on to the server** switch to the **Use a specific user name and password** position and enter the name and password to connect to the MS SQL Server (**2**).
d. Set the **Allow saving password** checkbox (**3**).
e. From the **Select the database on the server** drop-down list, select the name of the *Server of Control* database (MonitorSSTV by default) (**4**).
f. Click the **Test Connection** button (**5**). If the connection data is correct, a window with the message "Connection check completed" will be displayed.
g. Click **OK** (**6**).

3. The configured string of connection to the *Server of Control* database will be displayed in the text field (**2**).



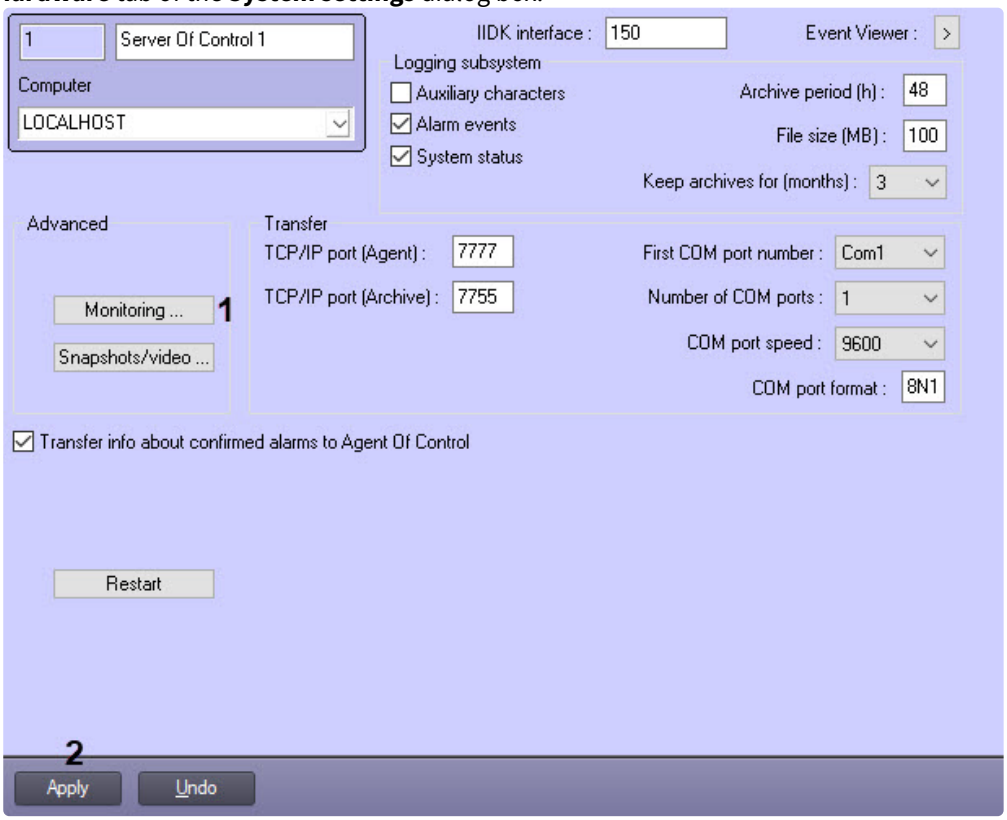
4. As a result, you can start configuring the *Server of Control* (see Configuring Server of Control).

Configuring the *Server of Control* from another server in a distributed configuration is now complete.

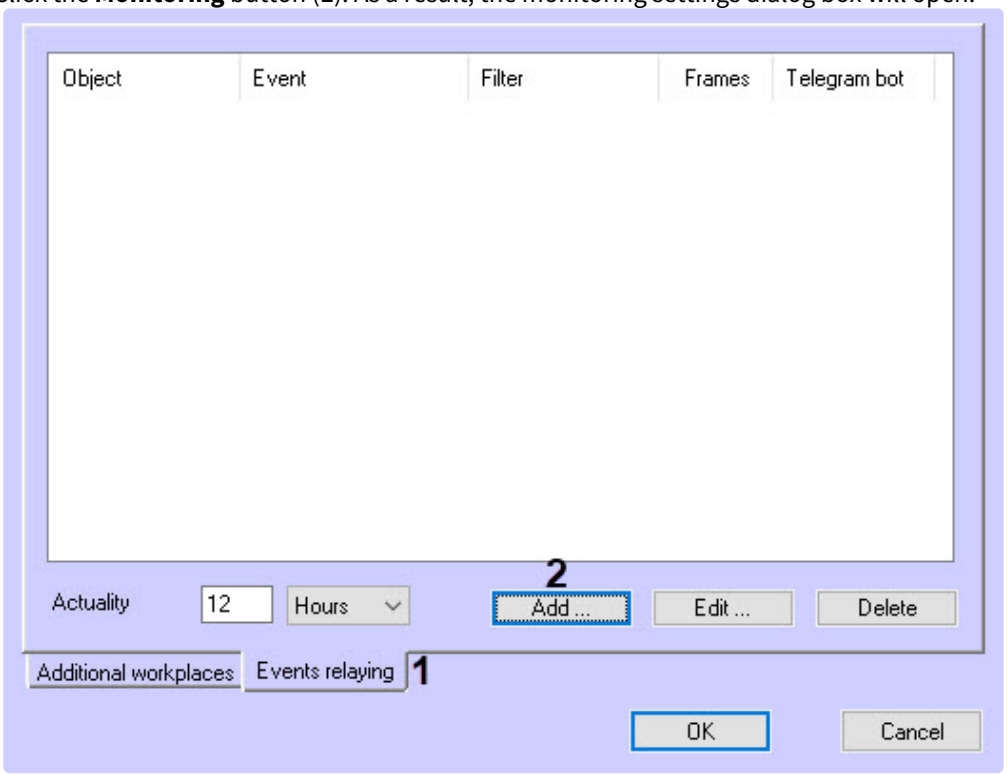
6.10 Sending alarm events via Telegram bot

Configure the sending of alarm events via **Telegram bot** as follows:

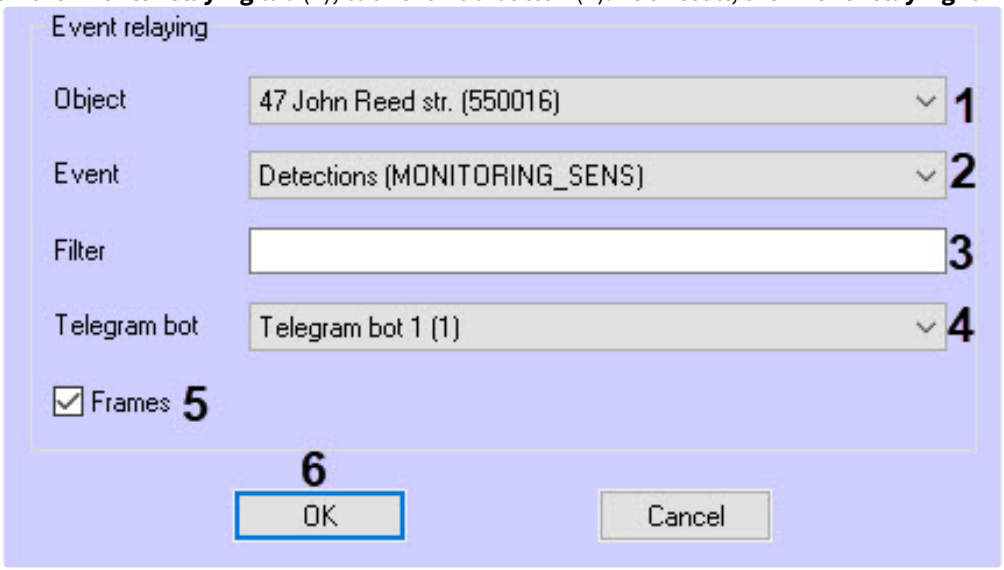
1. Go to the settings panel of the **Server Of Control** object created on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog box.



2. Click the **Monitoring** button (**1**). As a result, the monitoring settings dialog box will open:



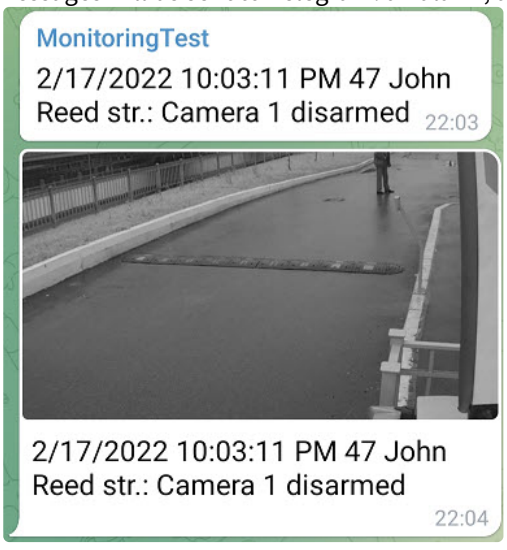
3. On the **Events relaying** tab (**1**), click the **Add** button (**2**). As a result, the **Event relaying** form will open:



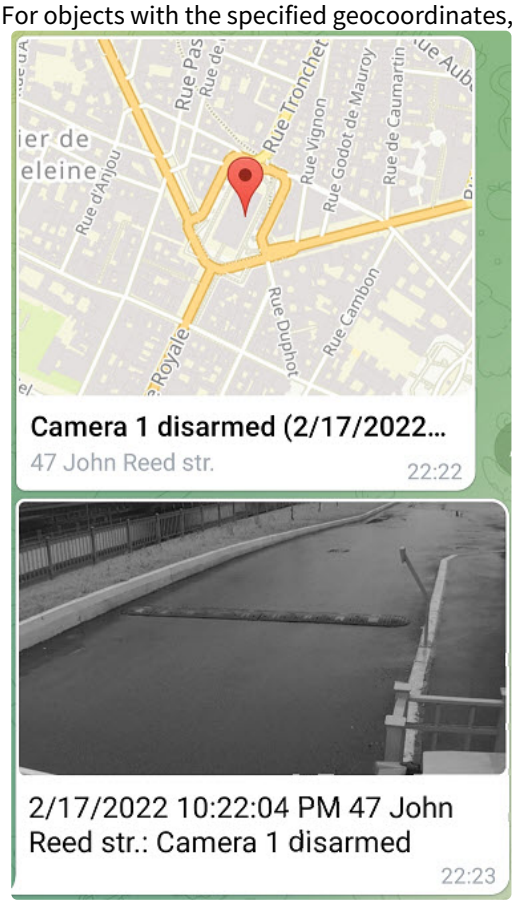
4. From the **Object** drop-down list (**1**), select the object which events should be sent via **Telegram bot**. The field is empty by default; if you leave it blank, events from all objects will be relayed.
5. From the **Event** drop-down list (**2**), select an event to send via **Telegram bot**. The field is empty by default; if you leave it blank, all events of the selected object will be relayed.
6. If necessary, fill in the **Filter** field (**3**). Example: at the **Agent of Control** object, when describing monitoring events, two events are assigned to the **Detection tools** button: **Camera disarmed** and **Camera armed**. If you enter **disarmed** in the **Filter** field, then only the **Camera disarmed** event will be relayed to the **Telegram bot**.
7. From the **Telegram bot** drop-down list (**4**), select the bot via which the events will be relayed.

> **Note**
>
> The **Telegram bot** object should be created and configured beforehand (see Sending messages via Telegram bot).

8. Set the **Frames** checkbox (**5**) to relay the jpeg frame linked to the event. When the checkbox is set, two messages will be sent to Telegram: an alarm, and then a frame:

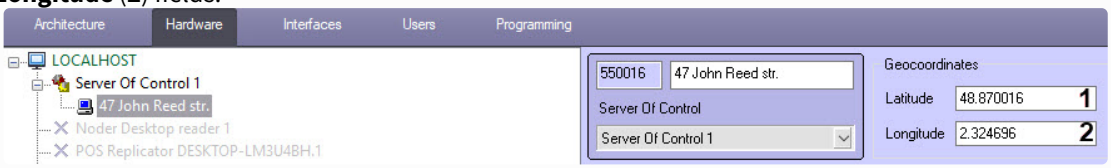


For objects with the specified geocoordinates, a geo-link will be sent in the message:

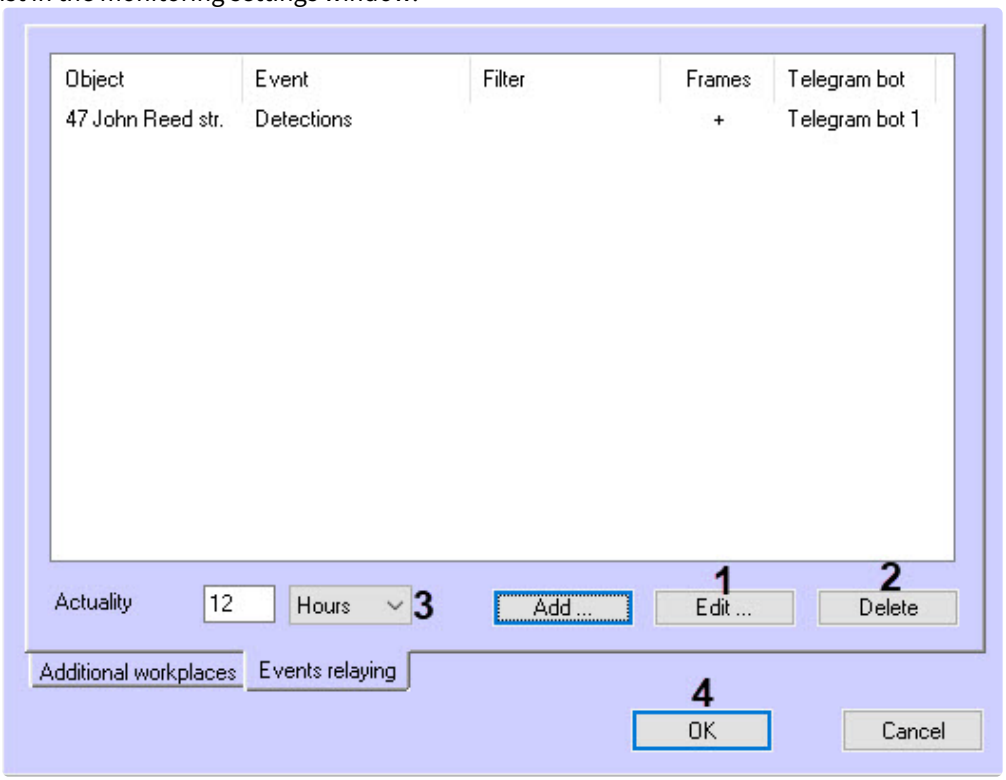


Note

To specify the **Geocoordinates**, go to the settings panel of the **Partition Of Control** object (see Creating necessary Server Of Control objects) and enter the values in the **Latitude** (**1**) and **Longitude** (**2**) fields:



9. Click the **OK** button (**6**). As a result, the **Event relaying** form will be closed and a new entry will appear in the list in the monitoring settings window:



10. In the **Monitoring** settings window, click the **Edit** button (**1**) to change an existing entry, or the **Delete** button (**2**) to remove an entry from the list.
11. Fill in the **Actuality** field (**3**). To do this, enter a value in the numeric field and select **Hours** or **Minutes** from the drop-down list of measurement units. The default value is 12 hours. This setting is used to filter out non-relevant alarms. For example, **Agent Of Control** was disconnected for several days. After the connection is established, the old alarms that occurred during this time will be sent. To prevent old alarms from being relayed to Telegram, you can set their actuality in hours or minutes.
12. Click the **OK** button (**4**). As a result, the **Monitoring** settings window will be closed and you will return to the settings panel of the **Server Of Control** object.
13. To save the changes, click the **Apply** button (**2**) on the settings panel of the **Server Of Control** object.

Configuring the sending of alarm messages via the **Telegram bot** is now complete.

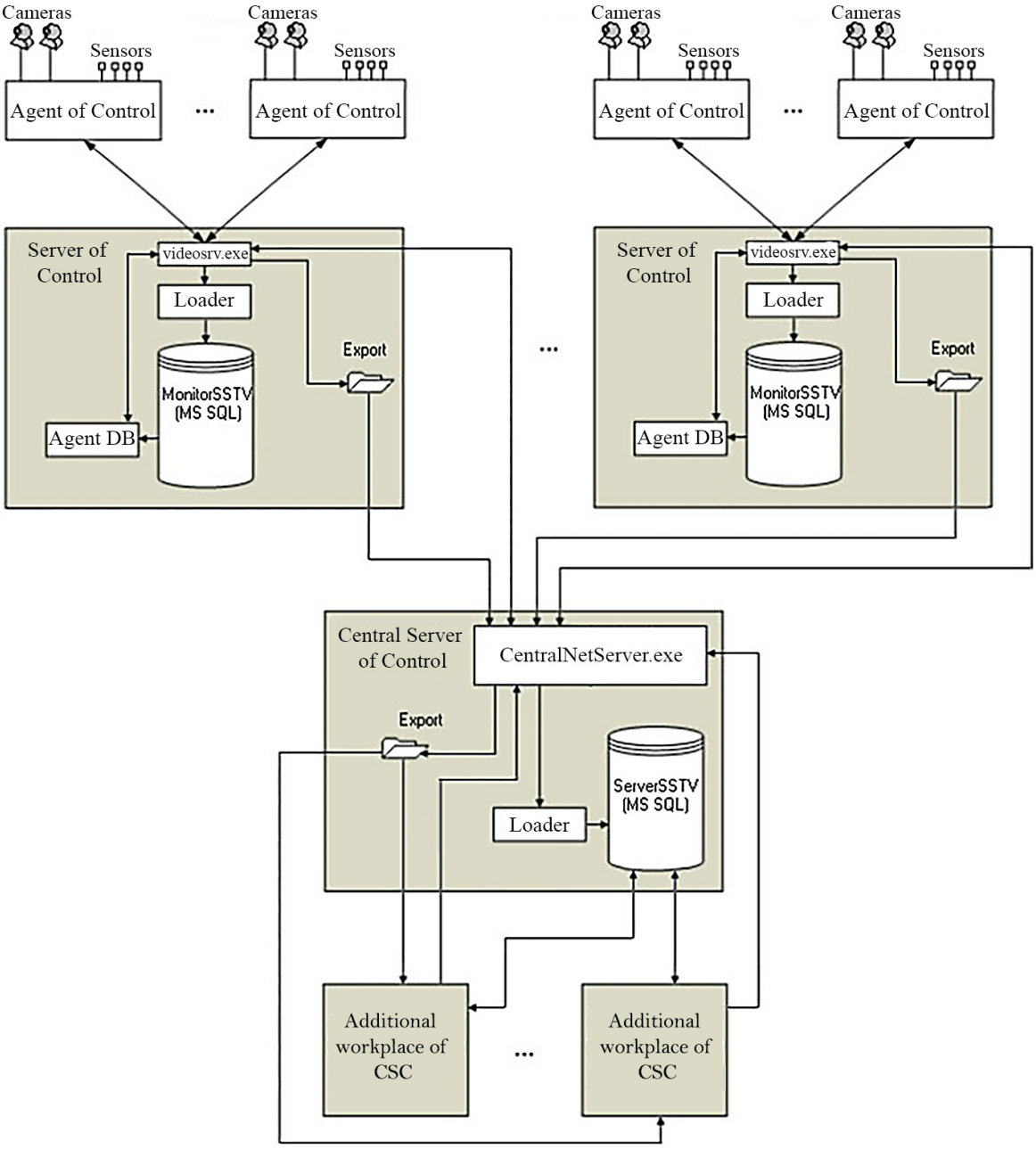
7 Configuring Central Server of Control

7.1 General principles of the Central Server of Control software

The CentralNetServer.exe communication module of the *Central Server of Control* (hereinafter referred to as *CSC*) polls the *Servers of Control* at specified intervals, sending the requests for information about changes in the MonitorSSTV database. Each *Server of Control* is requested in parallel in a separate thread. When the *Server of Control* receives such a request, it unloads the latest changes from the MonitorSSTV database with the help of the *Agent DB* (MonitorSSTVClient.exe). The CentralNetServer.exe communication module of the *CSC* receives this data and sends it to the Loader (MonitorSSTVAgent.exe), which then loads this data into the ServerSSTV database.

The data between the *CSC* and the *Servers of Control* is exchanged via FTP protocol, therefore it is necessary to configure the FTP server (see Configuring the FTP server for the Central Server of Control operation) on the *Server of Control* side.

The general scheme of the *Central Server of Control* software operation is shown in the figure below.



The *Central Server of Control* software provides the same functionality as the *Server of Control* software, but with some restrictions that are listed below.

The main functionality of the *Central Server of Control* software:

- Monitoring of all objects of the video surveillance system, as well as viewing live video and providing the ability to use the **Data gateway** object for this (you can do it in the **Monitoring** interface object).
- Searching for titles and video fragments and, based on the search results, downloading the frames and videos (you can do it in the **Search in archive** interface object).
- Generating the reports on the whole system (you can do it in the **Monitoring reports** interface object).

Restrictions of the *Central Server of Control* software:

- Demo mode is not supported.
- Alarms and errors received from the *Servers of Control* do not appear immediately on the *CSC*, but with the specified polling frequency of the Servers (see the **PeriodRequestOfStatistic** registry key in Advanced settings of the Central Server of Control).
- The *CSC* operator cannot confirm alarms in the **Monitoring** interface object. There are no **Confirm selected**, **Confirm**, and **Confirm all** buttons in the **Reaction to alarm** window.
- The toolbar of the **Monitoring** interface object has no **Force error closing** and **Show closed errors** buttons.
- The **Owner** directory cannot be edited. This directory is automatically filled with the *Servers of Control* names with which the *CSC* works. The filtering by the *Servers of Control* is supported. Also, the information from the **Owner** directory filled out on the *Server of Control* side is not transmitted to the *CSC*.
- The special operation mode joint with *Auto Intellect* is not supported (see Configuring special operation mode joint with Auto Intellect). If this mode is used in the *Server of Control*, then the information from the corresponding tables is not transmitted to the *CSC*.
- The special operation mode joint with *ACFA Intellect* is not supported (see Configuring the special mode of Monitoring operation with ACFA Intellect).
- The commands for *Agents of Control* are not supported (see Sample script for processing Server of Control command on Agent of Control).
- The video data received with the alarm is not displayed. In the **Monitoring** interface object, when right-clicking on an object, the **Video data** item is missing in the context menu.
- The **Search in archive** interface object does not support the automation of downloading videos using the xml files.

7.2 Configuring the FTP server for the Central Server of Control operation

By default, the *Central Server of Control* software works via FTP in a passive mode, and this requires adding the range of ports to which the *Central Server of Control* software will connect in the FTP server settings. It is possible to switch to the active mode. To do this, it is necessary to set the **0** value for the **PassiveModeForFTP** registry key (for details, see Registry keys reference guide).

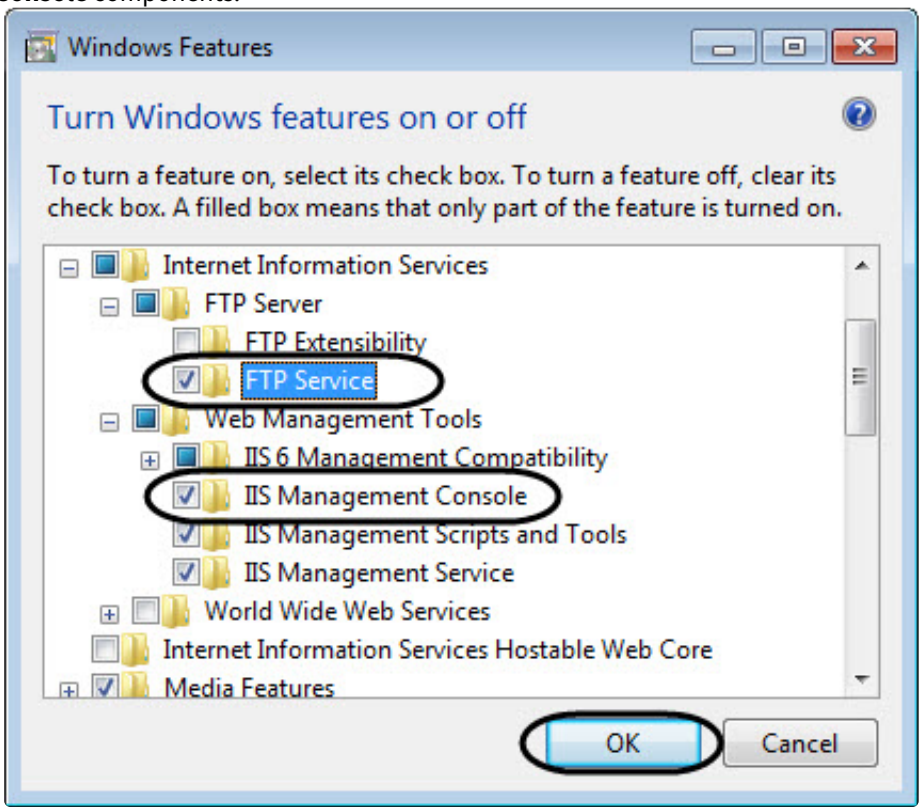
The FTP server for the *Central Server of Control* operation should be configured on the side of each *Server of Control* as follows:

1. Create a user with administrator rights in the system.

   > **Note**
   >
   > The password validity period for this user should not be limited in time.

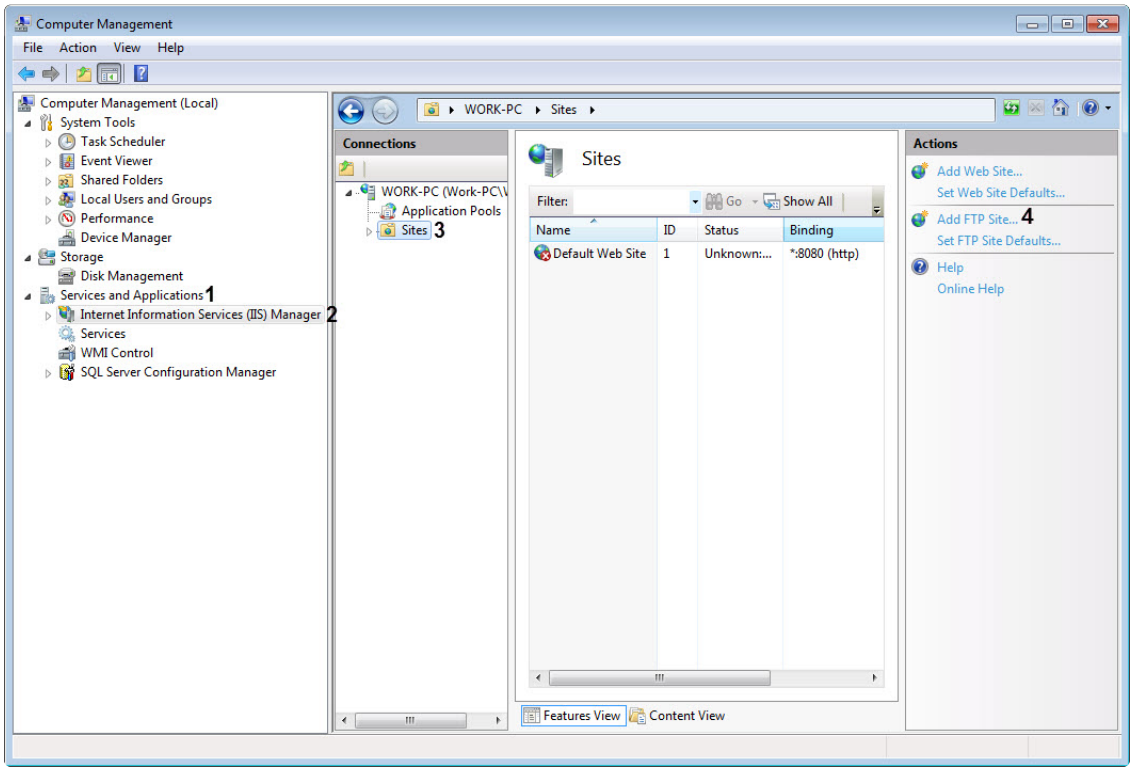
2. If IIS is not installed, install it:
   a. Open the **Control Panel** → **Programs and Features** → **Turn Windows Features on or off**.

b. In the **IIS Services** section, select the checkboxes next to the **FTP Service** and **IIS Management Console** components.



c. Click **OK**.

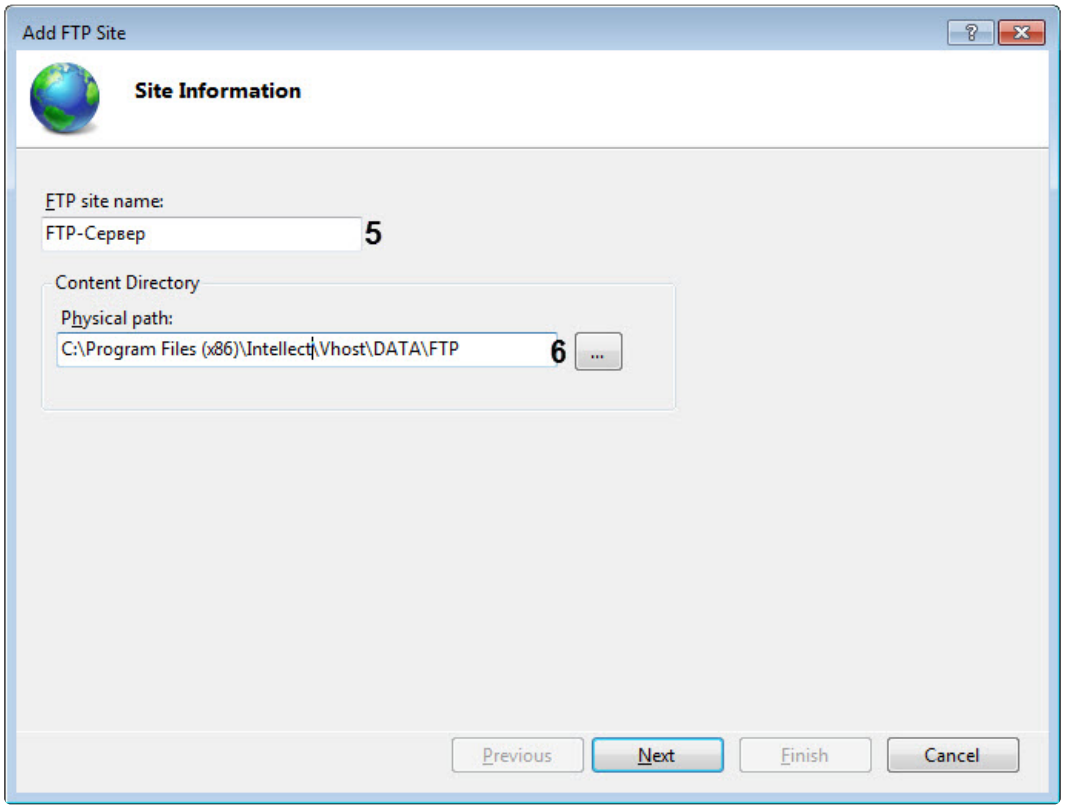
3. Open **Computer Management** and in the **Services and Applications** section (**1**), select **IIS Manager** (**2**).
   a. In the **Connections** area, select the **Sites** folder (**3**), and then in the **Actions** area, click the **Add FTP Site...** link (**4**). As a result, the **Add FTP Site** window appears.



b. In the **FTP site name** field (**5**), enter the name of the FTP site.

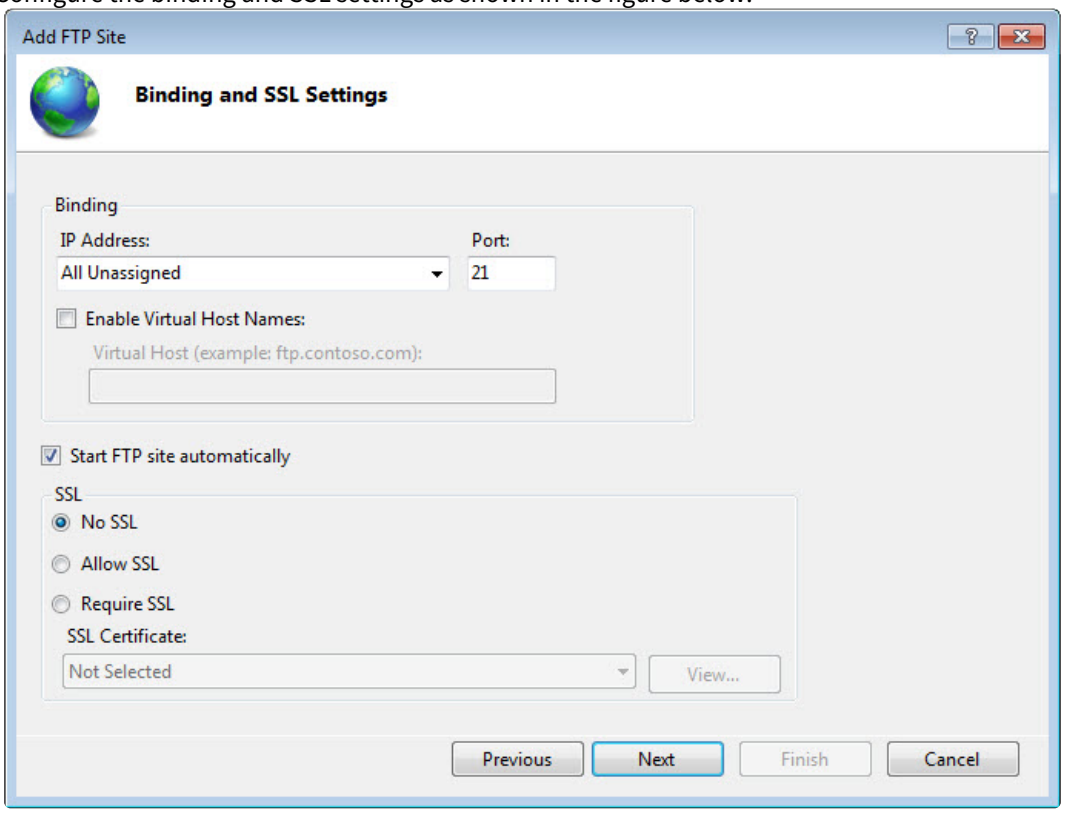
c. In the **Physical path** field (**6**), or using the  button, specify the path to the FTP directory. By default, the FTP directory is located at *<Intellect installation directory>\Vhost\DATA\FTP*. You can change this directory using the **FtpPath** registry key (for details, see Registry keys reference guide).

> **Note**
>
> To increase the performance of data exchange, it is recommended that the export directory (see Specifying the export directory) and the FTP directory are located on the same disk.



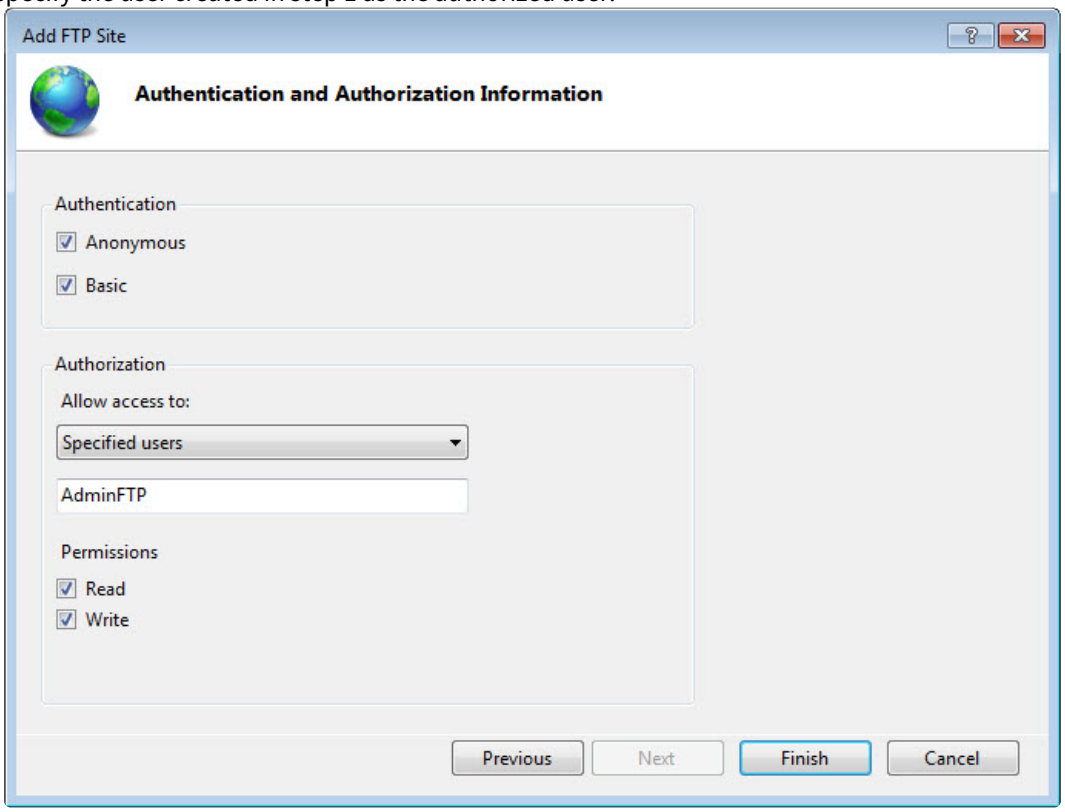
d. Click **Next**.

e. Configure the binding and SSL settings as shown in the figure below.



f. Click **Next**.

g. Configure the authentication and authorization as shown in the figure below. It is necessary to specify the user created in step 1 as the authorized user.



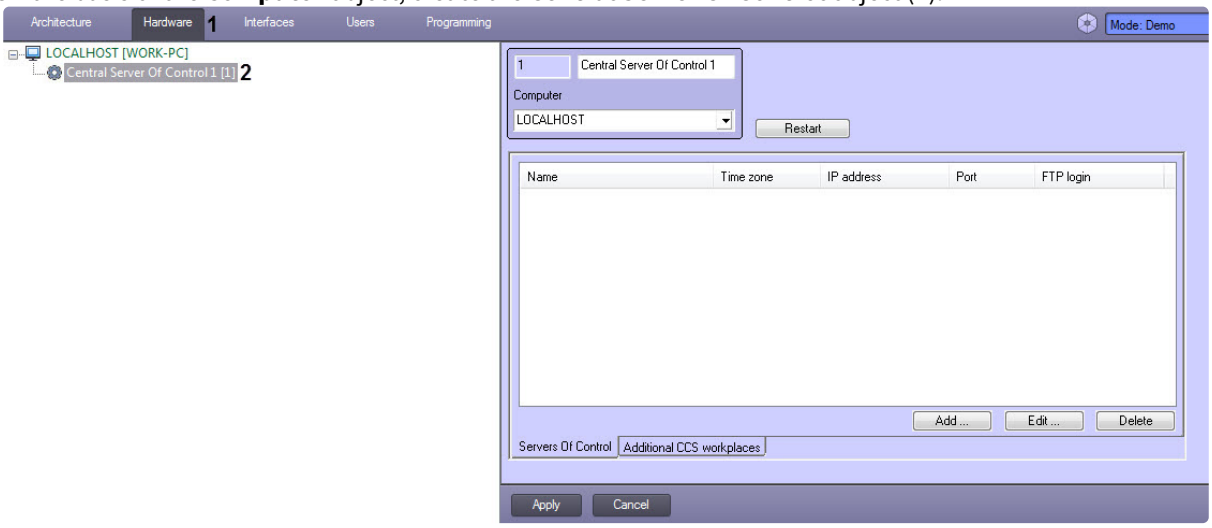
h. Click **Finish**.

Configuring the FTP server for the *Central Server of Control* software operation is complete.

7.3 Creating the Central Server Of Control object

Create the *Central Server Of Control* object in the hardware tree as follows:

1. Go to the **Hardware** tab of the **System settings** dialog box (**1**).
2. On the basis of the **Computer** object, create the **Central Server Of Control** object (**2**).



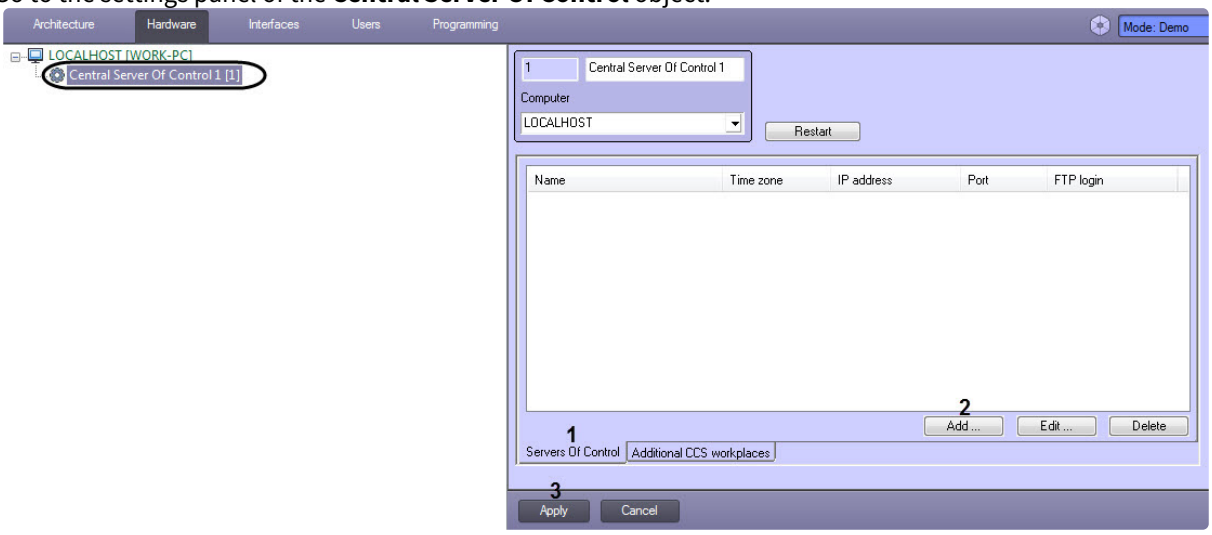
Creation of the *Central Server Of Control* object is completed.

7.4 Configuring the Servers of Control tracking

7.4.1 Adding the Server Of Control

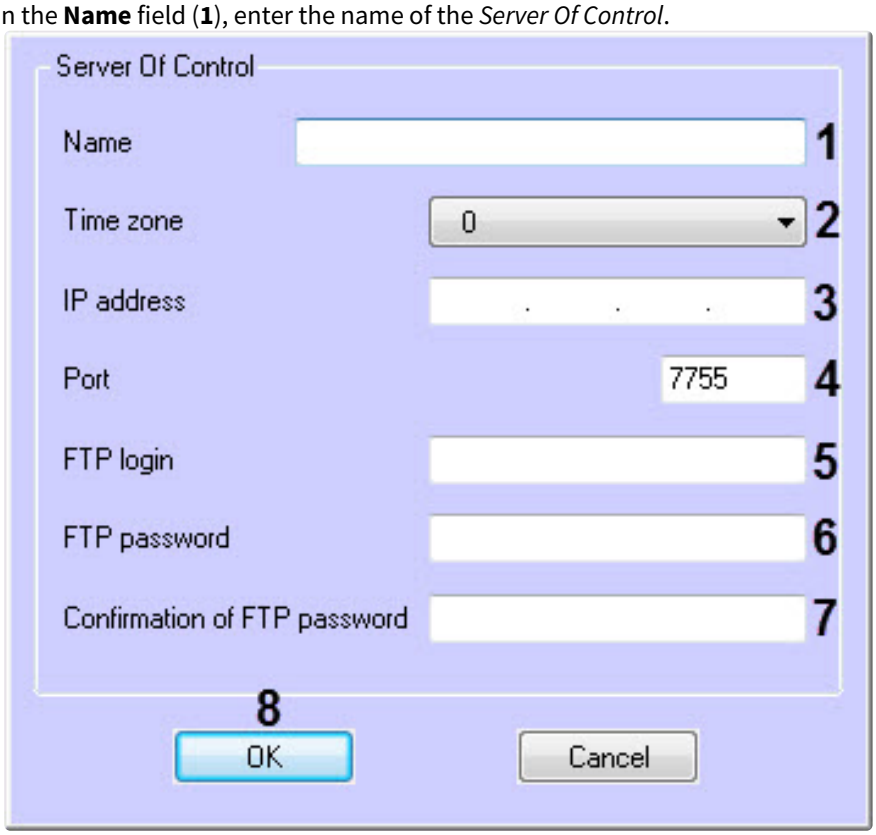
To add the *Server Of Control*, do the following:

1. Go to the settings panel of the **Central Server Of Control** object.



2. On the **Servers Of Control** tab (**1**), click the **Add** button (**2**).
3. In the **Server Of Control** window that appears, do the following:

a. In the **Name** field (**1**), enter the name of the *Server Of Control*.

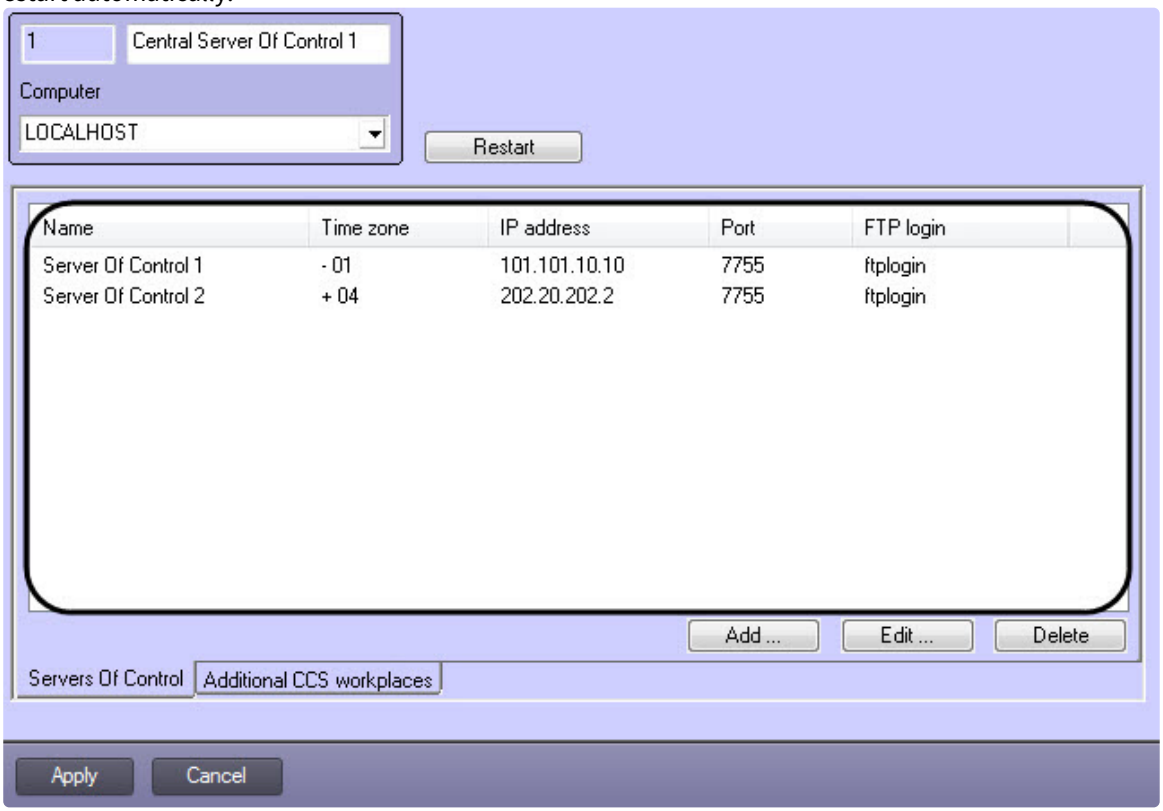


b. From the **Time zone** drop-down list (**2**), select the value corresponding to the time zone difference between the Server that should be tracked and the Server on which the *Central Server Of Control* is installed.

> **Note**
>
> For example, if the *Central Server Of Control* is installed on the Server in Oslo, and the Server that should be tracked is located in London, then it is necessary to select the time zone **-1**.

c. In the **IP address** field (**3**), specify the IP address of the *Server Of Control*.
d. In the **Port** field (**4**), specify the connection port of the *Server Of Control*.
e. In the **FTP login** field (**5**), enter the username with administrator rights to connect to the FTP Server. This server will be used for exchanging the data between the *Central Server Of Control* and the *Server Of Control* (see Configuring the FTP server for the Central Server of Control operation).
f. In the **FTP password** field (**6**), enter the password of the user with administrator rights to connect to the FTP server.
g. In the **Confirmation of FTP password** field (**7**), re-enter the password for connecting to the FTP Server.
h. Click the **OK** button (**8**).

4. As a result, the specified *Server Of Control* will be added to the list, and the *Central Server Of Control* will restart automatically.



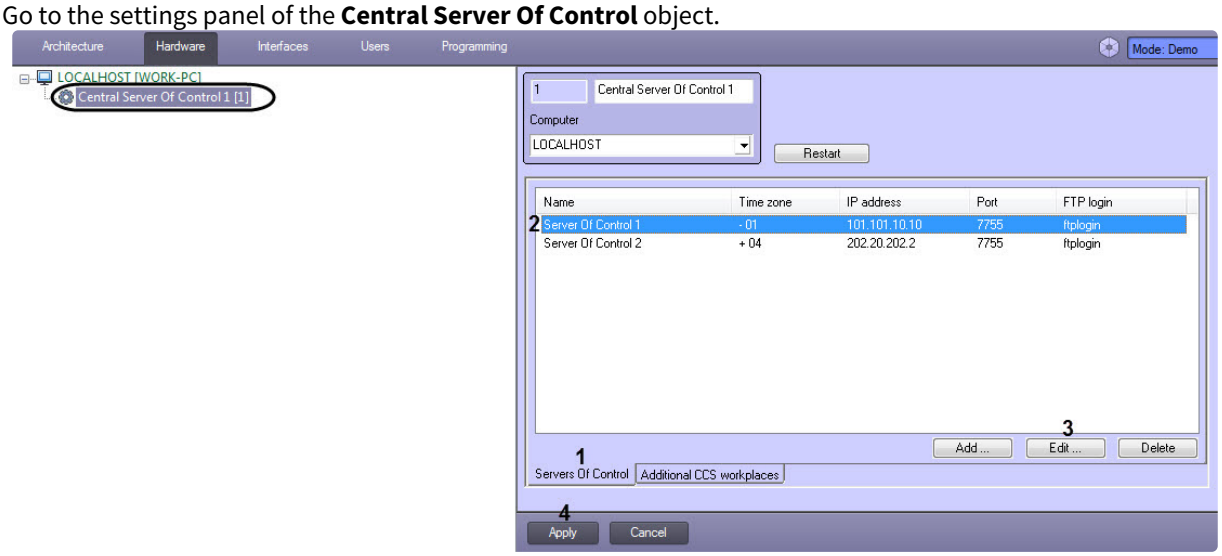
5. To add other *Servers Of Control*, repeat steps 2-3.
6. Click the **Apply** button (**3**).

The *Server Of Control* is added.

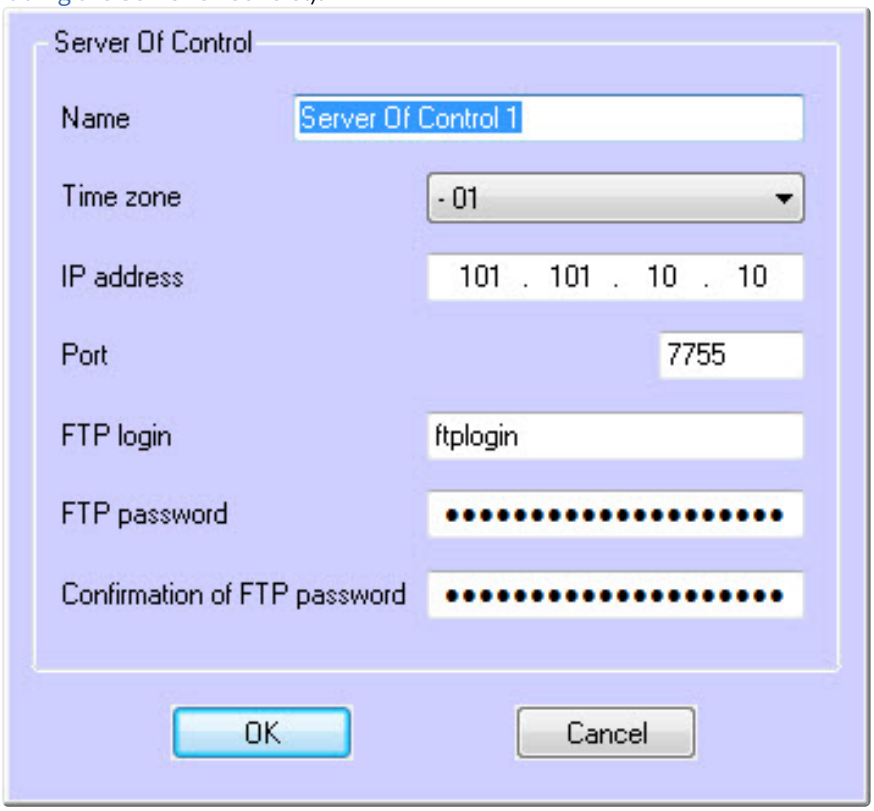
7.4.2 Editing the Server Of Control

To edit the *Server Of Control*, do the following:

1. Go to the settings panel of the **Central Server Of Control** object.



2. On the **Servers Of Control** tab (**1**), select the *Server Of Control* that should be edited (**2**), and click the **Edit** button (**3**).
3. As a result, the **Server Of Control** window will be displayed. Make the necessary changes (for details, see Adding the Server Of Control).



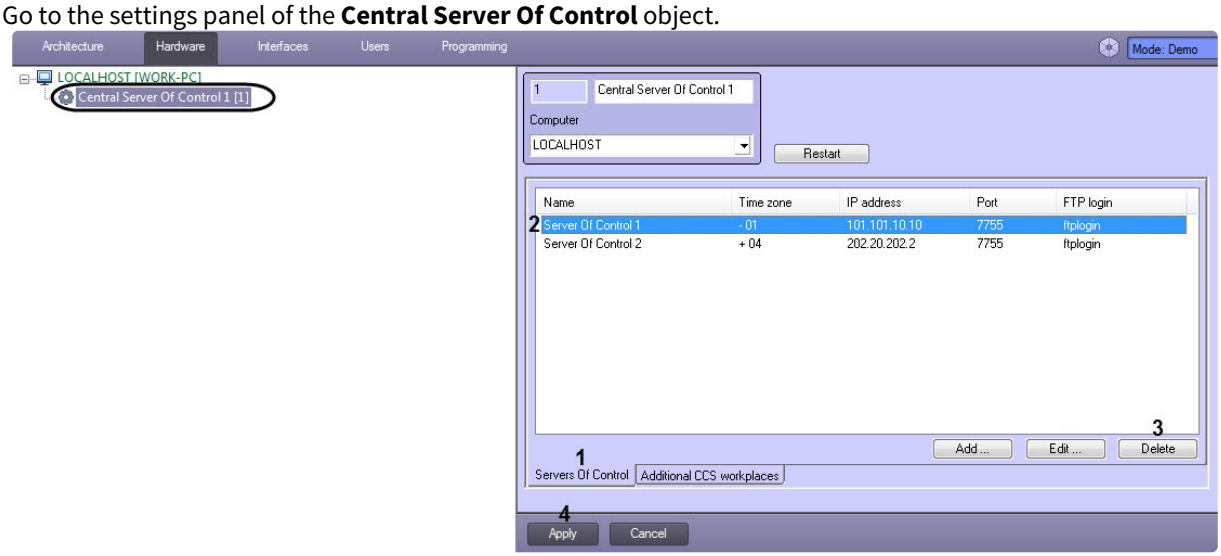
4. Click the **OK** button.
5. Click the **Apply** button (**4**).

The *Server Of Control* is edited.

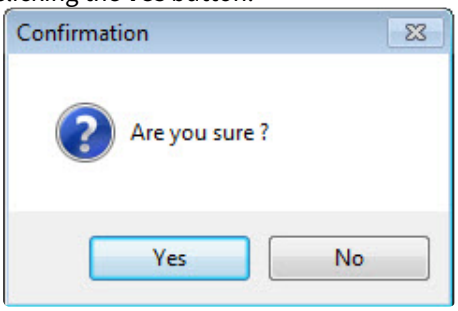
7.4.3 Deleting the Server Of Control

To delete the *Server Of Control*, do the following:

1. Go to the settings panel of the **Central Server Of Control** object.



2. On the **Servers Of Control** tab (**1**), select the *Server Of Control* that should be deleted (**2**), and click the **Delete** button (**3**).
3. As a result, a confirmation window will open. Confirm the deletion of the selected *Server Of Control* by clicking the **Yes** button.



4. Click the **Apply** button (**4**).

The *Server Of Control* is deleted.

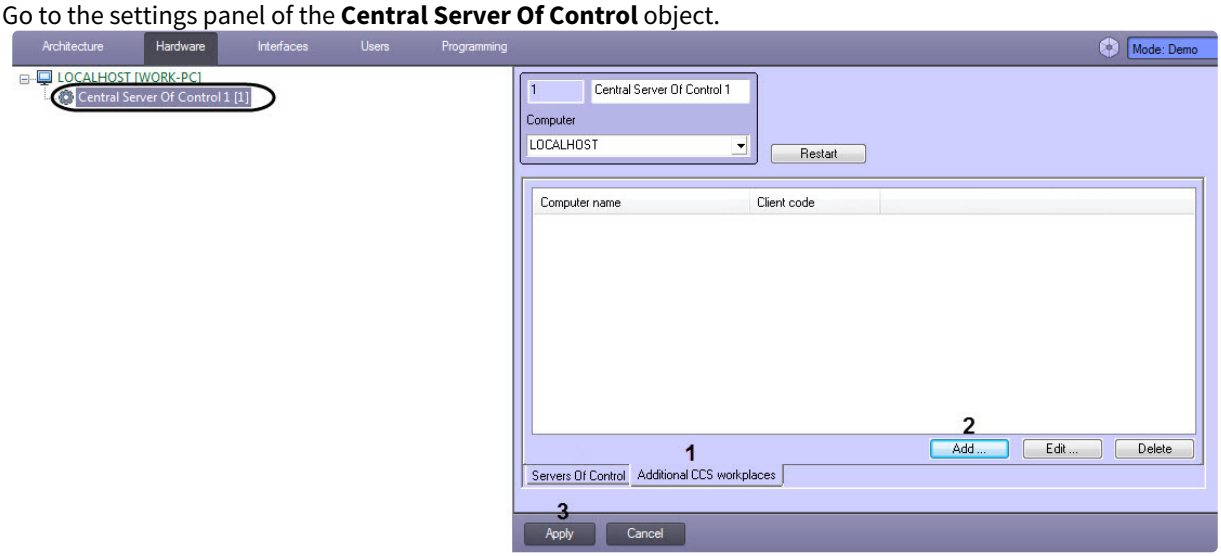
7.5 Configuring the Additional workplace of CSC connection rights to the Central Server Of Control

7.5.1 Adding the Additional workplace of CSC

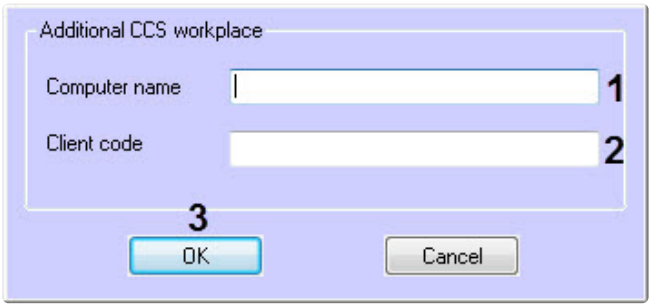
For the *Additional workplace of CSC* software to work, it is necessary to add the *Additional workplaces of CSC* to the *Central Server Of Control*, and specify the computer name and the client code for each of them.

To add the *Additional workplace of CSC*, do the following:

1. Go to the settings panel of the **Central Server Of Control** object.

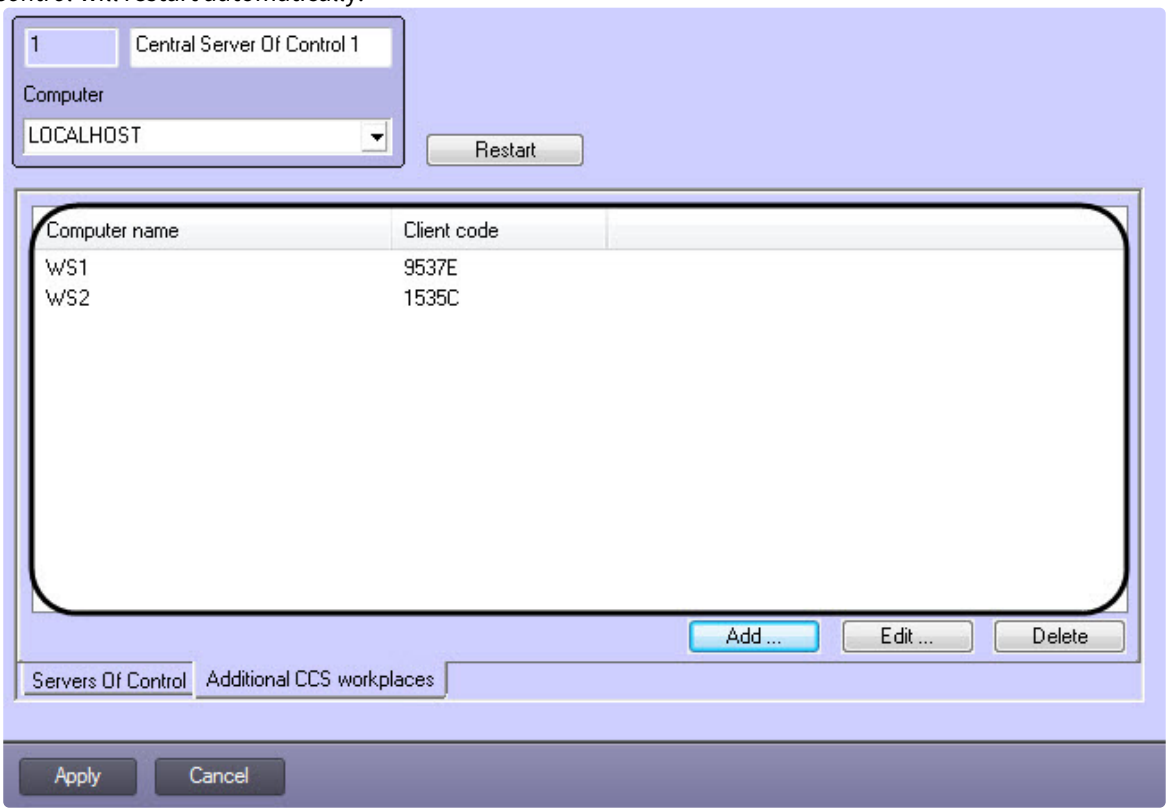


2. On the **Additional CSC workplaces** tab (**1**), click the **Add** button (**2**).
3. In the **Additional CSC workplace** window that appears, do the following:
   a. In the **Computer name** field (**1**), enter the computer name on which the *Additional workplace of CSC* software is installed.



   b. In the **Client code** field (**2**), specify the Client code that is linked with the computer hardware (for details, see List of Additional workplaces).
   c. Click the **OK** button (**3**).

4. As a result, the specified *Additional workplace of CSC* will be added to the list, and the *Central Server Of Control* will restart automatically.



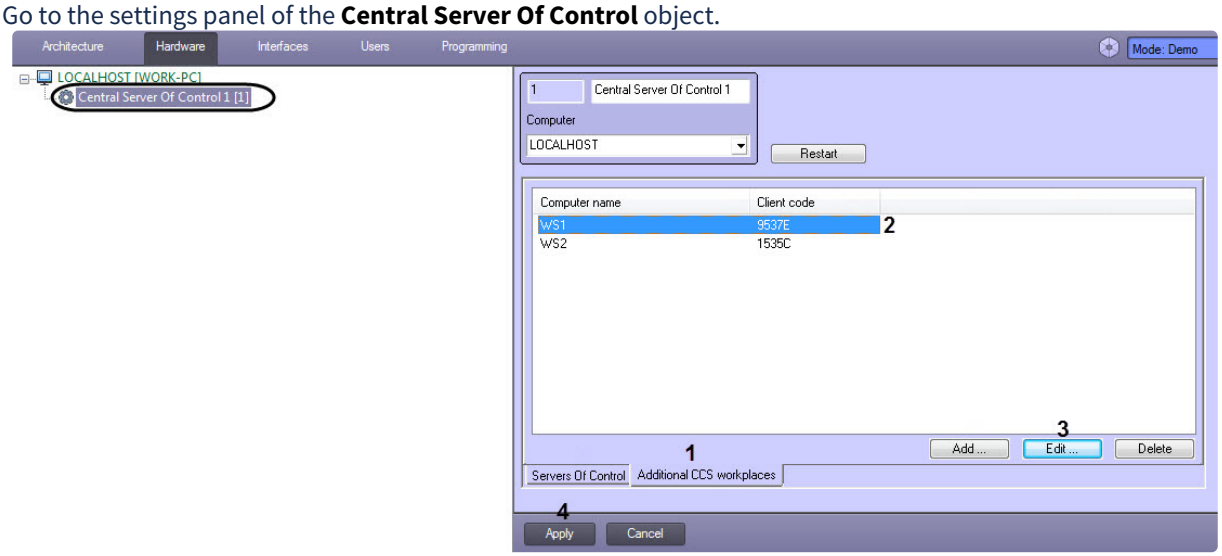
5. To add other *Additional workplaces of CSC*, repeat steps 2-3.
6. Click the **Apply** button (**3**).

The *Additional workplace of CSC* is added.

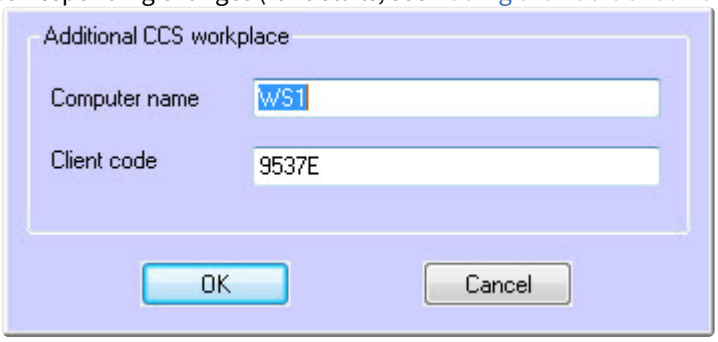
7.5.2 Editing the Additional workplace of CSC

To edit the *Additional workplace of CSC*, do the following:

1. Go to the settings panel of the **Central Server Of Control** object.



2. On the **Additional CSC workplaces** tab (**1**), select the *Additional workplace of CSC* which should be edited (**2**), and click the **Edit** button (**3**).
3. As a result, the **Additional CSC workplace** window will be displayed where it is necessary to make the corresponding changes (for details, see Adding the Additional workplace of CSC).



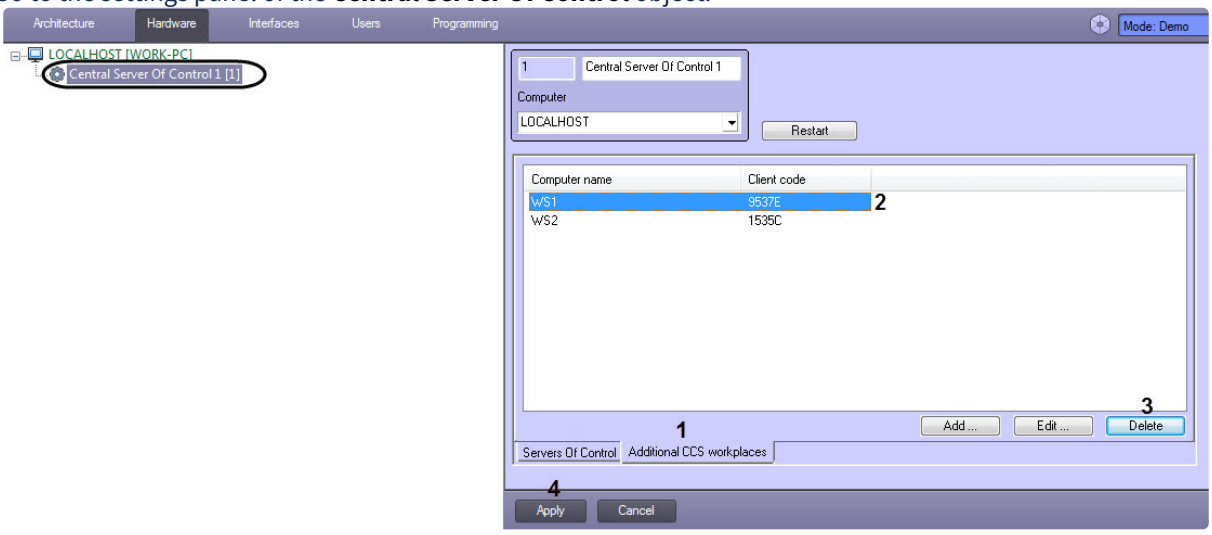
4. Click the **Apply** (**4**) button.

The *Additional workplace of CSC* is edited.

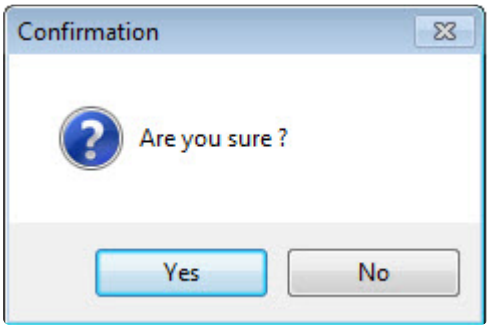
7.5.3 Deleting the Additional workplace of CSC

To delete the *Additional workplace of CSC*, do the following:

1. Go to the settings panel of the **Central Server Of Control** object.



2. On the **Additional CSC workplaces** tab (**1**), select the *Additional workplace of CSC* which should be deleted (**2**), and click the **Delete** button (**3**).
3. As a result, the **Additional CSC workplace** window will be displayed where it is necessary to click the **Yes** button to confirm the deletion of the selected *Additional workplace of CSC*.



4. Click the **Apply** (**4**) button.

The *Additional workplace of CSC* is deleted.

7.6 Advanced settings of the Central Server of Control

> **Note**
>
> The registry keys reference guide can be found in the Registry keys reference guide, for more information about working with the registry, see Working with Windows OS registry.

You can apply the advanced settings of the *Central Server of Control* using the following registry keys:

1. To change the polling period of *Servers of Control* statistics, it is necessary to specify the corresponding value in minutes for the **PeriodRequestOfStatistic** registry key.
2. To change the archive period of the CentralNetServer.log log file which belongs to the CentralNetServer.exe communication module, it is necessary to specify the corresponding value in hours for the **LogArchPeriod** registry key.
3. To change the maximum size of the CentralNetServer.log log file which belongs to the CentralNetServer.exe communication module at which it begins to archive ignoring the **LogArchPeriod** parameter, it is necessary to specify the corresponding value in megabytes for the **LogMaxSize** registry key.
4. To change the archive retention period of the CentralNetServer.log log files which belong to the CentralNetServer.exe communication module, it is necessary to specify the corresponding value in months for the **LogArchDelPeriod** registry key. When the retention period is exceeded, the archives are removed.
5. To change the data retention period of closed errors and alarms in the Server SSTV DB, it is necessary to specify the corresponding value in months for the **KeepDB** registry key. When the retention period is exceeded, the data are removed.
6. By default, the *Central Server of Control* requests a complete package of statistics from all *Servers of Control* only once, when it first connects to the *Servers of Control*.
   - To execute a request for a complete statistics package from a specific *Server of Control* once, it is necessary to activate the **RequestFullStatistic[N]** registry key, where N is the internal identifier of the *Server of Control* object. The request will be executed when the CentralNetServer.exe communication module is launched, and the value of this key will automatically change to **0**.
   - To request a complete statistics package from all *Servers of Control* every time the CentralNetServer.exe communication module is launched, it is necessary to activate the **RequestFullStatisticOnStartup** registry key.

     > **Attention!**
     >
     > Requesting a complete statistics package is a resource-intensive operation. It is only necessary to activate the keys request a complete statistics package if absolutely necessary.

Applying the advanced settings of the *Central Server of Control* is completed.

7.7 Working with Central Server of Control without Windows administration rights

To allow the user not added to the Administrators group in the Windows operating system to work correctly with *Central Server of Control*, make sure the following conditions are fulfilled:

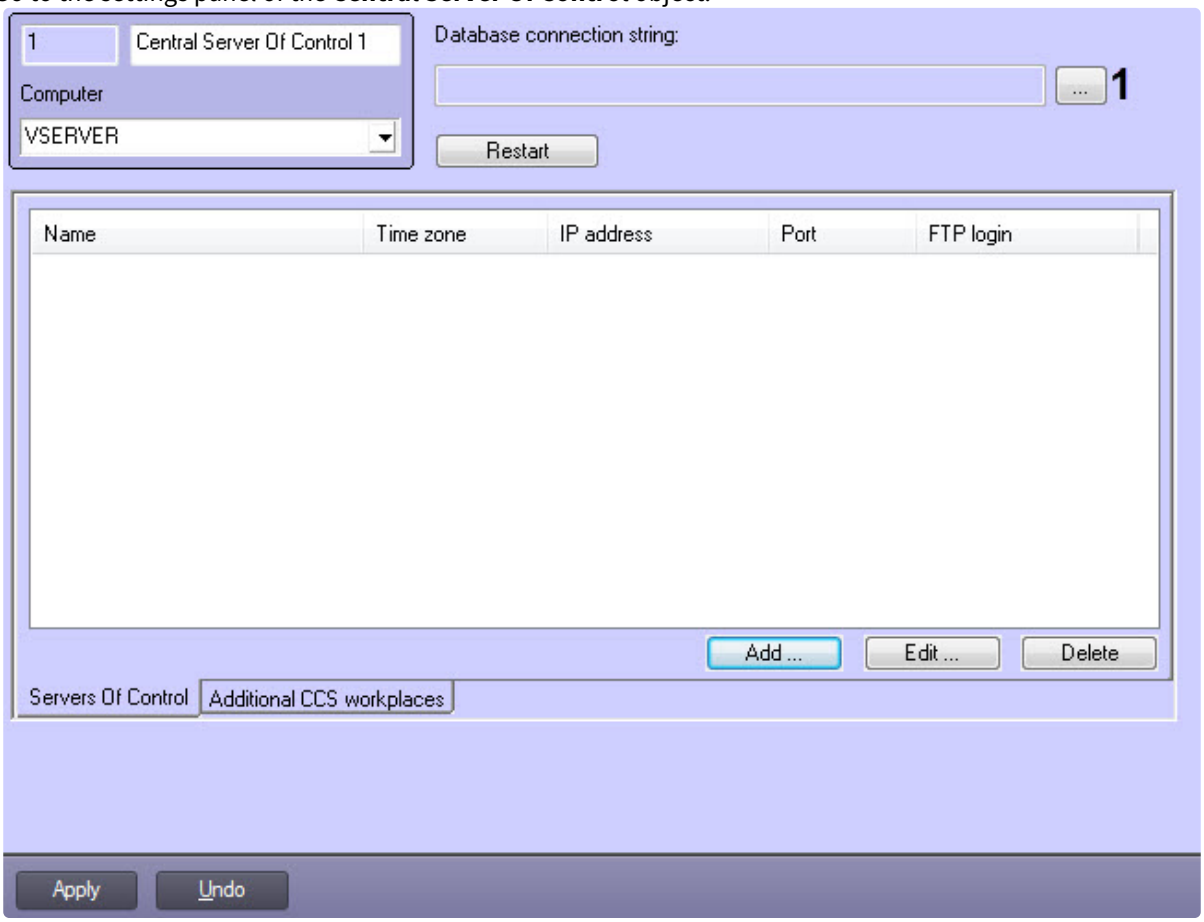
1. The user must be given full access to the registry key:
   - For a 32-bit system: HKEY_LOCAL_MACHINE\Software\BitSoft
   - For a 64-bit system: HKEY_LOCAL_MACHINE\Software\Wow6432Node\BitSoft

2. The user must be granted full rights to the export directory (see Specifying the export directory).

7.8 Configuring the Central Server Of Control from another server in a distributed configuration

To configure the *Central Server Of Control* from another server in a distributed configuration, do the following:

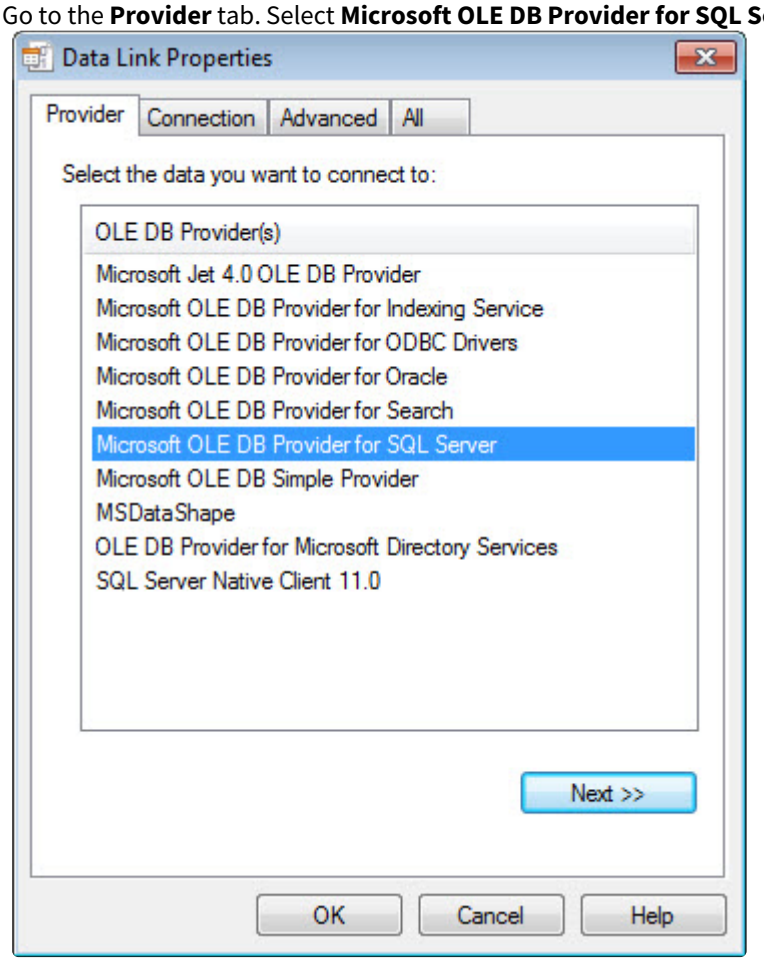
1. Go to the settings panel of the **Central Server Of Control** object.



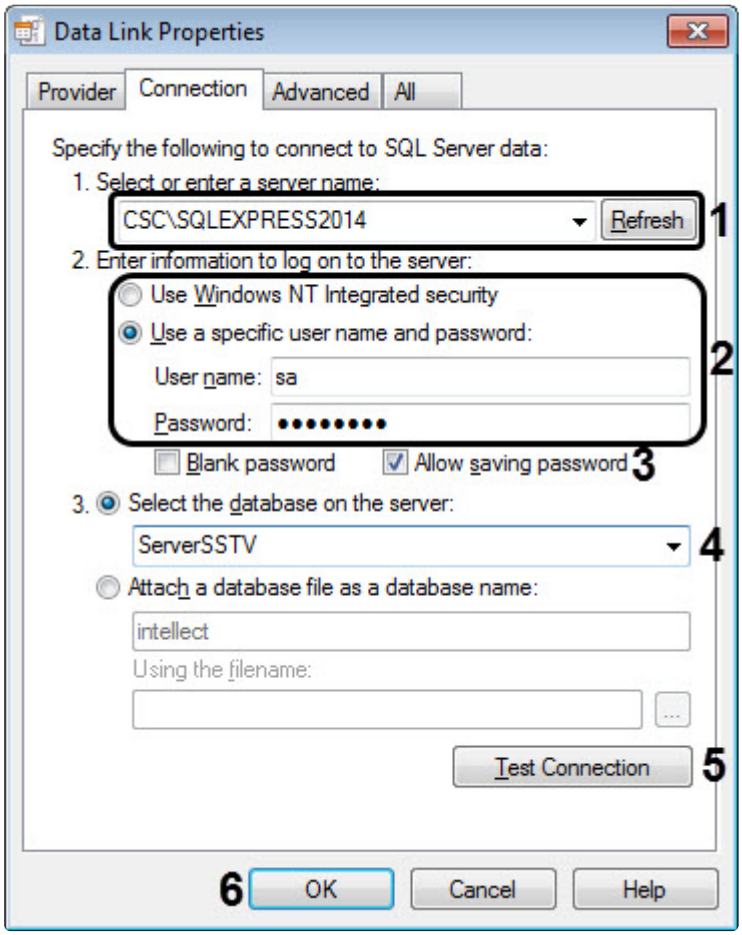
2. Click the ... button (**1**). The **Data Link Properties** window opens. Configure the connection to the remote *Central Server Of Control* database as follows:

> **Note**
>
> The **Database connection string** parameter is displayed only if the *Central Server Of Control* is configured from another server in a distributed configuration.

a. Go to the **Provider** tab. Select **Microsoft OLE DB Provider for SQL Server**.

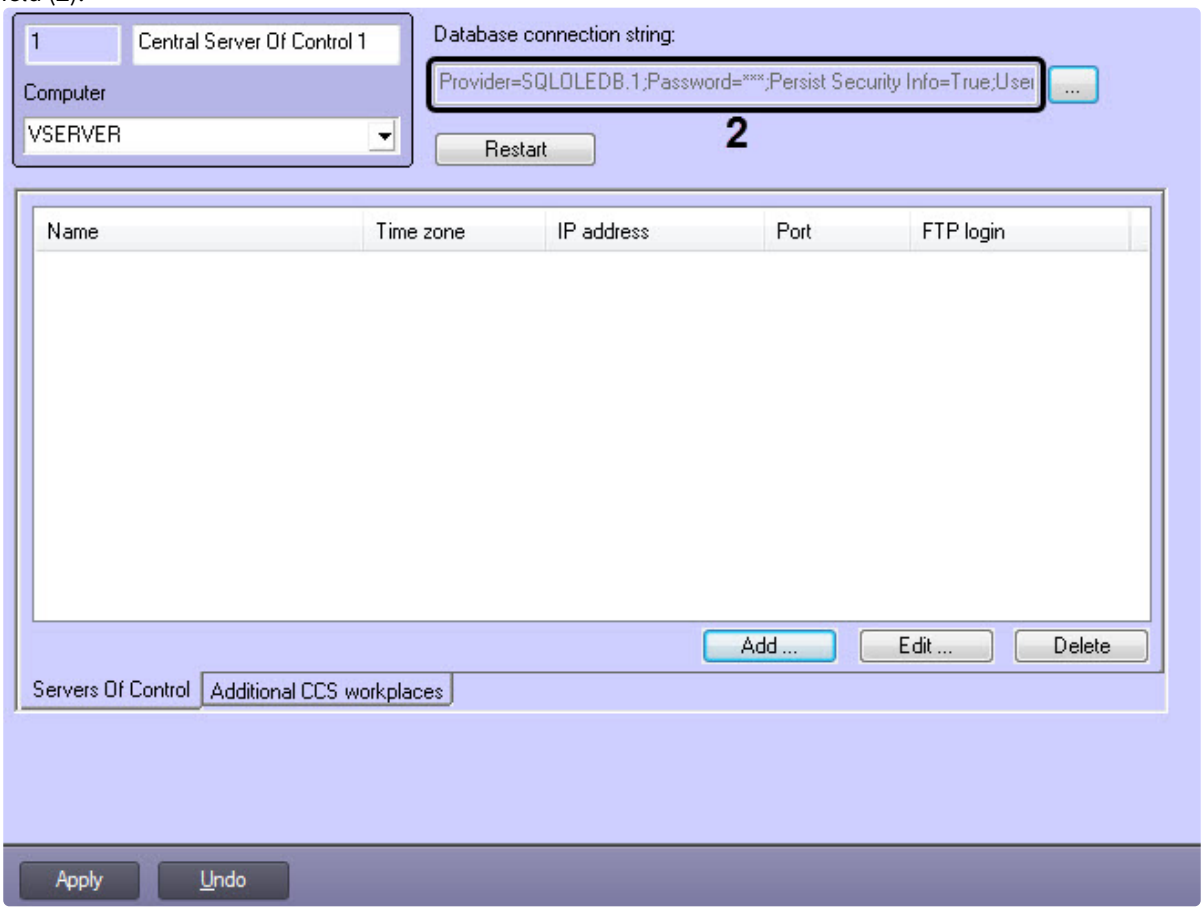


b. Go to the **Connection** tab. From the **Select or enter a server name** drop-down list, select the name of the database server that stores the *Central Server Of Control* database (**1**).



c. Set the **Enter information to log on to the server** switch to the **Use a specific user name and password** position and enter the name and password to connect to the MS SQL Server (**2**).
d. Set the **Allow saving password** checkbox (**3**).
e. From the **Select the database on the server** drop-down list, select the name of the *Central Server Of Control* database (ServerSSTV by default) (**4**).
f. Click the **Test Connection** button (**5**). If the connection data is correct, a window with the message "Connection check completed" will be displayed.
g. Click the **OK** button (**6**).

3. The configured string of connection to the *Central Server Of Control* database will be displayed in the text field (**2**).



4. As a result, you can start configuring the *Central Server Of Control* (see Configuring Central Server of Control).

Configuring the *Central Server Of Control* from another server in a distributed configuration is now complete.

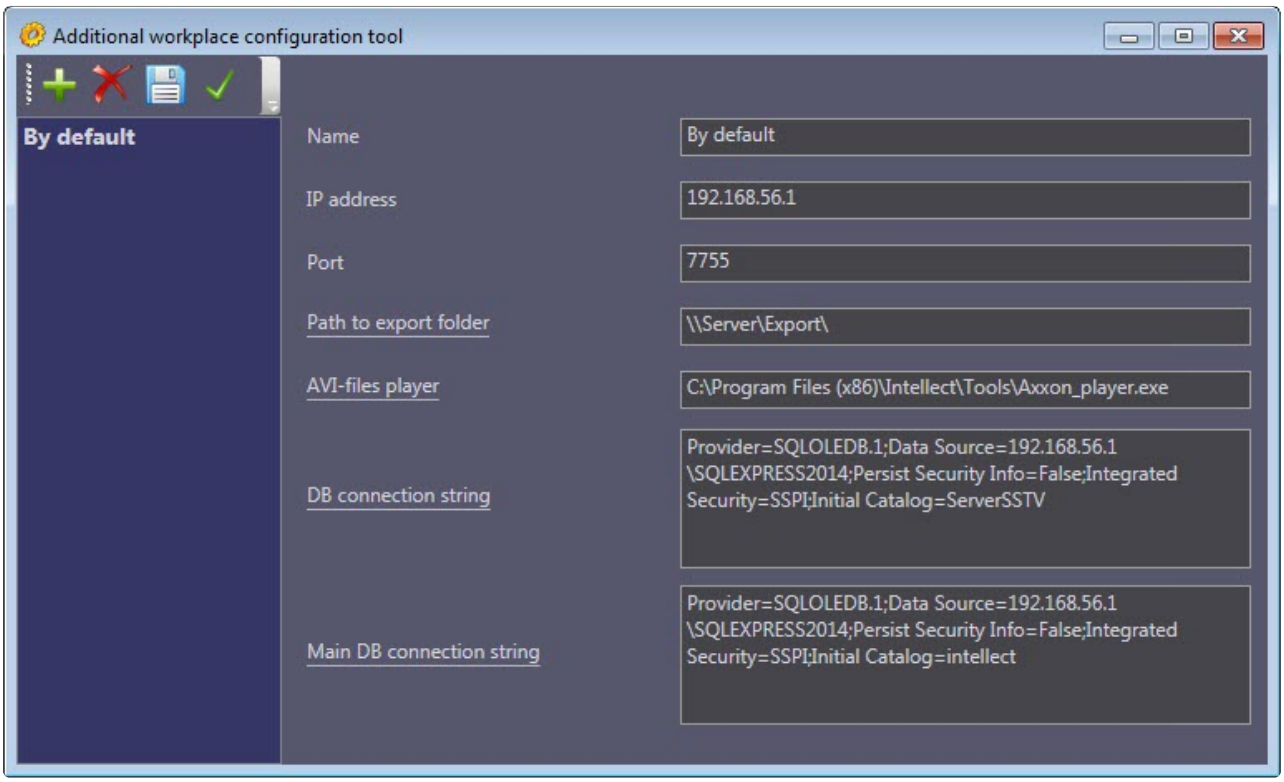
8 Configuring Additional workplace and Additional workplace of CSC

8.1 List of Servers of Control/CSC

Additional workplace/Additional workplace of CSC can operate with only one *Server of Control/Central Server of Control* (further named Server) at a time. However, the list of Servers can be configured and the active Server can be selected. For this use the *Additional workplace configuration tool*. The tool can be run in one of the following ways:

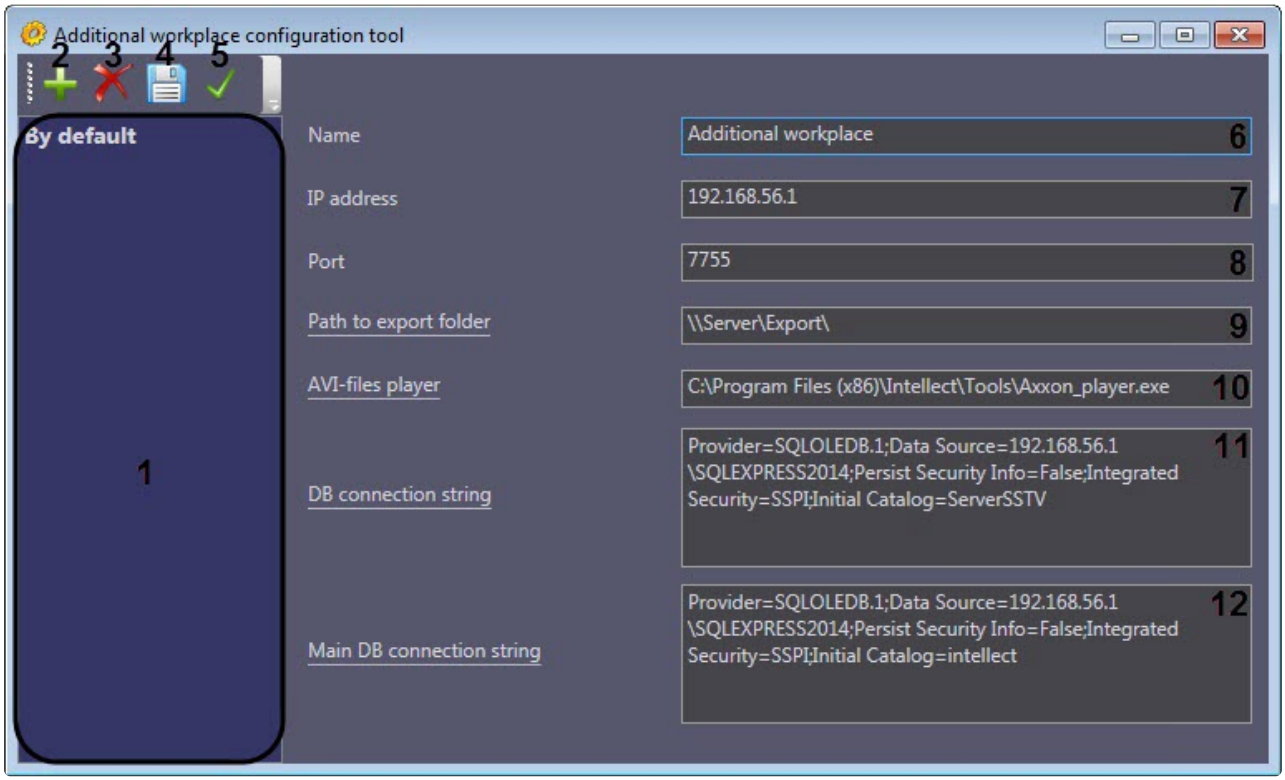
1. Click **Start -> All Programs -> Intellect -> Monitoring -> Additional workplace configuration tool**.
2. Use the ARMSelector.exe executable file, located in the <Intellect installation directory>\VHost\SYSTEM\ folder.

The tool is shown in the figure.



8.1.1 Interface of Additional workplace configuration tool

Interface elements of *Additional workplace configuration tool* are described in the table.



#	Name	Method of setting the parameter value	Default value	Description
1	List of Servers	The **Add**, **Remove** and **Set as active** buttons	By default there is the Server in the list. It is named **By default** and is created during installation.	Displays the list of existing Servers. An active Server is highlighted in bold.
2	The **Add** button	Click the button	-	Adding a new Server to the list.
3	The **Delete** button	Click the button	-	Deleting a selected Server from the list.
4	The **Save** button	Click the button	-	Saving the changes
5	The **Set as active** button	Click the button	-	Setting a selected Server as an active one.
6	The **Name** field	Enter a value in the field	See #1. When a new Server is added to the list it is named **New** by default.	Setting a name for Server. This name is used only in this tool.

7	The **IP address** field	Enter a value in the field	127.0.0.1 **Important! The value of this parameter is to be changed according to the IP address of the Server.**	Setting the IP address to connect to the VideoSrv.exe module (if the *Server of Control* is added) or CentralNetServer.exe (if the *Central Server of Control* is added).
8	The **Port** field	Enter a value in the field	7755	Setting a port to connect to the corresponding communication module VideoSrv.exe/ CentralNetServer.exe. To connect to the VideoSrv.exe module, it is necessary to specify the port that is selected in the **TCP/ IP port (Archive)** field on the settings panel (see Configuring a connection). To connect to the CentralNetServer.exe module, it is necessary to specify the port that is selected in the **IPPort** registry key (see Registry keys reference guide, for more information about working with the registry, see Working with Windows OS registry).
9	The **Path to export folder** field	The **Path to export folder** link or enter a value in the field	-	Setting a path to the network folder on the Server where there are archive files requested from the *Agents of Control*.
10	The **AVI-files player** field	The **Path to executable file** link or enter a value in the field	-	Setting the path to the executable file of the video player on the *Additional worksplace/Additional workplace of CSC* used to playback the video clips requested from the *Agents of Control* (see Request for video clips from objects).

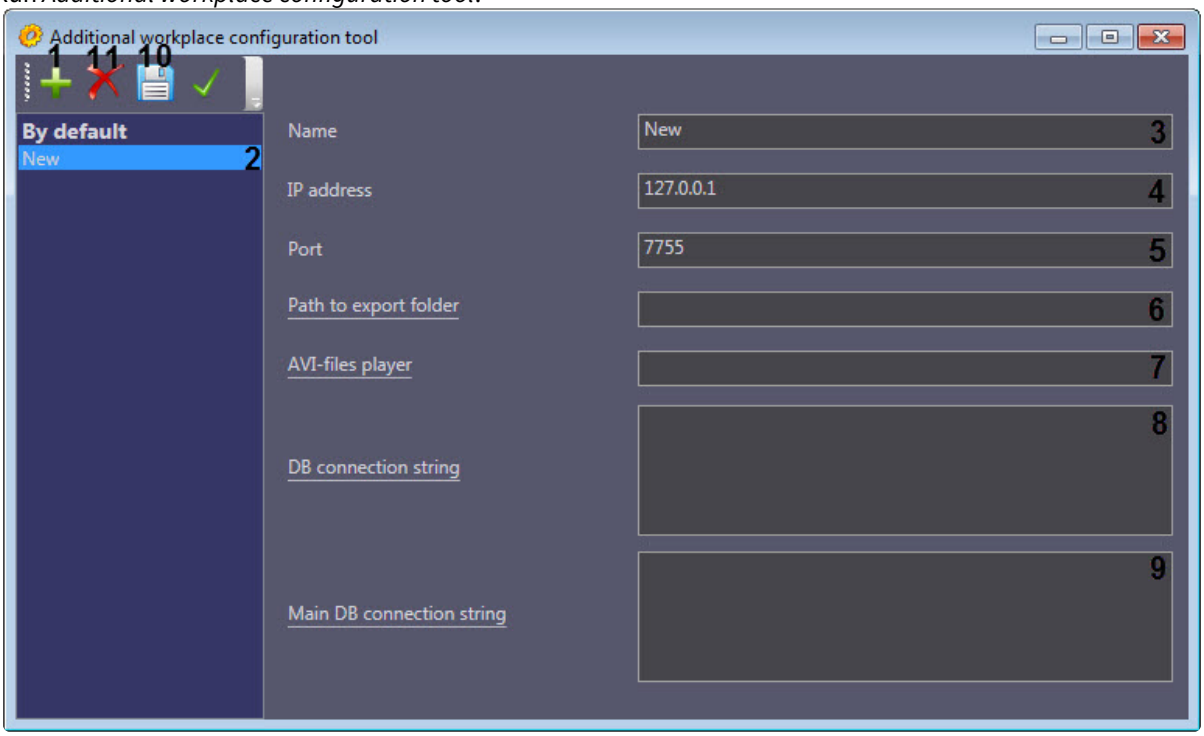
11	The **DB connection string** field	The **DB connection string** link	-	Setting the Server DB connection string. The **Data Link Properties** box appears when clicking the **DB connection string** link.
12	The **Main DB connection string** field	The **Main DB connection string** link	-	Setting the connection string to the base *Intellect* DB on the Server. The Data Link Properties box appears when clicking the **Main DB connection string** link.

8.1.2 Adding Server of Control to the list

By default the Server (named “By default”) is added to Additional workplace configuration right after installation *of Monitoring* software package. Its settings are the same as those specified during installation (see Additional workplace installation section).

Add a new Server to the list as follows:

1. Run *Additional workplace configuration tool*.



2. Click the  button (**1**).
3. A new Server named **New** is added to the list (**2**).
4. Rename the Server if necessary (**3**).

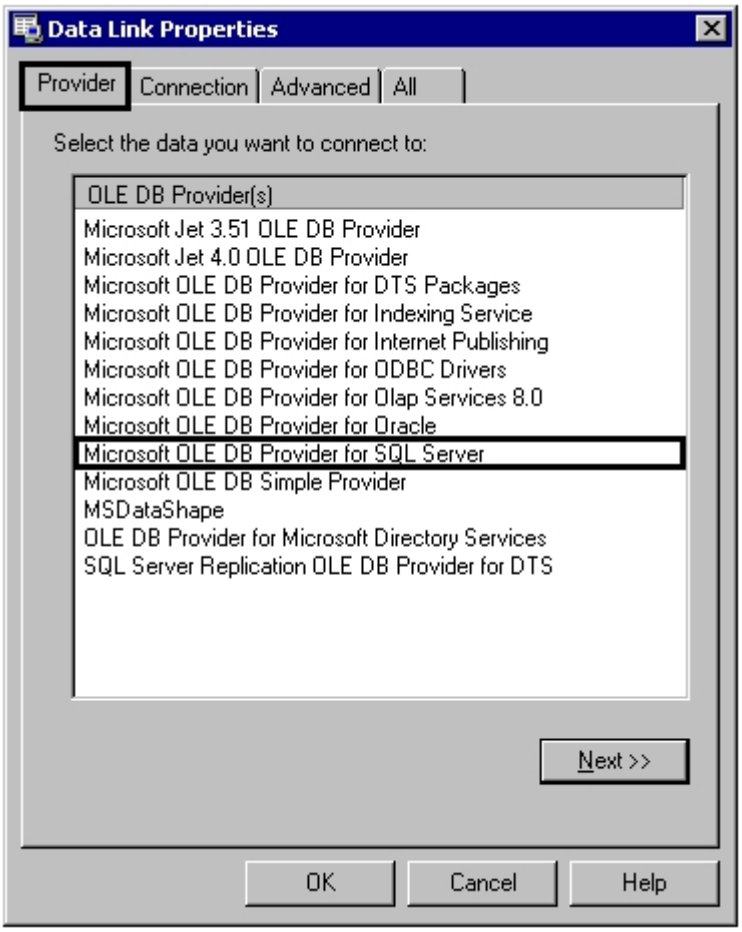
> **Note.**

This name is used in the *Additional workplace configuration tool* only.

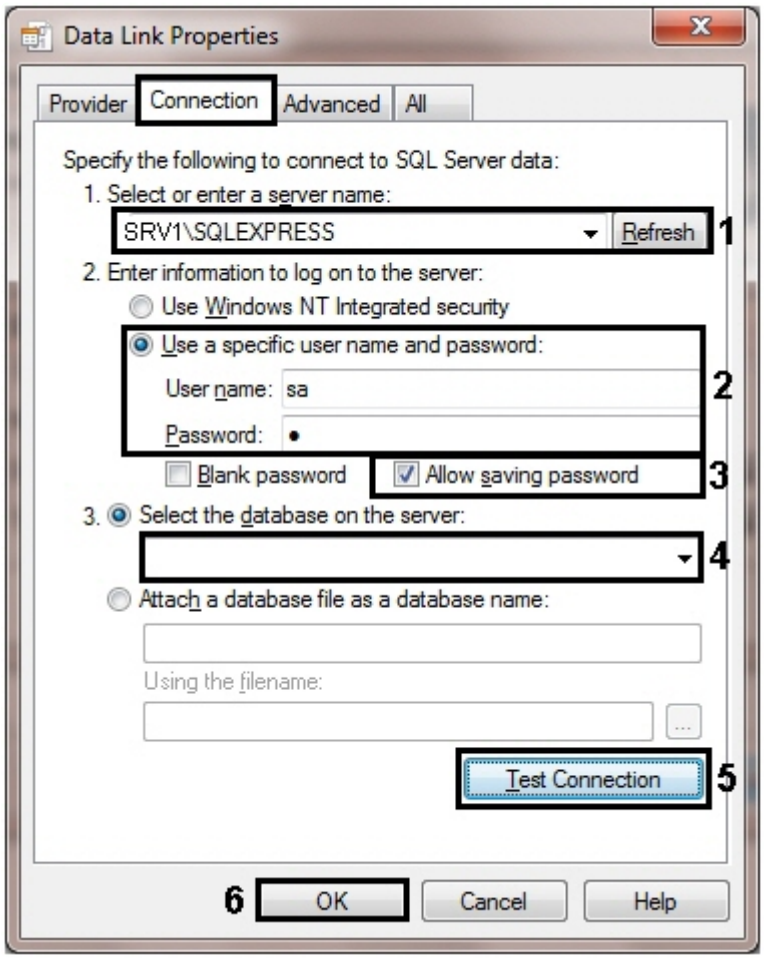
5. Specify the IP address of computer where the corresponding communication module is run: *VideoSrv.exe* module (if the *Server of Control* is added) or *CentralNetServer.exe* (if the *Central Server of Control* is added) (**4**).
6. Specify the connection port to the *VideoSrv.exe/CentralNetServer.exe* module (**5**).

> **Note.**
>
> To connect to the VideoSrv.exe module, it is necessary to specify the port that is selected in the **TCP/IP port (Archive)** field on the settings panel (see Configuring a connection).
> To connect to the CentralNetServer.exe module, it is necessary to specify the port that is selected in the **IPPort** registry key (see Registry keys reference guide).

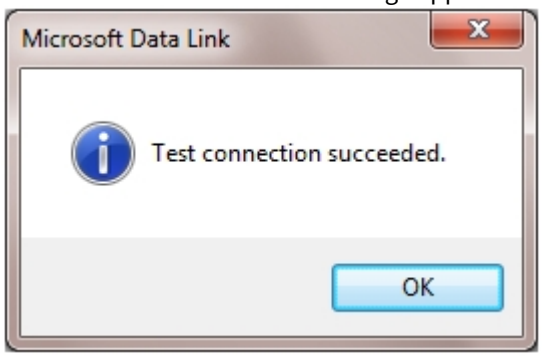
7. Specify the path to network folder on the Server where there are archive files requested from the *Agent of Control* (**6**) (see Specifying the export directory). A standard **Browse for Folder** dialog box appears when clicking the **Path to export folder** link. Select a required folder.
8. Specify the path to the executable file of the video player on the *Additional workplace/Additional workplace of CSC* used to playback the video clips requested from the *Agents of Control* (see Request for video clips from objects) (**7**).
9. Click the **DB connection string** link (**8**). The **Data Link Properties** box appears. Configure DB connection to remote *Server* as follows:
    a. Go to the **Provider** tab. Select **Microsoft OLE DB Provider for SQL Server**.



b. Go to the **Connection** tab.



c. In the **1. Select or enter a server name:** dropdown list select a name of DB server where the Server DB is stored (**1**).
d. Set the **2.Enter information to log on to the sever**: to the **Use a specific user name and password**: position and specify the user name and password to connect to MS SQL Server (**2**).
e. Select the **Allow saving password** check box (**3**).
f. In the **Select the database on the server**: dropdown list select the name of the Server DB (**4**).
g. Click the **Test Connection** button (**5**). If connection data is specified correctly, then the box with the **Test connection succeeded** message appears.



Note.

If there is the **Connection failed** message, then check if there is connection to the Server computer and if the server DB is configured correctly and then repeat steps 9.a-9.g.

h. Click the **OK** button (**6**).

10. The configured connection string is displayed in the text field (**8**).
11. Click the **Main DB connection string** link (**9**). The **Data Link Properties** box appears. Configure DB connection to the base *Intellect* DB similarly to the Server (see steps 9.a-9.h). The configured connection string is displayed in the text field.
12. Click the  button to save the changes (**10**).

Note.

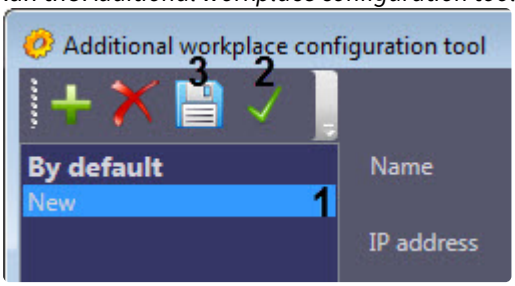
To remove the Server from the list, select it and click the  button (**11**).

Server is now added to the list.

8.1.3 Selecting active Server of Control

Select an active Serverused by the *Additional worksplace/Additional workplace of CSC* as follows:

1. Run the *Additional workplace configuration tool*.



2. Select the required Server in the list (**1**).
3. Click the  button (**2**).
4. Click the  button (**3**).

Active Server is now selected.

8.2 Working with Additional worksplace/Additional workplace of CSC without Windows administration rights

To allow the user not added to the Administrators group in the Windows operating system to work correctly with *Additional worksplace/Additional workplace of CSC*, make sure the user has the full access to the following registry section:

- For a 32-bit system: HKEY_LOCAL_MACHINE\Software\BitSoft\
- For a 64-bit system: HKEY_LOCAL_MACHINE\Software\Wow6432Node\BitSoft\

8.3 Creating and configuring Data gateway

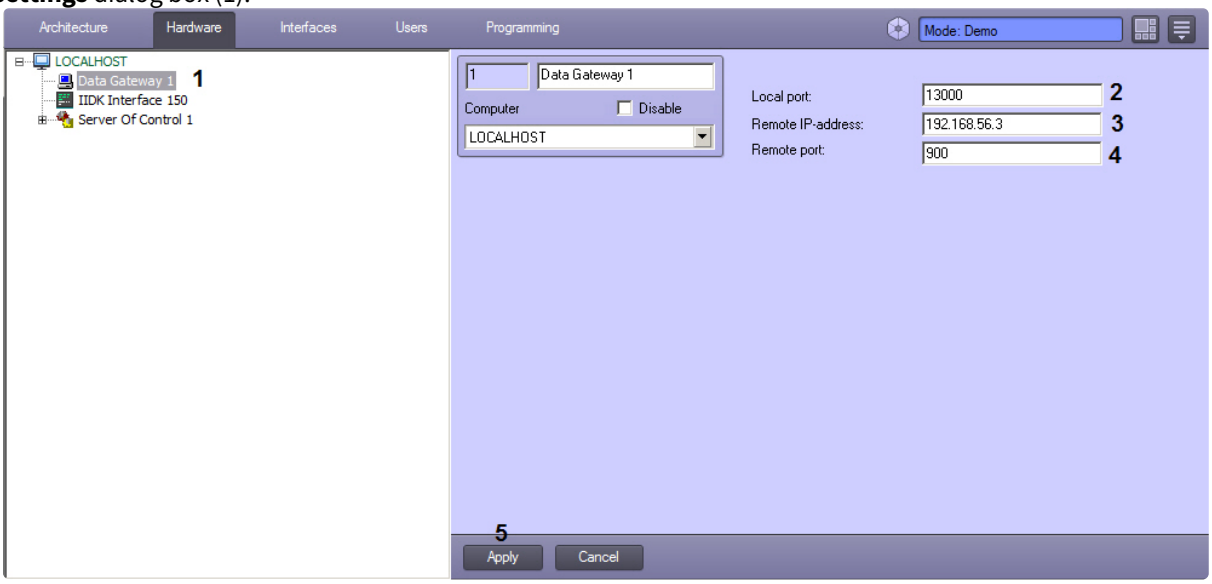
Data gateway is needed when live video is transmitted from *Agents of Control* to *Additional workplaces/Additional workplaces of CSC* in another subnet and *Monitoring* software components are not united in the distributed video surveillance system, as so as in this case **Video gate** object cannot be used.

The **Data gateway** objects are created on the computers with *Server of Control/CSC* installed. The number of the **Data gateway** objects must be equal to the number of *Agent of Control* to receive live video from. For example, if there are 10 **Agents of Control**, then create 10 **Data Gateways** with **Local port** and **Remote IP-address** corresponding to those *Agents of Control*.

In this section, the description of **Data gateway** configuration is given. By default, this module is not enabled for live video transmitting to *Additional workplaces/Additional workplaces of CSC.* In order to enable Data gateway, set the **View live video through the gate** in the **Monitoring** interface object settings panel – see Configuring the Monitoring interface object.

Data gateway object configuration is performed as follows:

1. Create the **Data gateway** object based on the **Computer** object on the **Hardware** tab of the **System settings** dialog box (1).



2. In the **Local port** field enter the number of the port in the system for connection of *Additional workplace/ Additional workplace of CSC* (**2**).
3. In the **Remote IP-address** field enter IP-address of the *Agent of Control* (**3**).
4. In the **Remote port** field enter the standard port of the *Agent of Control* intended to transmit live video (**4**). Do not change the default value in most cases. It is to be changed only if by some reason the system uses intermediate server with port forwarding.
5. Click **Apply** (**5**).

Data gateway configuration is completed.

9 Configuring the Monitoring fault tolerance

To configure the *Monitoring* fault tolerance, do the following:

1. Configure the main *Server of Control* (see Configuring Server of Control).
2. Configure the *Agent of Control* (see Configuring Agent of Control) and set the **Partition of Control** connection to the main *Server of Control* (see Configuring communication between Agent Of Control and Server Of Control).
3. Create the second **Partition of Control**, configure in the same way, but with a different **Partition of Control** ID (see Configuring the Partition Of Control unique ID).
4. Configure a backup *Server of Control* (see Configuring Server of Control).
5. When configuring the second **Partition of Control**, set the connection parameters to the backup *Server of Control* (see Configuring communication between Agent Of Control and Server Of Control).

> **Attention!**
>
> If the list of cameras for tracking was added when configuring the first **Partition of Control** (see Configuring the camera list), then to add the same cameras to the second **Partition of Control**, it is necessary to change the **MonitoringReserving** key value to **1** in the Windows registry (for details, see Registry keys reference guide. for more information about working with the registry, see Working with Windows OS registry).

The *Monitoring* fault tolerance is configured.

10 Configuring the special mode of Monitoring operation with ACFA Intellect

On this page:

10.1 General information about special mode of *Monitoring* operation with *ACFA Intellect*

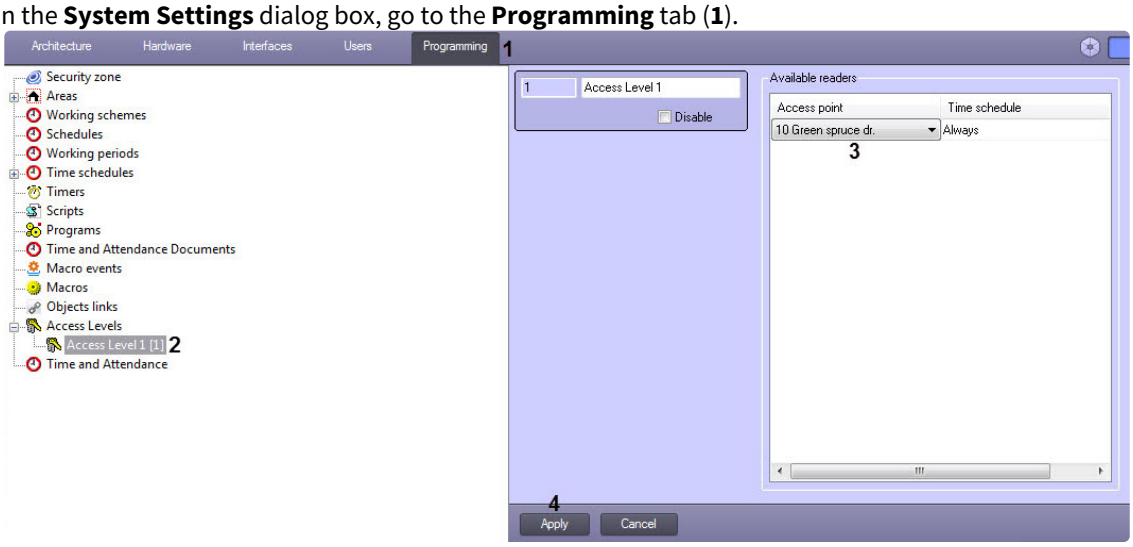
The special mode of *Monitoring* operation with *ACFA Intellect* allows to provide access to the object with the installed *Agent Of Control* using the user's access card, and to monitor the object status on the *Server Of Control*. This operating mode is relevant if the *Monitoring* and *ACFA Intellect* are not combined into a single system with a distributed architecture.

10.2 Configuring the special mode of *Monitoring* operation with *ACFA Intellect* on the *Server Of Control* side

The special mode of *Monitoring* operation with *ACFA Intellect* is configured on the *Server Of Control* side as follows:

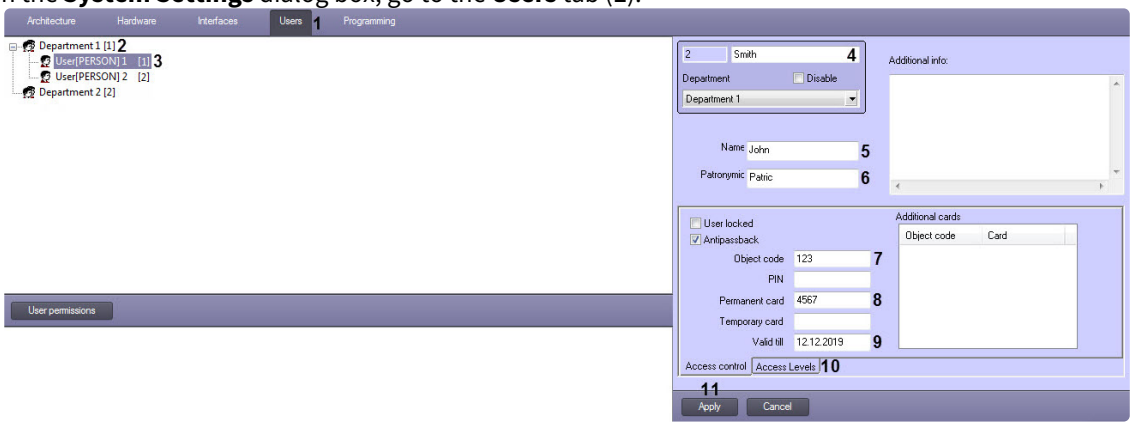
1. Create an **AccessByCardEnable** string registry key and set **1** as its value (for details, see Registry keys reference guide, for more information about working with the registry, see Working with Windows OS registry).
2. Create the necessary number of access levels, which include one or more *Partitions Of Control* of the corresponding *Agent Of Control* objects, the access to which should be obtained. Do it as dollows:

a. In the **System Settings** dialog box, go to the **Programming** tab (**1**).



b. In the object tree, create an **Access Level** object (**2**) on the basis of the **Access Levels** object.
c. On the settings panel of this object, specify one or more access points to which the *Partitions Of Control* on *Server Of Control* correspond (**3**).
d. Click **Apply** (**4**).

3. Create the necessary number of users who will be able to access objects, and assign an access card and access level to each user. Do it as dollows:
   a. In the **System Settings** dialog box, go to the **Users** tab (**1**).

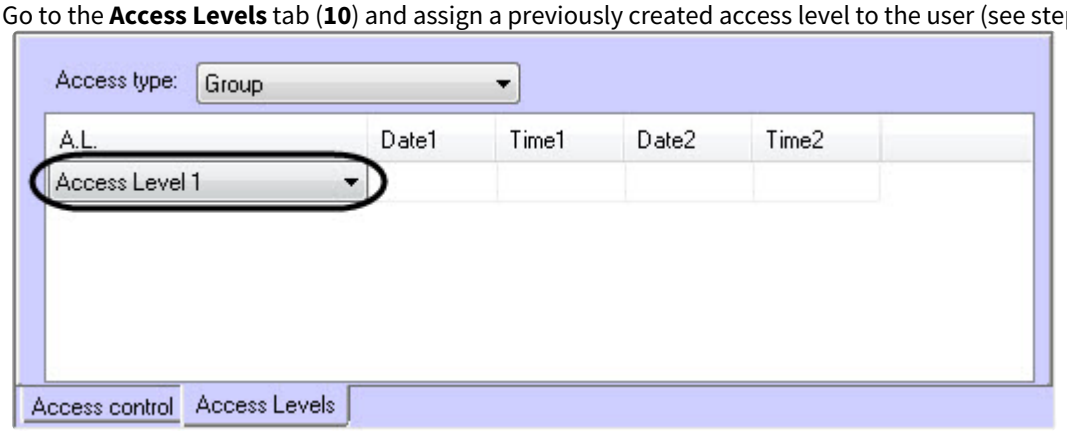


b. In the object tree, create a **Department** object (**2**), and then create a **User** object (**3**) on its basis.
c. On the settings panel of the **User** object, specify the following parameters:
a. In the field (**4**) enter the last name of the user.
b. In the **Name** field (**5**), enter the first name of the user.
c. In the **Patronymic** field (**6**), enter the middle name of the user.
d. In the **Object code** field (**7**), enter the room code.
e. In the **Permanent card** field (**8**) enter the card number.

> **Attention!**
>
> Both **Object code** and **Permanent card** fields should be filled in.

f. If necessary, in the **Valid til** field (**9**), specify the date upon which access to the object will be restricted.

g. Go to the **Access Levels** tab (**10**) and assign a previously created access level to the user (see step 2).



h. Click **Apply** (**11**).

> **Note**
>
> Similar actions can also be performed using the *Access Manager* module, which is part of the *ACFA Intellect* software package (see Working with the Access Manager software module).

Configuring the special mode of *Monitoring* operation with *ACFA Intellect* on the *Server Of Control* side is complete.

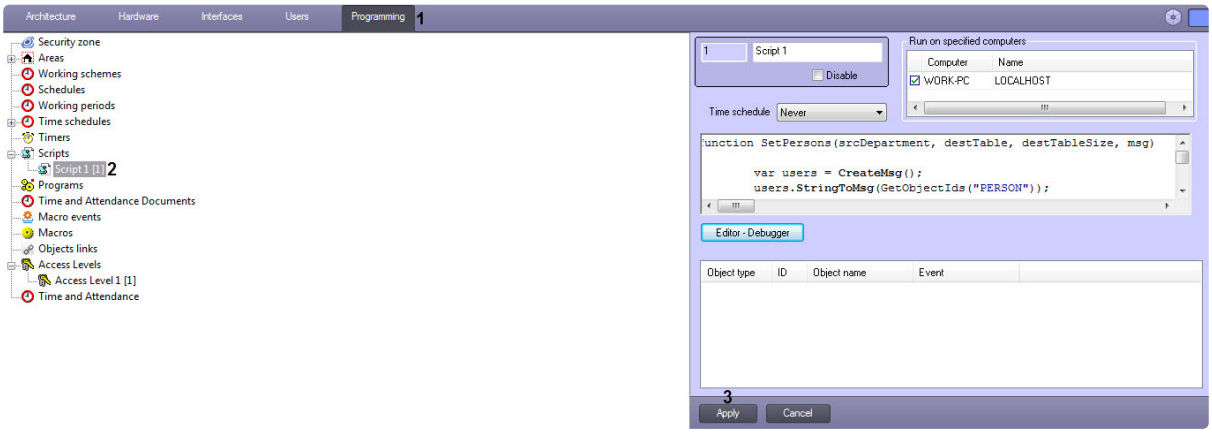
10.3 Configuring the special mode of *Monitoring* operation with *ACFA Intellect* on the *Agent Of Control* side

The special mode of *Monitoring* operation with *ACFA Intellect* is configured on the *Agent Of Control* side as follows:

1. Create an **AccessByCardEnable** string registry key and set **1** as its value (for details, see Registry keys reference guide, for more information about working with the registry, see Working with Windows OS registry).
2. Install *ACFA Intellect* (see ACFA Intellect Installation Guide).

> **Attention!**
>
> The following is an example of configuring the interaction between the *Monitoring* and the *Rovalant (A6, A16)* integration module, which is part of the *ACFA Intellect* software package. The configuration guide for the *Rovalant (A6, A16)* integration module is available only in the Russian documentation for *ACFA Intellect*. Instead of the *Rovalant (A6, A16)* integration module, you can use any other integration module that supports user entry into the controller.

3. Configure the *Rovalant (A6, A16)* integration module.
4. In the **System Settings** dialog box, go to the **Programming** tab (**1**).



5. To transfer the user data from the *Server Of Control* side to the *Agent Of Control* side, it is necessary to create script №1 in the object tree on the basis of the **Scripts** object (**2**) by copying the contents of an example of this script (see Sample script for configuring the interaction between the Monitoring and the Rovalant (A6, A16) integration module).
6. To monitor the object status on the *Server Of Control* side, it is necessary to configure the alarm group (see Configuring alarms for monitoring the object state on the Agent Of Control side). As a result of this configuration, the script №2 will be created.

> **Attention!**
>
> If an integration module other than *Rovalant (A6, A16)* is used, it is necessary to modify the script examples for the corresponding integration module.

> **Note**
>
> For more information on creating scripts, see The Script object. Programming using the JScript language.

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

Configuring the special mode of *Monitoring* operation with *ACFA Intellect* on the *Agent Of Control* side is complete.

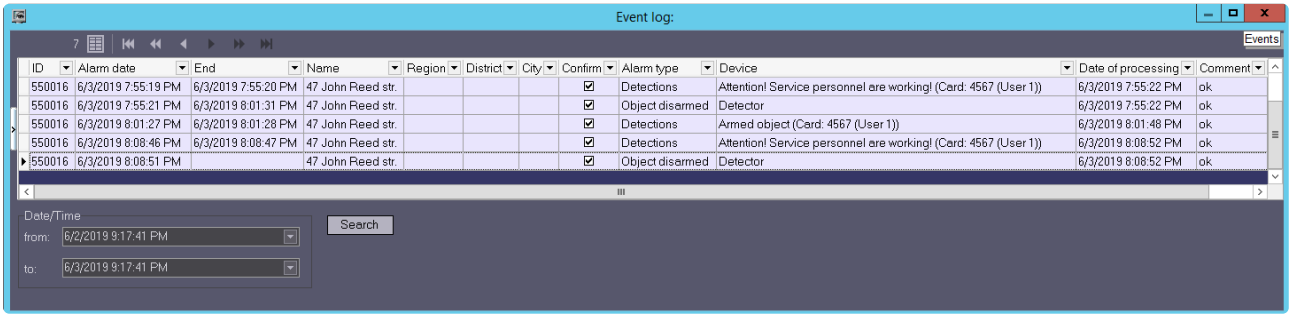
10.4 Operating procedure

At startup, and then every 15 minutes, *Agent Of Control* sends the hash of existing users to *Server Of Control*. Initially, there are no such users. At startup, *Server Of Control* receives the hash of all objects including users from the *Intellect* core, and puts them in a list that is updated if objects are edited or deleted. *Server Of Control* compares the user hash received from *Agent Of Control* with the value from the list and, if there is a mismatch, requests new data, and then transfers it to *Agent Of Control*. *Agent Of Control*, upon receiving this data (hash + configuration), updates the information about the users and generates the **SPR_DATA_UPDATED** event, which is processed in script №1. As a result, the users with the right to access the corresponding *Agent Of Control* will be loaded into the memory of the *Rovalant (A6, A16)* controller and will be able to access the object upon presenting of their access card.

Also at startup, and then every 15 minutes, *Agent Of Control* sends a **GET_OBJECT_STATE** event to the *Intellect* core. This event is processed in script №2, which generates an **OBJECT_STATE_INFO** event with the object status in the **state** field and the user's access card number used when arming/disarming the object in the **card** field. When arming an object using the user's access card, this script generates an **OBJ_ARM** event (alarm type: **Armed object**). When disarming an object using the user's access card, the same script generates the **OBJ_DISARM** event (alarm type: **Attention! Service personnel are working!**) and activates a long alarm **Object disarmed**.

> **Note**
>
> Only the user access card numbers are stored on the *Agent Of Control* side, the users' full names are not available. Therefore, in order to obtain the users' full names by the access card numbers, *Server Of Control* queries the *Intellect* database on the *Server Of Control* side.

As a result, when the access to an object is received, the access card number and the full name of the user who gained the access is displayed in the *Event log* as an additional information (see Event log).

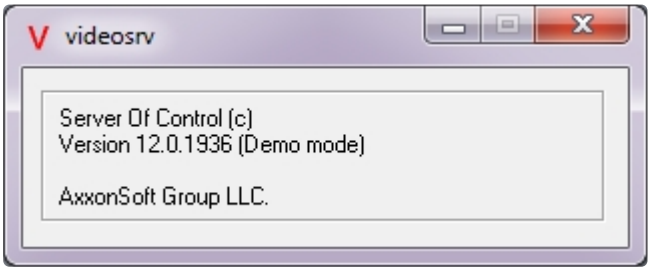


11 Data Loader for Monitoring

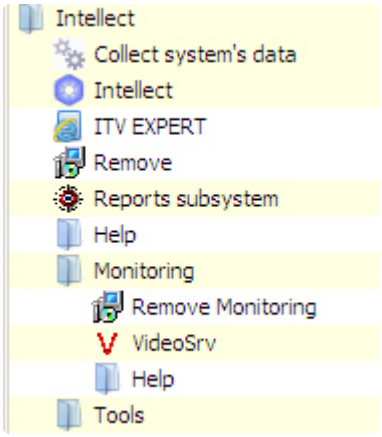
11.1 Server of Control communication module

Server of *Control* is a communication module that is responsible for receiving information from objects. The icon of the module (a red "V" symbol) is shown in the toolbar, in the lower-right corner of the screen.

If you double click on the icon, the window shown in the following figure opens.

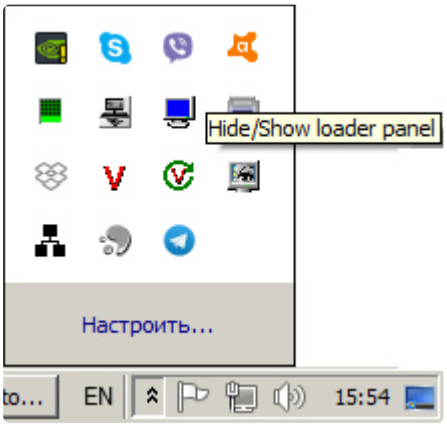


Server of *Control* starts automatically. If *Server* of *Control* has been stopped by mistake or any other reason, it can be restarted from **Start** – **All programs** – **Intellect** – **Monitoring** – **VideoSrv** menu.

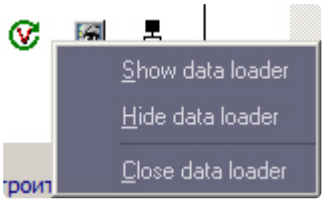


11.2 Data Loader

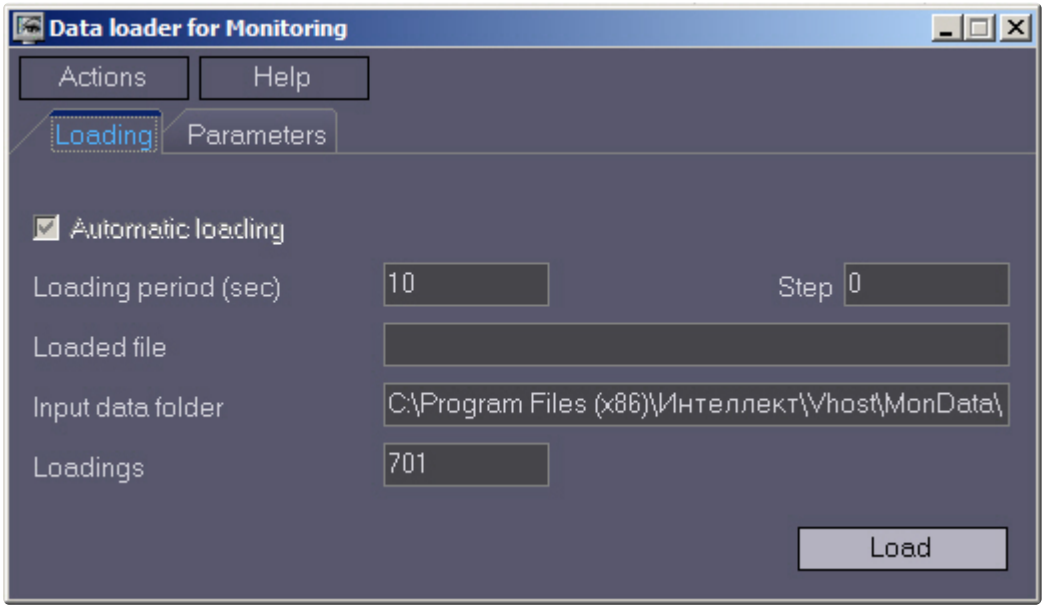
Server of *Control* creates files that contain object status information and puts them in the exchange folder. The files are then loaded from the folder to the database by the *Data loader for Monitoring* module. The icon of the module (a "monitor" symbol) is shown in the toolbar, in the lower-right corner of the screen.



If you right-click on this icon, a context menu opens.



If you select the **Show data loader** menu item, the **Data loader for Monitoring** window opens.



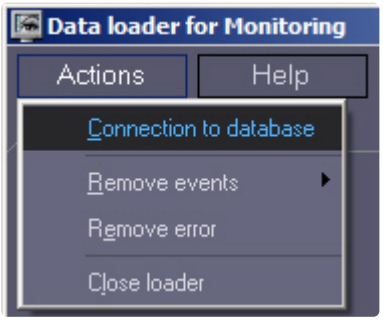
This window contains the following parameters:

1. **Input data folder**: The path to the folder that contains incoming files from *Server* of *Control*.
2. **Loading period (sec)**: The time (in seconds) between two consecutive loads of incoming files from *Server* of *Control* into the database. This parameter applies to non-alarm messages. Alarm messages are recorded to the database immediately. Each time after data is loaded into the database, the system sends to the **Log Panel** interface component a data update request. The Log Panel refreshes the information from the database every minute.
3. **Automatic loading**: If you select this check box, data is loaded automatically. Otherwise, the load starts only when you click **Load**.

4. **Loaded file**: This field shows the name of the file being processed, or an error message if an error occurred while loading the data.
5. Message files received from *Server* of *Control* are processed in several steps. The current step is shown in the **Step** field.

11.3 Connecting to the database

To configure the database connection string, select the **Connection to database** item in the **Actions** menu.

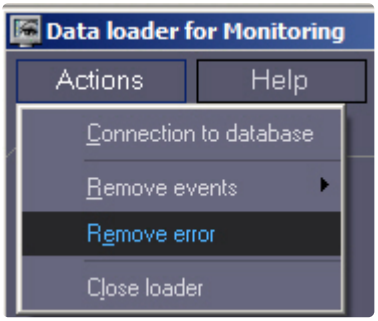


Attention!

If the location of the MonitorSSTV database changes from local to remote, then it is necessary to set the **0** value for the **UseBulkInsert** registry, if it changes from remote to local, then set the **1** value (for details, see Registry keys reference guide. for more information about working with the registry, see Working with Windows OS registry).

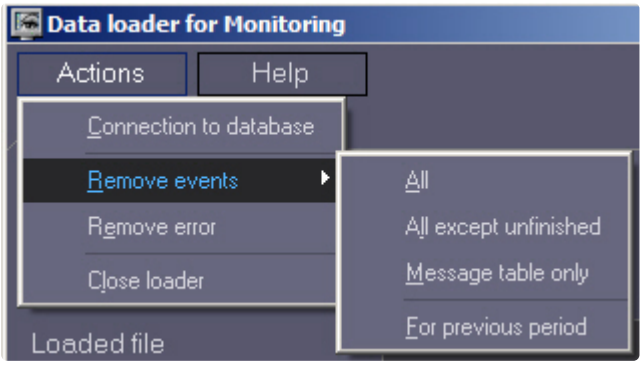
11.4 Removing errors

If there was a failure while loading data, you cannot close the program in a usual way, because the loading process cannot be interrupted. To close the program, use the **Remove error** menu item.



11.5 Removing events from the database

The **Remove events** menu item allows you to clear database. You can use the following modes:

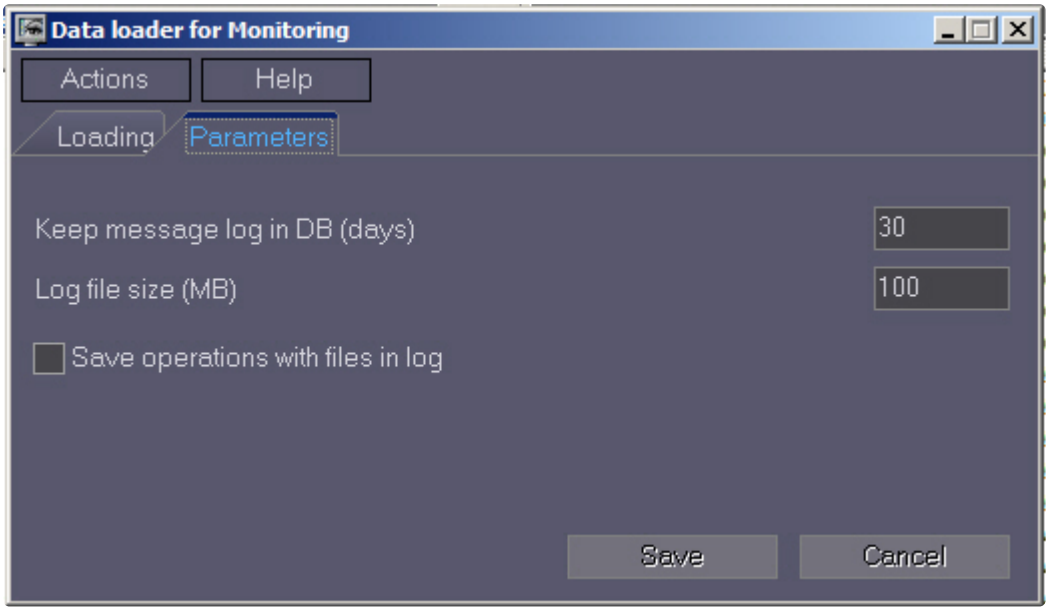


1. **Full** – Clears the database from alarms completely.
2. **All except incomplete** – Clears the database from alarms completely, but leaves the information on the start of the alarm for those alarms that did not yet end (long-term alarms).
3. **Message table only** – Clears the message log. This allows you to decrease the size of the database. In **Settings** tab, you can specify how long messages are kept in the log (see Setting the log storage period).
4. **For the period** – Clears the data for a specified period.

11.6 Setting the log storage period

If you want to specify how long the *Data loader* messages are kept in the log (event log), go to the **Data loader for Monitoring** window and then to the **Parameters** tab.

The data loader's event log is stored in the <*Intellect* software installation folder>\VHost\MONITOR\LOADER\LoaderSSTV_L_M.log, where M is a month.



1. **Keep messages log in DB (days)**: You can specify for how long will the data be kept in the MonitorSSTV database tables.
2. **Log file size (MB)** *:* You can specify the file size for the data loader's event log (in megabytes). After this limit is reached, the log file is archived.
3. **Save file operations in log**: This allows you to save details for the data loader's file operations in the data loader's event log.

11.7 Configuring automated video clip loading

To enable automated video clip loading, set the **FileQueryEnable** key in the Windows registry to 1 and specify folder to share data with third party system in the **FileQueryPath** key (see Registry keys reference guide for more details on the key and the Working with Windows OS registry section of *Intellect software. Administrator's Guide* for more details on how to operate registry keys). Restart the computer to ensure the changes applied.

Note.

The **C:\Query** folder is set by **FileQueryPath** key by default.

Important!

Specify different folders in **FileQueryPath** key if automated video clip loading is enabled both on *Server of Control* and *Additional workplace* simultaneously.

Note.

When *videosrv.exe communication module* starts at the *Server of Control,* the folder specified in the **FileQueryPath** key is automatically created with the following subfolders:
In – the folder for request files;
In\Work – the service folder for request files;
OutSuccess – the folder to place request files in after successful load of the video clips;
OutError – the folder for incorrect request files or request files with absent mandatory parameters;
OutFail – the folder to place correct request files in if video clip could not be loaded for some reason.

Important!

At *Additional workplace*, create the folder specified in the **FileQueryPath** key with all subfolders described above manually.

11.8 Specifying the export directory

An export directory is automatically created on the *Server Of Control* and on the *Central Server Of Control* to save all requested frames and video fragments. By default, the export directory is located at *DISK:\Export*, where DISK is the drive on which the operating system is installed. You can change the path to this directory using the **ExportPath** registry key (see Registry keys reference guide). Then the *Monitoring reports* and *Search in archive* modules can work with this data storage.

If necessary, you can configure saving frames and video fragments in the Monitoring database on the *Server Of Control* (MonitorSSTV) and the *Central Server Of Control* (ServerSSTV) instead of the export directory. For this purpose, it is necessary to set the string parameter of the **KeepVideoDataInBase** registry key equal to the number of days of storage in the database (see Vertical solutions). The data is stored in the video_data table.

To restore data from the Monitoring database to the export directory, use the RestoreExportDir.exe utility that is installed on the *Server Of Control* and on the *Central Server Of Control* at the <Intellect installation directory>\Vhost\SYSTEM path. To start restoring data, click the **Restore export folder** button.


RestoreExportDir
Restore export folder
Records processed : 8 out of 8

12 Configuration of the Monitoring interface

12.1 General information about the Monitoring interface

The Monitoring interface is accessible through the following interface elements

1. **Monitoring**.
2. **Search in archive**.
3. **Monitoring Reports**.

These objects are created based on the **Display** object, in the **Interfaces** tab of the **System settings** dialog box. It is recommended to create these objects on the basis of different **Display** objects.

Interface objects are available at the following *Monitoring* installation types: *Server of Control*, *Additional workplace*.

> **Note.**
>
> Operations with interface objects are described in the Monitoring. Operator's Guide document.

12.2 Configuring the Monitoring interface object

> **Attention!**
>
> Before creating the **Monitoring** object, create and configure the **Server Of Control** object (see Creating necessary Server Of Control objects).

To configure the **Monitoring** interface object:

1. In the object tree, select the **Monitoring** object. On the right side of the **System settings** dialog box, the settings panel of the relevant object is displayed.

2. Set the checkboxes next to the alarm groups that should be visualized (**1**). The **Extra 1** and **Extra 2** groups of alarms can be renamed.
3. If it is necessary to display the **Owners panel** component on the screen, set the **Owners panel** checkbox and specify the component position coordinates on the monitor screen. Also, from the **Monitor** drop-down list, select the number of the physical monitor, which coordinates should be specified (**2**). You can also set the scaling of objects from 100% to 500%.

> **Note**
>
> If the scaling parameter exceeds 110%, then the high resolution icons will be displayed on the object, and the Courier New font will be used for the text in the object title, otherwise—MS Sans Serif.

4. If it is necessary to display the **Control panel** component on the screen, set the **Control panel** checkbox and specify the component position coordinates on the monitor screen. Also, from the **Monitor** drop-down list, select the number of the physical monitor, which coordinates should be specified (**3**). You can also set the scaling of objects from 100% to 500%.

> **Note**

If the scaling parameter exceeds 110%, then the high resolution icons will be displayed on the object, and the Courier New font will be used for the text in the object title, otherwise—MS Sans Serif.

5. If it is necessary to display the **Log panel** component on the screen, set the **Log panel** checkbox and specify the component position coordinates on the monitor screen. Also, from the **Monitor** drop-down list, select the number of the physical monitor, which coordinates should be specified (**4**).
6. Set the **Non-empty Comment field** checkbox, if it is necessary for the operator to comment on this alarm and/or their actions, when accepting the alarm (**5**). This comment can be viewed later in the event log, as well as the name of the operator who received the alarm.
7. By default, objects can be filtered by **Alarm** and **Failure** events as well as by **Connected** and **Disconnected** states. Clear the **Use filter by events** checkbox to disable this feature (**6**). As a result, the corresponding drop-down list becomes disabled.
8. When you try to view live video and want to display a warning that it can create the critical load on the channel, set the **Warning when watching live video** checkbox (**7**).
9. If *Agents Of Control* and *Additional workplaces* are in different subnets and the *Monitoring* components are not in a distributed system configuration in *Intellect* object tree and **Data gateway** is in use for transmission of live video to *Additional workplaces*, set the **Viewing live video through gateway** checkbox (**8**).

   Note

   For the details about the **Data gateway**, see Creating and configuring Data gateway.

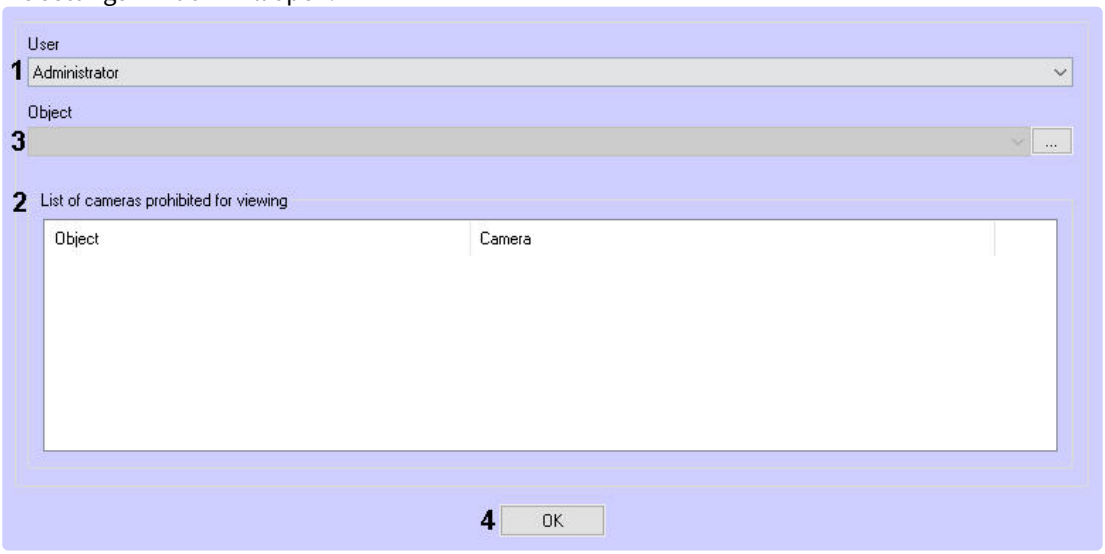
10. To add the **All cameras of *Partition Of Control*** item to the object's **Video image playback** context menu which enables viewing video from all cameras of the selected *Partition Of Control*, set the **Viewing live video from all cameras (add.)** checkbox (**9**).
11. In the **Video stream speed** field, enter the number of frames per second of the video image when viewing live or archive video (**10**). This parameter is used to limit the data flow between the *Server Of Control* and the *Agent Of Control* (for example, in case the communication channel has low bandwidth).

    Note

    - The **Video stream speed** setting works for the archive video only with CamMonitor.ocx 4.11.0.1766 or later versions.
    - If the archive is recorded with the H.264 codec and the video stream speed is set to more than **0** frames per second, then the archive video will be played back only by reference frames.
    - If the value of the video stream speed is **0**, then the live and archive video will be played back without scaling.

12. Select the required compression rate for the live video from the **Compression** drop-down list (**11**).
13. If it is necessary to set the cameras for which the user should be prohibited from viewing live video, do the following:
    a. Click the **Cameras** button (**12**).

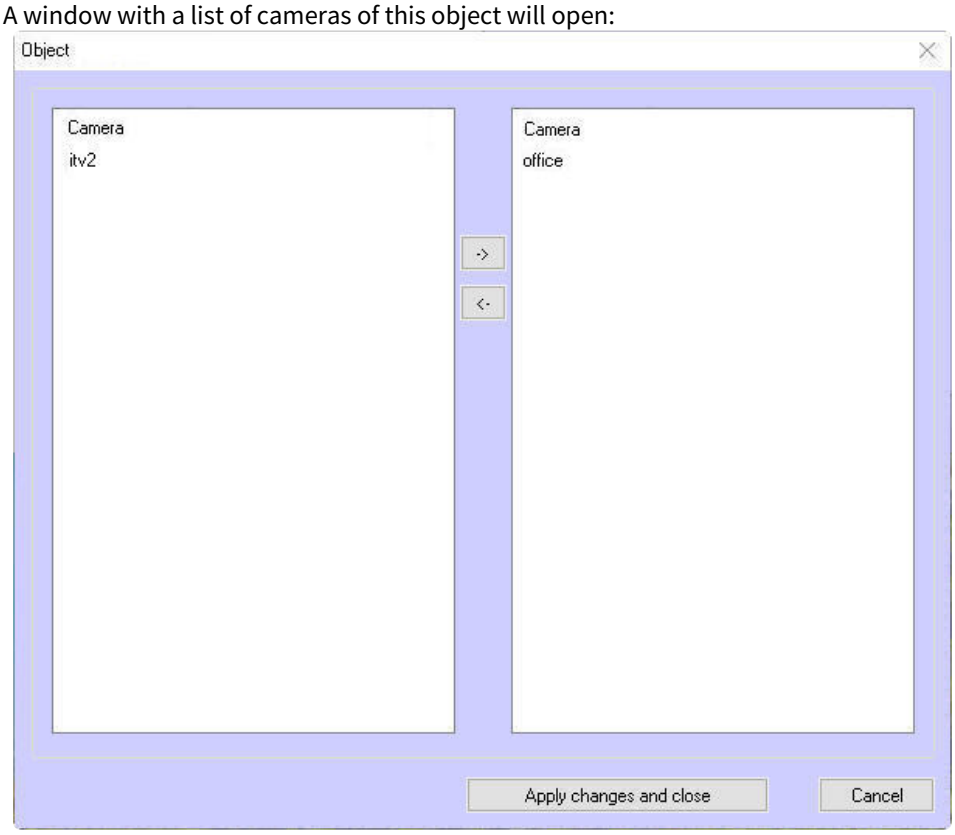
b. The settings window will open:



c. In the **User** drop-down list (**1**), select the user to whom the prohibition should be applied.
d. The **List of cameras prohibited for viewing** field (**2**) displays the cameras prohibited from viewing for the selected user. To add a camera to the list, select the required object from the **Object** drop-down list (**3**) and click the  button.

> **Note**
>
> The **Object** list contains only those objects that have cameras.

e. A window with a list of cameras of this object will open:



f. In the left part of the window, select the cameras that should be prohibited from viewing, and move them to the right part of the window using the  button. Then click the **Apply changes and close** button.

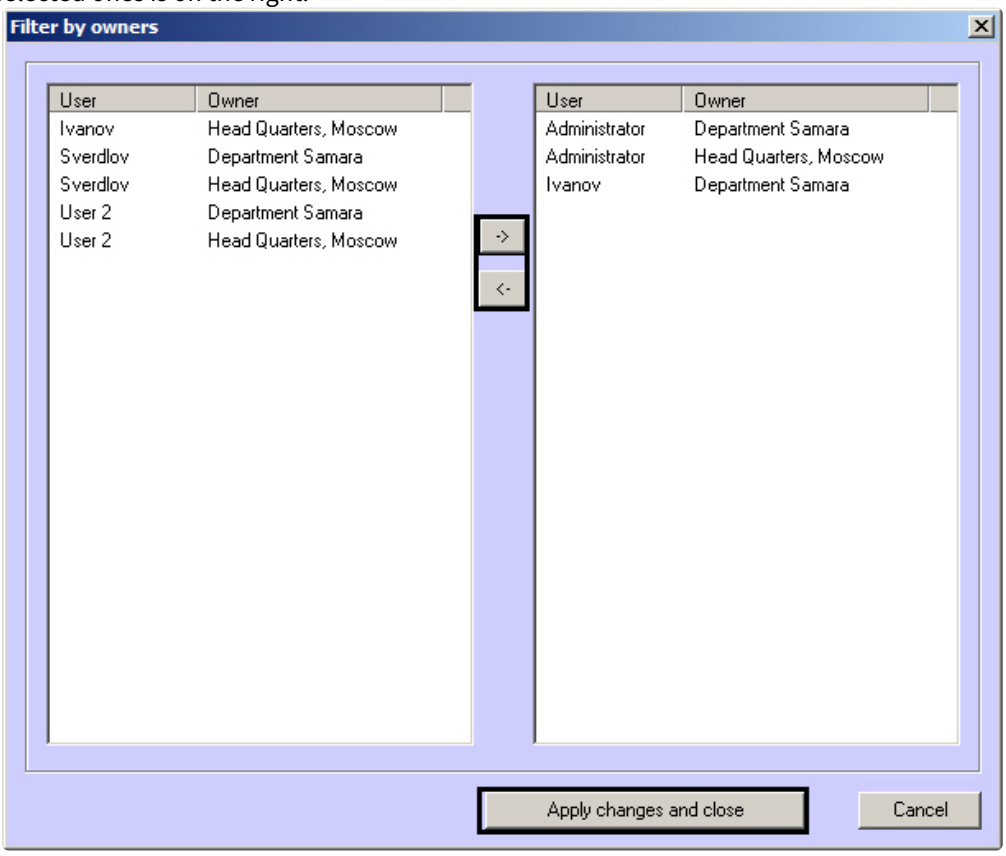
> **Note**
>
> To cancel the prohibition, select the camera in the right part of the window and click the  button.

g. Click the **OK** button (**4**).

> **Note**
>
> - If a filter by owner is used for the **Monitoring** interface object, then its value is taken into account when configuring prohibited cameras.
> - If the user selects a camera that is not prohibited from viewing live video in the **Monitoring** interface, they can enter the camera's functional menu and select a camera prohibited from viewing using the Camera menu item. To prevent this from happening, it is necessary to hide the Camera menu item using the MENU_CAMS_DISABLE_OPTION registry key (see Registry keys reference guide).
> - When adding a camera to the list of prohibited from viewing, the camera is not automatically removed from the previously created screens to which this camera was added.

14. If specific owners are to be available for specific users on the **Owners panel**, then set the filter by owners:
    a. Click the **Filter** button (**14**).

b. The **Filter by owners** window appears. The list of available user-owner pairs is on the left, the list of selected ones is on the right.



> **Note**
>
> The list of owners is set on the **Control Panel**—see Regulatory and reference information. Users and their rights are configured in the **Users** tab of the **System settings** dialog box—for details, see Limiting access to the system objects administration, control and viewing functions.

c. Move the pairs between the lists using the <- and -> buttons.
d. When the list of user-owner pairs is formed, click the **Apply changes and close** button.

15. Selected pairs of users and owners are displayed in the table (**13**).
16. Click the **Apply** button (**15**).

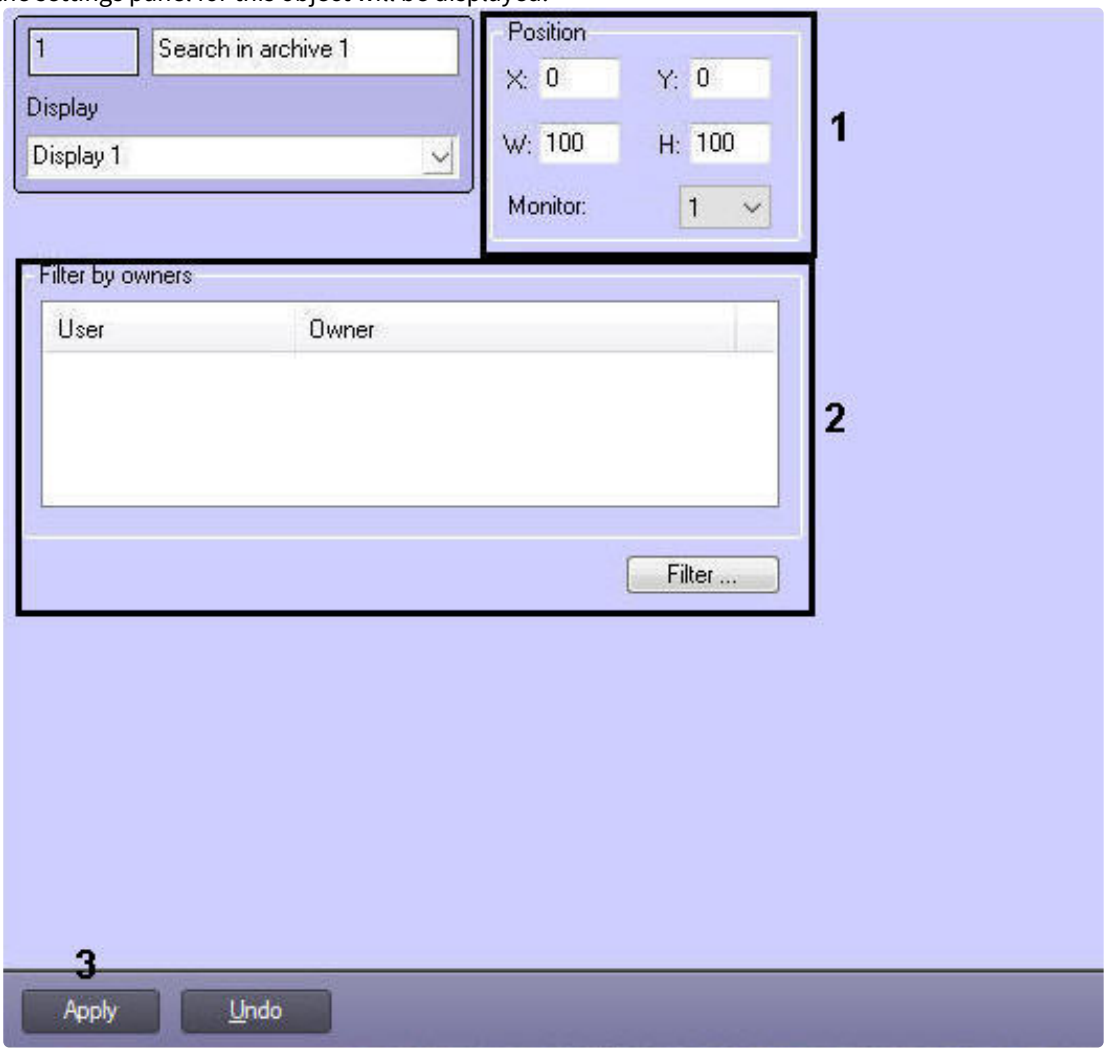
Configuration of the **Monitoring** interface object is now complete.

When a screen for which the **Monitoring** object has been created is selected in *Intellect,* the **Monitoring** interface window is displayed.

12.3 Configuring the Search in archive object

The **Search in archive** interface object is configured as follows:

1. Select the **Search in archive** object in the objects tree. In the right part of the **System settings** dialog box, the settings panel for this object will be displayed:



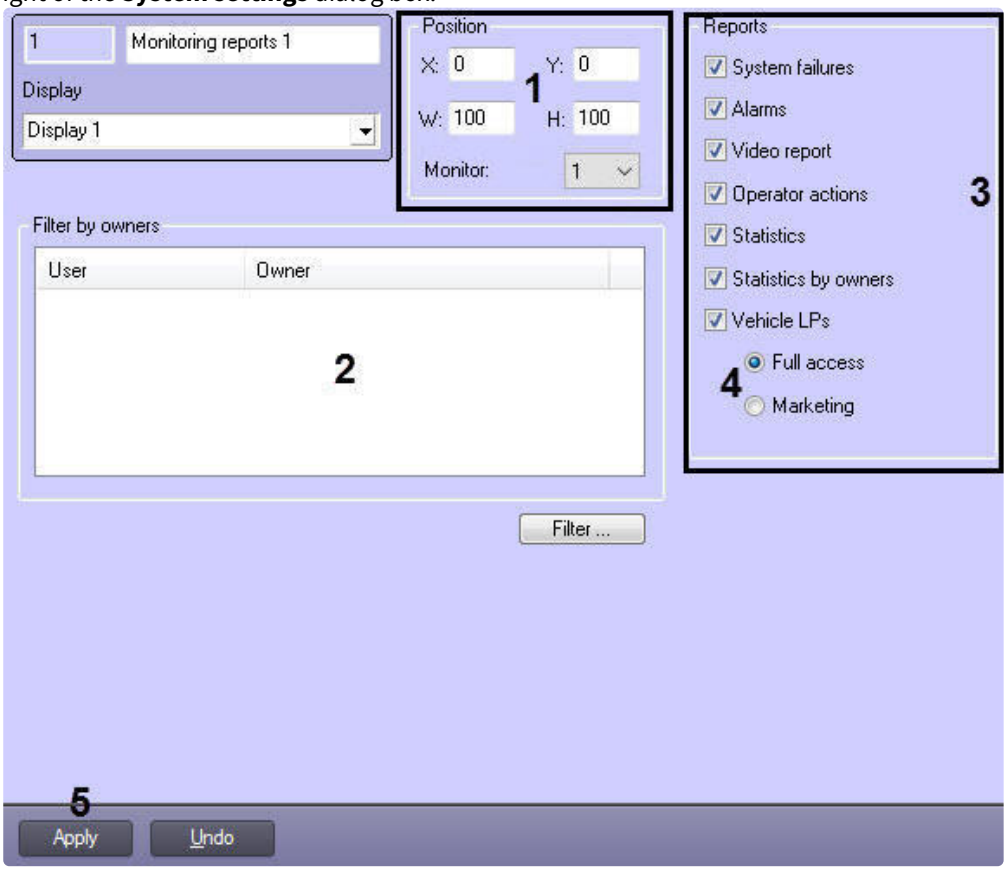
2. From the **Monitor** drop-down list (**1**), select the number of the physical monitor, which coordinates should be specified. Specify the **Search in archive** window position coordinates on the screen of the selected monitor.
3. Set up a filter by owners (**2**) by analogy with the **Monitoring** interface object—see Configuring the Monitoring interface object.
4. Click the **Apply** button (**3**).

When you select the **Display** object on the basis of which the **Search in archive** object was created in *Intellect,* the **Search in archive** interface window will be visualized (see Search in archive).

12.4 Configuration of the Monitoring reports object

To configure the **Monitoring reports** object, do the following:

1. Select the **Monitoring reports** object in the objects tree. The settings panel of the object is displayed to the right of the **System settings** dialog box.



2. From the **Monitor** drop-down list (**1**), select the number of the physical monitor, which coordinates should be specified. Specify the **Monitoring reports** window position coordinates on the screen of the selected monitor.
3. Set the filter by owners similar to the one for the **Monitoring** object (**2**), see Configuring the Monitoring interface object.
4. By default, all reports are available for the operator. To hide some of the reports, clear the checkboxes next to them in the **Reports** group (**3**).
5. Select the type of access to the Vehicle LPs reports (**4**):
   a. **Full access**: all Vehicle LPs report types are available.
   b. **Marketing**: only the average time span at the gas station and number of vehicles reports are available, and the Vehicle LP field is restricted to three letters and a **%** character.
6. Click the **Apply** button (**5**).

Configuration of the **Monitoring reports** object is completed.

13 Configuring audio calls from the Monitoring interface

13.1 General information

Audio calls are supported between operators in a distributed configuration on the *Server Of Control*/*Agent Of Control* side. Audio calls are made using the **SIP-terminal** object. Physical SIP devices are not required.

> **Attention!**
>
> This functionality is only available in *Intellect* 4.11.2 or higher.

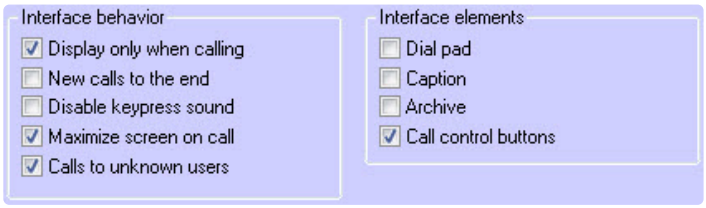
13.2 Configuring audio calls from the Monitoring interface

Configure audio calls from the **Monitoring** interface as follows:

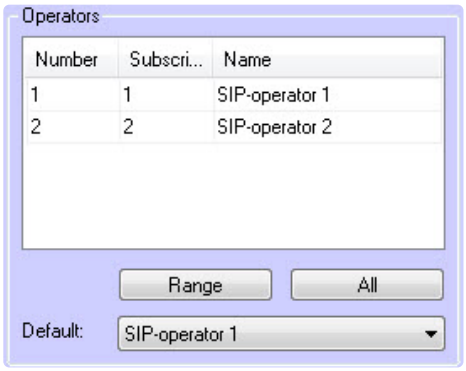
1. At the *Server Of Control* and *Agent Of Control* side:
   a. Create the **Audio card** object with the **Microphone** child object (see Audio subsystem configuration).
   b. Create the **Audio playback card** object with the **Speaker** child object (see Configuring audio playback).
2. At the *Server Of Control* side:
   a. Create the **SIP-terminal** object as a SIP-server in *Intellect* (see Configuring SIP-terminal).
   b. On the basis of the **SIP-terminal** object, create two **SIP-operator** child objects and for each of them specify the corresponding operator identification number (Configuring SIP-operators of the Intellect's SIP server).
   c. On the basis of the **SIP-terminal** object, create the **Address book** object and select the previously created SIP-operators (see Configuring address book of SIP-terminal).
   d. On the settings panel of each **SIP-operator**, select a previously created address book (see Configuring SIP-operators of the Intellect's SIP server).
   e. Create the **SIP-panel 1** interface object on the same **Display 1** object on which the **Monitoring** interface object was created (see Configuring the SIP-panel interface object).

   > **Note**
   >
   > Recommended coordinates of the SIP-panel: X = 40, Y = 40, W = 20, H = 21.

      i. On the **Basic settings** tab of the **SIP-panel 1** object, select the **SIP-terminal** as the terminal (see Basic settings of the SIP-panel interface object).
      ii. On the **Advanced settings** tab of the **SIP-panel 1** object, set the checkboxes as shown in the figure below (see Advanced settings of the SIP-panel interface object).



      iii. On the **Operator settings** tab of the **SIP-panel 1** object, configure the list of SIP-operators as shown in the figure below (see Operator settings of the SIP-panel interface object).

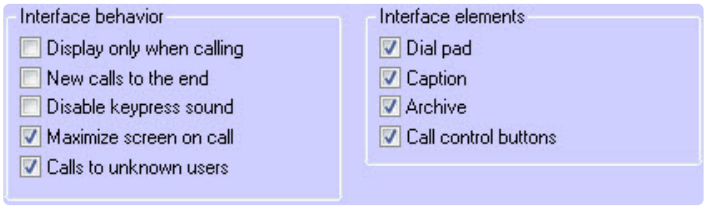


f. Create the **Display 2** object, which will be displayed only on the *Agent Of Control* side (see Assigning the displays to the operator workstations).

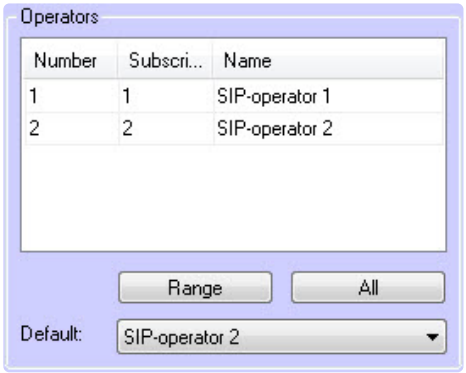
g. Create the **SIP-panel 2** child interface object.

   i. On the **Basic settings** tab of the **SIP-panel 2** object, select the **SIP-terminal** as the terminal (see Basic settings of the SIP-panel interface object).

   ii. On the **Advanced settings** tab of the **SIP-panel 2** object check the boxes as shown in the figure below (see Advanced settings of the SIP-panel interface object).



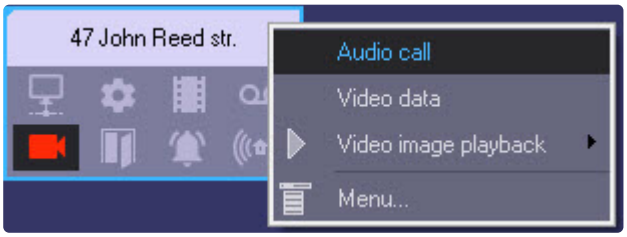
   iii. On the **Operator settings** tab of the **SIP-panel 2** object, configure the list of SIP-operators as shown in the figure below (see Operator settings of the SIP-panel interface object).



h. On the settings panel of the **Computer** object, select the speaker and microphone of the SIP-operator (see Selecting speaker, microphone and camera for SIP-operator).

Configuring audio calls from the **Monitoring** interface is now complete.

As a result, the **Audio call** item will appear in the context menu of the object in the **Monitoring** interface. When you select this menu item, an audio call will be made to the operator who is on the computer with the corresponding object.

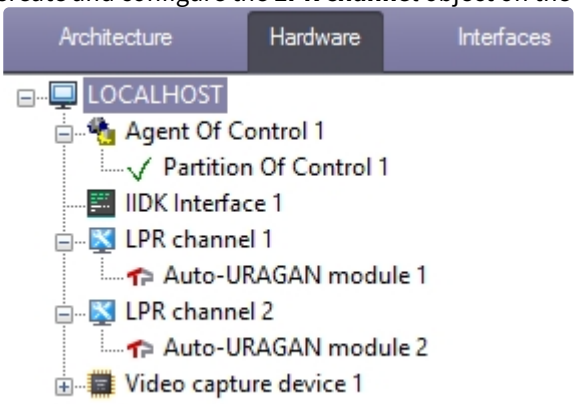

47 John Reed str.
Audio call
Video data
Video image playback
Menu...

14 Configuring special operation mode joint with Auto Intellect

14.1 Configuration on the Agent Of Control side

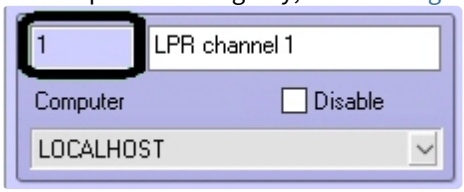
Configure special operation mode on *Agent Of Control* as follows:

1. Create and configure the **Agent Of Control** object on the **Hardware** tab (see Configuring Agent of Control).
2. Create and configure the **LPR channel** object on the **Hardware** tab (see Auto Intellect Guide).



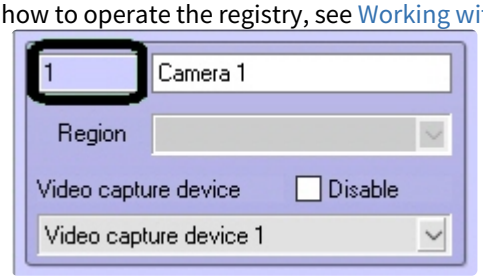
3. Create the **Partition Of Control** object based on the **Agent Of Control** object, then add to it the **LP recognized** events for entrance and exit (see Configuring the Partition Of Control object).

4. Create the **ULPR** section in the Windows registry if it is not created yet (see Registry keys reference guide. For more details on how to operate the registry, see Working with Windows OS registry).
5. In the **ULPR** section of the Windows registry create the **ULPRspecialProcessing** string parameter and set its value to **1** (see Registry keys reference guide. For more details on how to operate the registry, see Working with Windows OS registry).
6. In the **ULPR** section of the Windows registry create the **PlaceOfRecognitionN** string parameter, where **N** is the ID of the **LPR channel** object. This parameter corresponds to the point of recognition. Value **1** corresponds to entrance. Value **2** corresponds to exit (see Registry keys reference guide. For more details on how to operate the registry, see Working with Windows OS registry).



7. In the **ULPR** section of the Windows registry (see step 4) create the **CamOfRecognitionN** string parameter, where **N** is the ID of the **LPR channel** object. The value in this key should correspond to the ID of the **Camera** object specified in the **LPR channel** object settings (see Registry keys reference guide. For more details on

how to operate the registry, see Working with Windows OS registry).



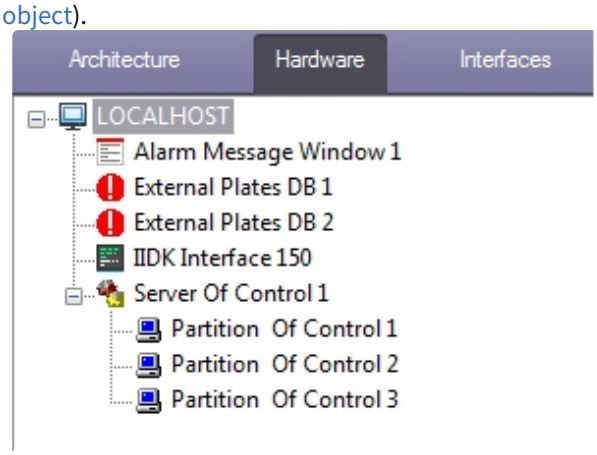
8. Restart the computer to apply the changes.

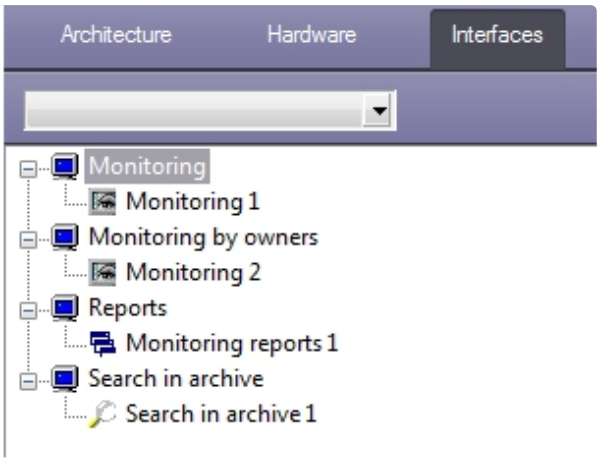
Configuring the special operation mode on the *Agent Of Control* side is now completed.

14.2 Configuration on the Server Of Control side

Configure the special operation mode on the *Server Of Control* side as follows:

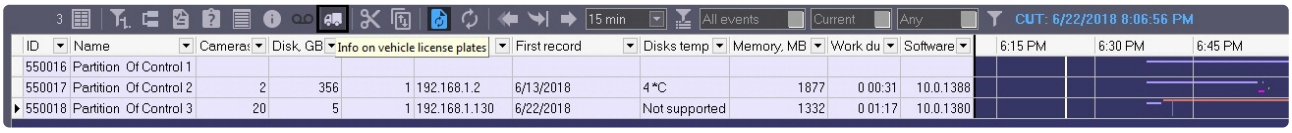
1. Create and configure the **Server Of Control** object on the **Hardware** tab (see Configuring Server of Control).
2. Create and configure one or several **External Plates DB** objects on the **Hardware** tab (see Connecting and setting up of the external LP number database).
3. Create and configure the **Monitoring** object on the **Interfaces** tab (see Configuring the Monitoring interface object).

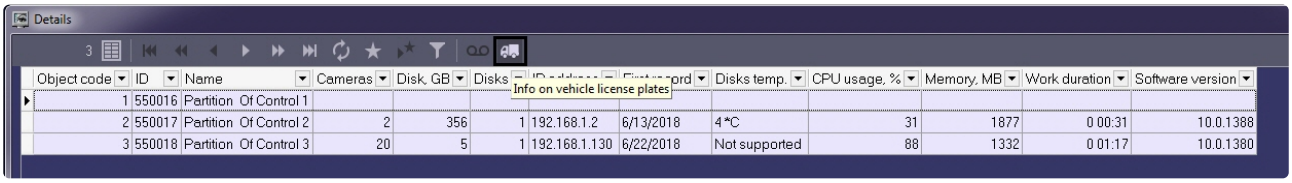




4. Create the **ULPR** section in the Windows registry if it is not created yet (see Registry keys reference guide. For more details on how to operate the registry, see Working with Windows OS registry).
5. In the **ULPR** section of the Windows registry, create the **ULPRspecialProcessing** string parameter and set its value to **1** (see Registry keys reference guide. For more details on how to operate the registry, see Working with Windows OS registry).
6. Restart the computer to apply the changes.

As a result, the **Info on vehicle license plates** button becomes available in the **Log panel** and **Details** window of the **Monitoring** interface. The **License plate search** window opens when you click this button (see Viewing recognized LPs).





Object code	ID	Name	Cameras	Disk, GB	Disks		Disks temp.	CPU usage, %	Memory, MB	Work duration	Software version
1	550016	Partition Of Control 1									
2	550017	Partition Of Control 2	2	356	1	192.168.1.2	4 °C	31	1877	0 00:31	10.0.1388
3	550018	Partition Of Control 3	20	5	1	192.168.1.130	Not supported	88	1332	0 01:17	10.0.1380

Note

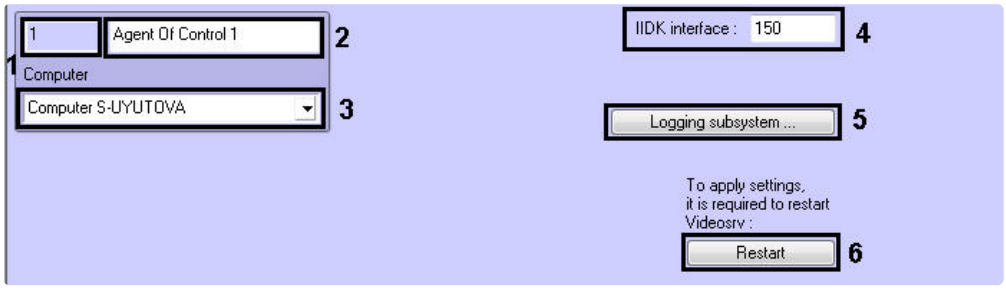
By default, the **LP found in the database** alarm is generated for the **Entrance** recognition point only. In order to generate alarm both on **Entrance** and **Exit** points, in the **ULPR** section of the Windows registry, create the **AlarmMsgOne** string parameter and set its value to **0** (see Registry keys reference guide. For more details on how to operate the registry, see Working with Windows OS registry).

Configuring the special operation mode on the *Server Of Control* side is now completed.

15 Appendix 1. Interfaces

15.1 Settings panel of the Agent of Control object

Settings panel of the **Agent of Control** object is given on figure.



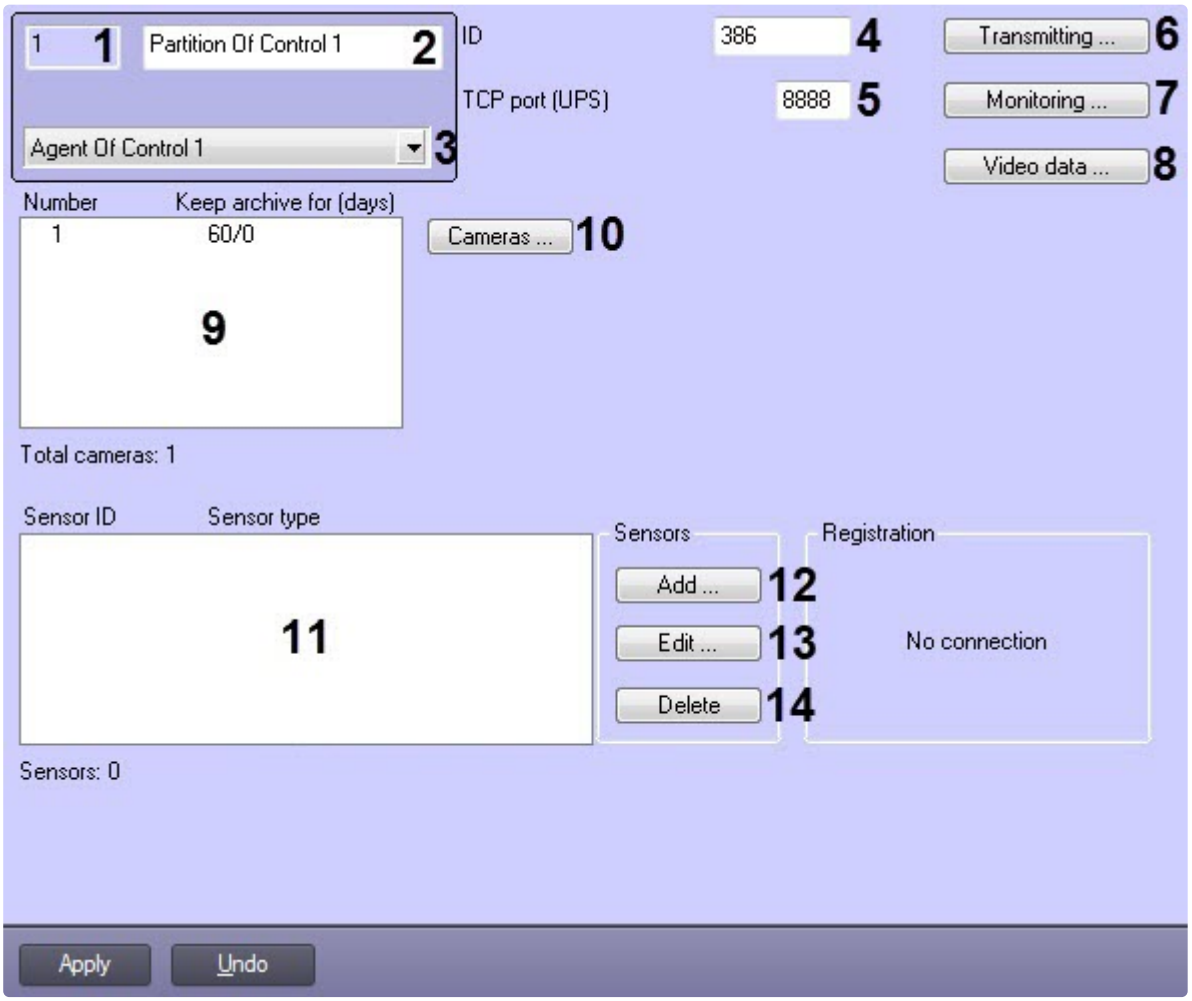
Description of the **Agent of Control** object settings panel elements is given in table.

#	Parameter	Method for setting the parameter value	Description	Type	Default value	Value range
1	Identifier	Automatically	Shows the identification number of the **Agent of Control** object in the system	Nonnegative integer	-	>=0
2	Name	Enter the value in the field	Shows the name of the **Agent of Control** object in the system	Latin, Cyrillic letters and service characters	Agent of Control	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	**Computer**	Is selected in the list	Assigns the parent **Computer** object for the **Agent of Control** object	Name of the **Computer** objects registered in the system.	Name of the parent **Computer** object	Depends on the number of the **Computer** objects in the system.

#	Parameter	Method for setting the parameter value	Description	Type	Default value	Value range
4	**IIDK interface**	Enter the value in the field	Sets the ID number of **IIDK interface** object used by the Agent of Control	Nonnegative integer	150	>=0
5	**Logging subsyste m...**	Click the button	Opens a dialog box for setting logging subsystem parameters	-	-	-
6	**Restart**	Click the button	VideoSrv communication module restarting	-	-	-

15.2 Settings panel of the Partition Of Control object

Settings panel of the **Partition Of Control** object is given on figure.



Description of the **Partition Of Control** object settings panel elements is given in table.

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
1	Identifier	Enter the value in the field	Shows the identification number of the **Partition of Control** object in the system	Latin, Cyrillic letters and service characters	-	-

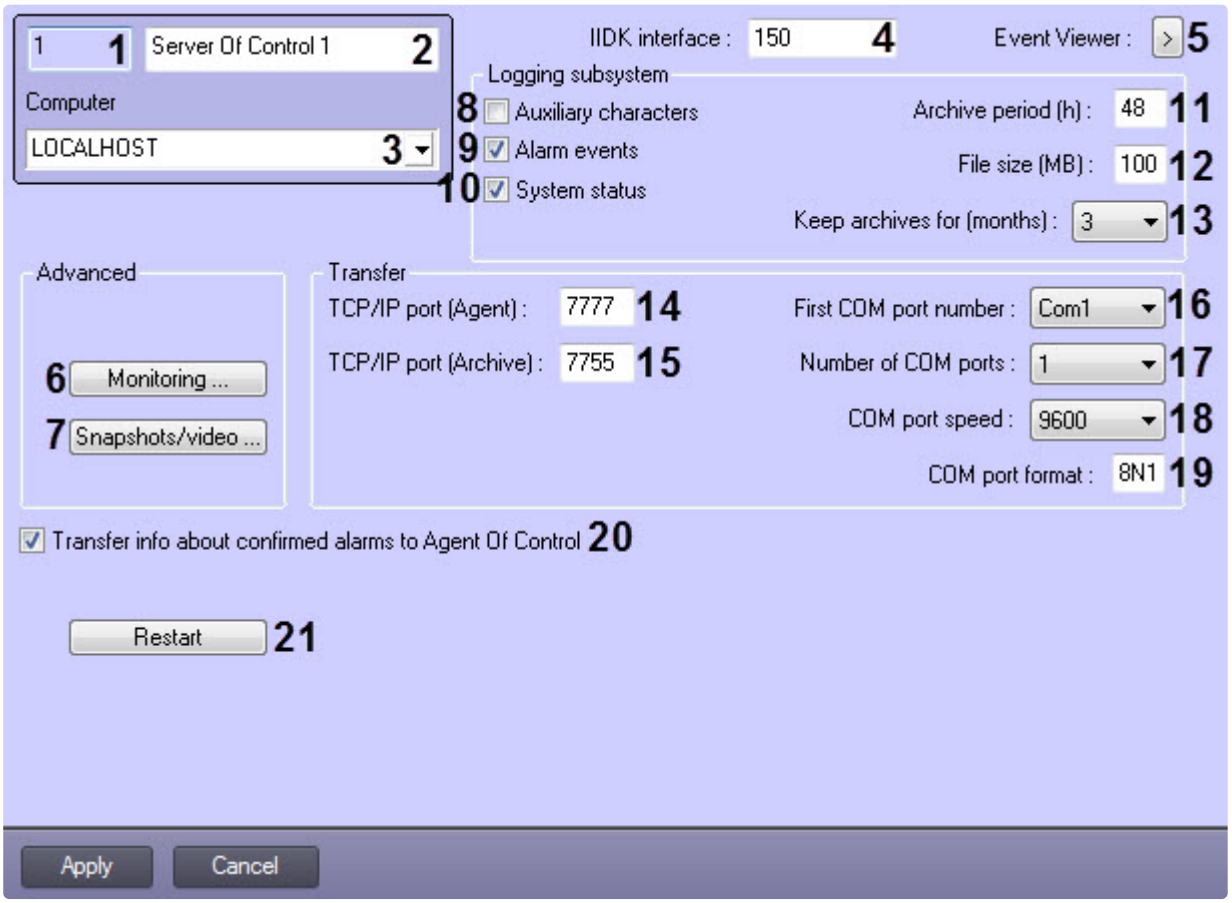
#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
2	Name	Enter the value in the field	Shows the name of the **Partition of Control** object in the system	Latin, Cyrillic letters and service characters	Partition of Control	A line representing a sequence of any symbols (letters, digits, service characters excluding characters: underscore "_", backslash "\", angle brackets ">" and "<", single quote "'"). Number of symbols – from 1 to 60.
3	Agent of Control	Is selected in the list	Assigns the parent **Agent of Control** object for the **Partition of Control** object	Names of **Agent of Control** objects registered in the system	Name of the parent **Agent of Control** object	Depends on the number of the **Agent of Control** objects in the system.
4	**ID**	Enter the value in the field	Sets the unique ID number for the object where *Agent of Control* is installed	Latin, Cyrillic letters and some characters	386	A line representing a sequence of any symbols (letters, digits, service characters excluding characters: space " ", underscore "_", backslash "\" and single quote "'"), not case-sensitive. Number of symbols – from 1 to 9.
5	**TCP port (UPS)**	Enter the value in the field	Sets the port on which to "listen" for UPS messages	Nonnegative integer	8888	from 1 to 60000

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
6	**Transmitting...**	Click the button	Opens a dialog box with settings for configuring the communication method between *Agent of Control* and *Server of Control*	-	-	-
7	**Monitoring...**	Click the button	Opens a dialog box for configuring alarm groups	-	-	-
8	**Video data...**	Click the button	Opens a dialog box for setting video data transferring configurations	-	-	-
9	Cameras	Using the **Cameras...** button	Displays the list of cameras whose state and archives are monitored by *Agent of Control* and operating with which shall be available from *Monitoring* software interface.	-	-	-
10	**Cameras...**	Click the button	Opens a dialog box for adding cameras for monitoring	-	-	-
11	Sensors	Using the **Add, Edit** and **Delete** buttons	Displays IDs and types of sensors whose state is monitored by *Agent of Control* and on whose triggering video data are sent to the Server of Control.	-	-	-

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
12	**Add...**	Click the button	Opens a dialog box for adding a sensor. In this dialog box one can also setup video data sending on the sensor triggering	-	-	-
13	**Edit...**	Click the button	Opens a dialog box for editing the sensor. This dialog box is similar to the one for adding a sensor	-	-	-
14	**Delete**	Click the button	Deletes sensor from the list	-	-	-

15.3 Settings panel of the Server of Control object

Settings panel of the **Server of Control** object is given on figure.



Description of the **Server of Control** object settings panel elements is given in table.

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
1	Identifier	Automatically	Shows the identification number of the **Server of Control** object in the system	Nonnegative integer	-	>=0

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
2	Name	Enter the value in the field	Shows the name of the **Server of Control** object in the system	Latin, Cyrillic letters and service characters	Server of Control	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	**Computer**	Is selected in the list	Assigns the parent **Computer** object for the **Server of Control** object	Name of the **Computer** objects registered in the system.	Name of the parent **Computer** object	Depends on the number of the **Computer** objects in the system.
4	**IIDK interface**	Enter a value in the field	Sets the ID of the **IIDK interface** object used by the *Server of Control*	Nonnegative integer	150	>=0
5	**Event Viewer**	Click the button	Opens the **Event Viewer** tool	-	-	-
Advanced group						
6	**Monitoring ...**	Click the button	Opens the box of setting the list of additional workplaces			
7	**Snapshots/ video...**	Click the button	Opens a dialog box for configuring reaction to snapshots and videos receiving on sensors alarms at the *Agent of Control*	-	-	-

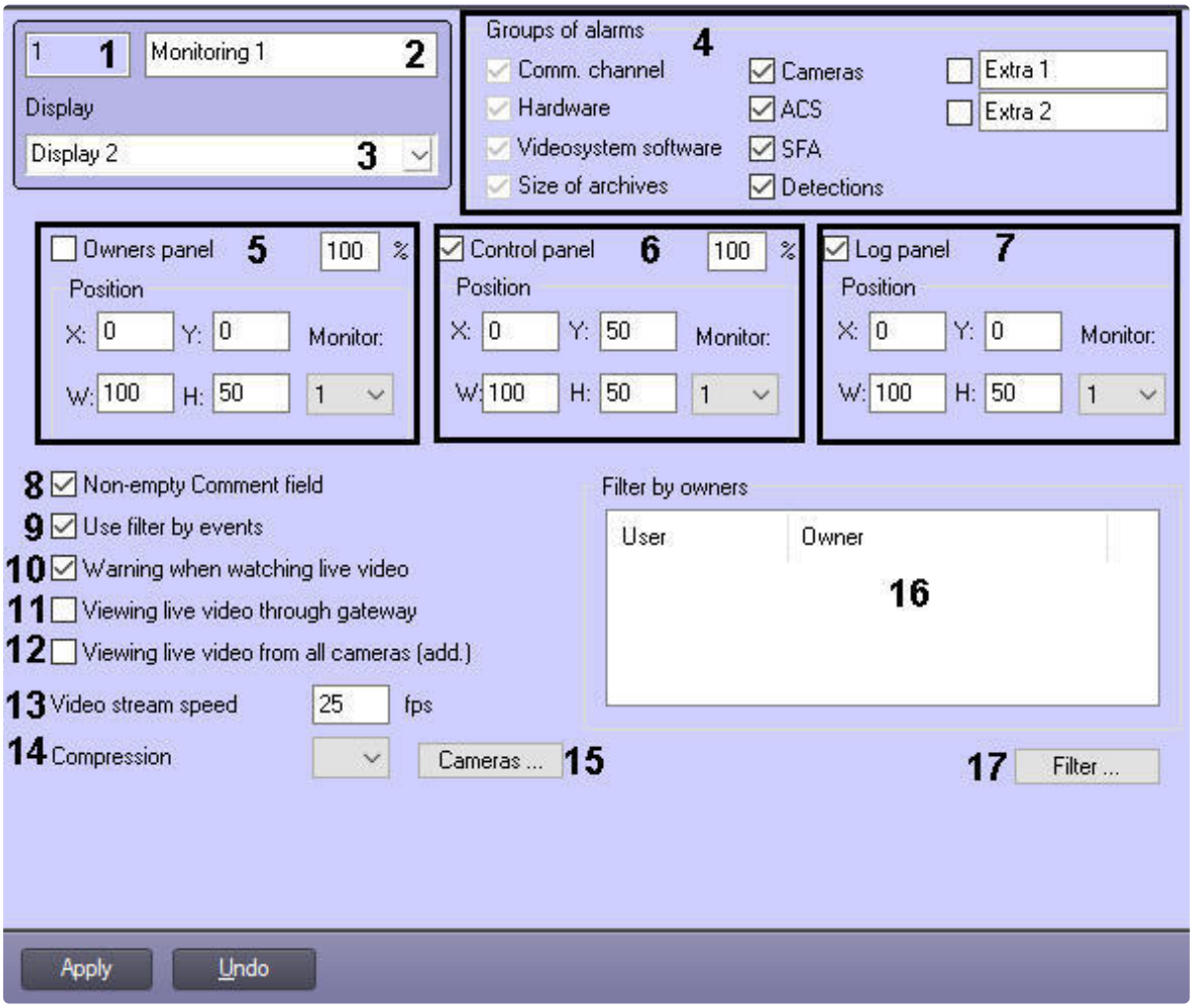
#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
Logging subsystem group						
8	**Auxiliary characters**	Is set in a checkbox	Enables logging of auxiliary characters at the transport level into the event log	Boolean	False	True – logging of auxiliary characters is enabled False – logging of auxiliary characters is not performed
9	**Alarms**	Is set in a checkbox	Enables logging alarms into the event log	Boolean	True	True – logging of alarms is enabled False – logging of alarms is not performed
10	**System status**	Is set in a checkbox	Enables logging of events related to system status	Boolean	True	True – logging of events related to system status is enabled False – logging of events related to system status is not performed
11	**Archive period (h)**	Enter the value in the field	Sets the frequency at which the log file is to be archived	Hours	48	>0
12	**File size (MB)**	Enter the value in the field	Sets the file size threshold upon which the log file is archived. This setting overrides the value in the **Archive period (h)** field.	Megabytes	100	>0
13	**Keep archives for (months)**	Enter the value in the field	Sets the length of time for which you want to store archived log files.	Months	3	from 1 to 24
Transfer group						

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
14	**TCP/IP port (Agent)**	Enter the value in the field	Sets the port number for TCP/IP communication with remote objects of **Agent of Control**	Nonnegative integer	7777	from 1 to 60000
15	**TCP/IP port (Archive)**	Enter the value in the field	Sets the port number for TCP/IP communication with remote *Search in archive* module	Nonnegative integer	7755	from 1 to 60000
16	**First COM port number**	Is selected in the list	Sets the first COM port number	COM-ports names	Com1	from Com1 to Com256
17	**Number of COM ports**	Is selected in the list	Sets number of COM ports used	Nonnegative integer	1	from 1 to 256
18	**COM port speed**	Is selected in the list	Sets the COM port speed	Baud	9600	110 300 1200 2400 4800 9600 19200 38400 57600

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
19	**COM port format**	Enter the value in the field	Sets the COM port format	COM port format	8N1	• first digit: from 5 to 9 data bits; • second letter: **N** (No parity) - no parity bit, **E** (Even parity) - even parity bit, **O** (Odd parity) - odd parity bit; • third digit: 1 or 2 stop bits.
Outside the groups						
20	**Transfer info about accepted alarms to Agent of Control**	Set the checkbox	Enables sending confirmations of alarm acceptance by the operator on the *Server of Control* to the *Agent of Control*.	Boolean type	Yes	**True** – confirmations of alarm acceptance are sent. **False** – confirmations of alarm acceptance are not sent
21	**Restart**	Click the button	*VideoSrv* communication module restarting	-	-	-

15.4 Settings panel of the Monitoring interface object

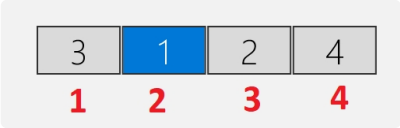
Settings panel of the **Monitoring** interface object is given on figure.

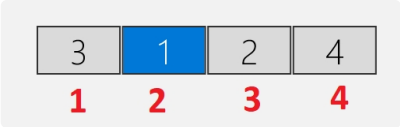


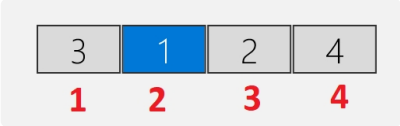
Description of the **Monitoring** object settings panel elements is given in table.

#	Name	Method for setting the parameter value	Description
1	Identifier	Automatically	Shows the identification number of the **Monitoring** object in the system
2	Name	Enter the value in the field	Shows the identification number of the **Monitoring** object in the system

#	Name	Method for setting the parameter value	Description
3	**Display**	Is selected in the list	Assigns the parent **Display** object for the **Monitoring** object
4	**Groups of alarms** checkboxes	Is set in a checkbox	Sets alarms that one want to visualize on the Control panel
5	**Owners panel** checkbox	Is set in a checkbox	Enables Owners panel displaying
	X: field	Enter the value in the field	Set the X coordinate in the horizontal axis for the upper-left corner of the Owners panel interface box
	Y: field	Enter the value in the field	Set the Y coordinate in the vertical axis for the upper-left corner of the Owners panel interface box
	W: field	Enter the value in the field	Set the width of the Owners panel interface box
	H: field	Enter the value in the field	Set the height of the Owners panel interface box
	% field	Enter the value in the field	Sets the scaling of objects in the Owners panel

#	Name	Method for setting the parameter value	Description
	Monitor drop-down list	Select from the list	Sets the number of the physical monitor which coordinates are specified. Monitors ar numbered in physical order from left to right, top to bottom. Thus, number 1 corresponds to the top-left monitor, regardless of which monitor is the primary or firs in the OS numbering. In the figure, the monitor numbers in the OS are highlighted in gray, and monitor numbers in *Intellect* are highlighted in red:  ***Attention! It is recommended to use the same resolution for all monitors in the system. Different resolutions are allowed only if each row of logical monitors is aligned to some sort of boundary (for example, to the top).***
6	**Control panel** checkbox	Is set in a checkbox	Enables Control panel displaying
	X: field	Enter the value in the field	Set the X coordinate in the horizontal axis for the upper-left corner of the Control panel interface box
	Y: field	Enter the value in the field	Set the Y coordinate in the vertical axis for the upper-left corner of the Control panel interface box
	W: field	Enter the value in the field	Set the width of the Control panel interface box
	H: field	Enter the value in the field	Set the height of the Control panel interface box

#	Name	Method for setting the parameter value	Description
	% field	Enter the value in the field	Sets the scaling of objects in the Control panel
	Monitor drop-down list	Select from the list	Sets the number of the physical monitor which coordinates are specified. Monitors ar numbered in physical order from left to right, top to bottom. Thus, number 1 corresponds to the top-left monitor, regardless of which monitor is the primary or firs in the OS numbering. In the figure, the monitor numbers in the OS are highlighted in gray, and monitor numbers in *Intellect* are highlighted in red:  ***Attention! It is recommended to use the same resolution for all monitors in the system. Different resolutions are allowed only if each row of logical monitors is aligned to some sort of boundary (for example, to the top).***
7	**Log panel** checkbox	Is set in a checkbox	Enables Log panel displaying.
	X: field	Enter the value in the field	Set the X coordinate in the horizontal axis for the upper-left corner of the Log panel interface box.
	Y: field	Enter the value in the field	Set the Y coordinate in the vertical axis for the upper-left corner of the Log panel interface box.
	W: field	Enter the value in the field	Set the width of the Log panel interface box.

#	Name	Method for setting the parameter value	Description
	H: field	Enter the value in the field	Set the height of the Log panel interface box.
	Monitor drop-down list	Select from the list	Sets the number of the physical monitor which coordinates are specified. Monitors ar numbered in physical order from left to right, top to bottom. Thus, number 1 corresponds to the top-left monitor, regardless of which monitor is the primary or firs in the OS numbering. In the figure, the monitor numbers in the OS are highlighted in gray, and monitor numbers in *Intellect* are highlighted in red:  ***Attention! It is recommended to use the same resolution for all monitors in the system. Different resolutions are allowed only if each row of logical monitors is aligned to some sort of boundary (for example, to the top).***
8	**Non-empty Comment field** checkbox	Is set in a checkbox	Is set to require that operators leave comments when accepting an alarm to describe the alarm and/or their actions.
9	**Use filter by events** checkbox	Is set in a checkbox	Is set to enable filtering objects by Alarm and Failure events and Connected and Disconnected states.
10	**Warning when watching live video** checkbox	Is set in a checkbox	Is set if it is necessary to display a warning upon the live video playback attempt that can create the critical load on the data channel.
11	**Viewing live video through gateway** checkbox	Is set in a checkbox	Is set if Agents of Control and Additional workplaces are in different subnets and the *Monitoring* components are not in a distributed system configuration in *Intellect* objec tree and **Data gateway** is in use for transmission of live video to *Additional workplaces.*

#	Name	Method for setting the parameter value	Description
12	**Viewing live video from all cameras (add.)** checkbox	Is set in a checkbox	Is set if the "All cameras of Partition of Control" item should be added to the object's "Video image playback" context menu which enables viewing video from all cameras of the selected Partition of Control.
13	**Video stream speed** field	Enter the value in the field	Sets the number of frames per second of the video image when viewing live video or video from the archive. • *Note 1. The **Video stream speed** setting works for the archive video only with CamMonitor.ocx 4.11.0.1766 or later versions.* • *Note 2. If the archive is recorded with the h264 codec and the video stream speed is set to more than **0** frames per second, then the archive video will be played back only by reference frames.* • *Note 3. If the value of the video stream speed is **0**, then the live and archive video will be played back without scaling.*
14	**Compression** drop-down list	Select from the list	Sets live video compression rate.
15	**Cameras...** button	Click the button	Opens a window for configuring cameras prohibited from viewing live video for users.
16	**Filter by owners** field	Via the **Filter...** button	Displays selected pairs of users and owners.
17	**Filter...** button	Click the button	Opens a window for configuring the correspondence of owners to users.

15.5 Settings panel of the Monitoring reports interface object

Settings panel of the **Monitoring reports** interface object is given on figure.

Description of the **Monitoring reports** object settings panel elements is given in table.

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
1	Identifier	Automatically	Shows the identification number of the **Monitoring reports** object in the system	Nonnegative integer	-	>=0
2	Name	Enter the value in the field	Shows the identification number of the **Monitoring reports** object in the system	Latin, Cyrillic letters and service characters	Monitoring reports	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	**Display**	Is selected in the list	Assigns the parent **Display** object for the **Monitoring reports** object	Names of **Display** objects registered in the system	Name of the parent **Display** object	Depends on the number of the **Display** objects in the system.

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
4	**X:**	Enter the value in the field	Set the X coordinate in the horizontal axis for the upper-left corner of the **Monitoring reports** interface box	% of the screen width	0	From 0 to 100. When more than one monitor is connected to the computer it is possible to use coordinates outside this range, but it is not recommended to use coordinates less than -200.
5	**Y:**	Enter the value in the field	Set the Y coordinate in the vertical axis for the upper-left corner of the **Monitoring reports** interface box	% of the screen height	50	From 0 to 100. When more than one monitor is connected to the computer it is possible to use coordinates outside this range, but it is not recommended to use coordinates less than -200.
6	**W:**	Enter the value in the field	Sets width of he **Monitoring reports** interface box	% of the screen width	100	From 0 to 100. When more than one monitor is connected to the computer it is possible to use coordinates outside this range, but it is not recommended to use coordinates less than -200.

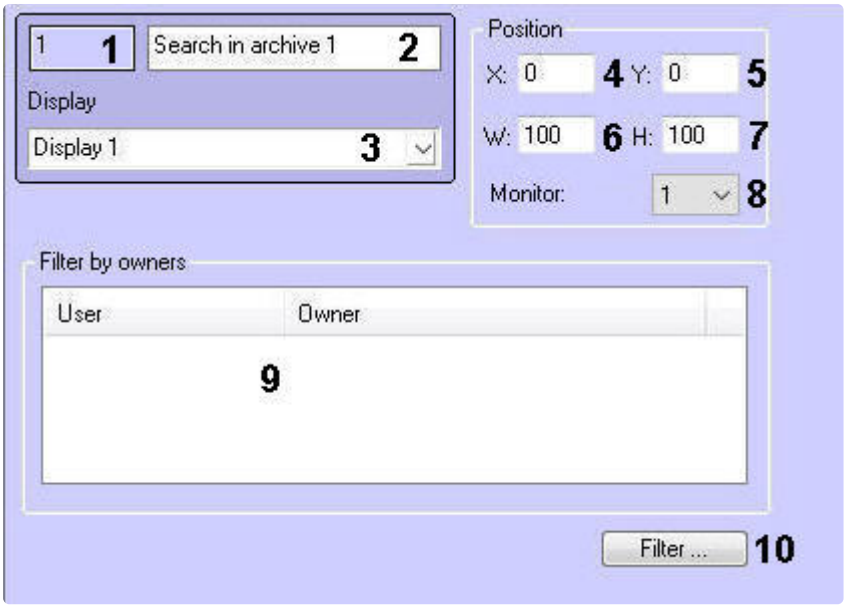
#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
7	**H:**	Enter the value in the field	Sets height of he **Monitoring reports** interface box	% of the screen height	50	From 0 to 100. When more than one monitor is connected to the computer it is possible to use coordinates outside this range, but it is not recommended to use coordinates less than -200.

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
8	**Monitor**	Select from the list	Sets the number of the physical monitor which coordinates are specified. Monitors are numbered in physical order from left to right, top to bottom. Thus, number 1 corresponds to the top-left monitor, regardless of which monitor is the primary or first in the OS numbering. In the figure, the monitor numbers in the OS are highlighted in gray, and monitor numbers in *Intellect* are highlighted in red:  ***Attention! It is recommended to use the same resolution for all monitors in the system. Different resolutions are allowed only if each row of logical monitors is aligned to some sort of boundary (for example, to the top).***	Nonnegative integer	1	From 1 to 16

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
9	**Filter by owners**	Via the **Filter...** button	Displays selected pairs of users and owners	-	-	-
10	**Filter...**	Click the button	Opens a dialog box to match owners to users	-	-	-
11	**Reports**	Set the checkbox	Select reports available in the interface window.	Boolean	All checkboxes are set, full access to the Vehicle PLs report is set	Yes – the report button is displayed in the **Monitoring Reports** interface window. No – the report button is not displayed in the **Monitoring Reports** interface window.

15.6 Settings panel of the Search in archive interface object

Settings panel of the **Search in archive** interface object is given on figure.



Description of the **Search in archive** object settings panel elements is given in table

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
1	Identifier	Automatically	Shows the identification number of the **Search in archive** object in the system	Nonnegative integer	-	>=0
2	Name	Enter the value in the field	Shows the name of the **Search in archive** object in the system	Latin, Cyrillic letters and service characters	Search in archive	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	**Display**	Is selected in the list	Assigns the parent **Display** object for the **Search in archive** object	Names of **Display** objects registered in the system	Name of the parent **Display** object	Depends on the number of the **Display** objects in the system.
4	**X:**	Enter the value in the field	Set the X coordinate in the horizontal axis for the upper-left corner of the **Search in archive** interface box	% of the screen width	0	From 0 to 100. When more than one monitor is connected to the computer it is possible to use coordinates outside this range, but it is not recommended to use coordinates less than -200.

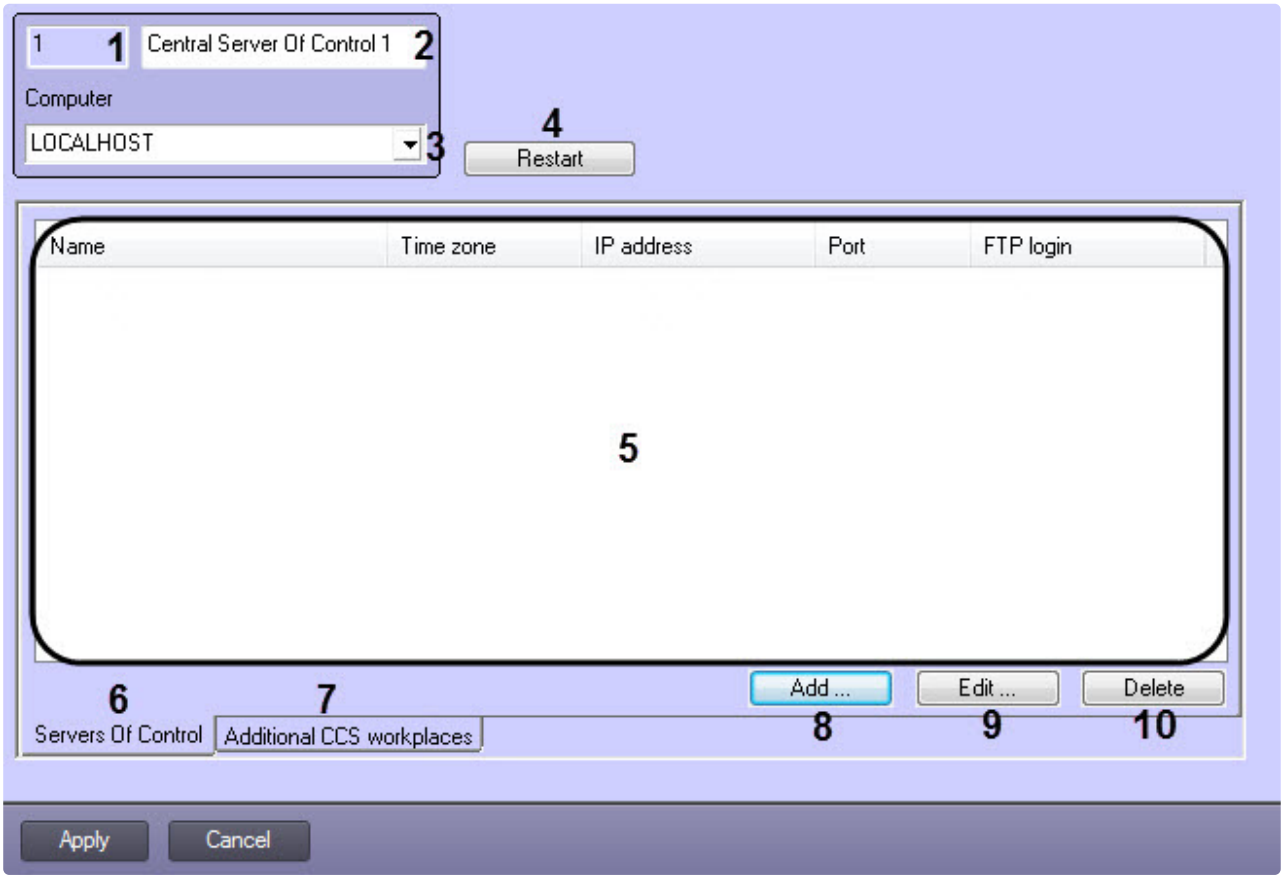
#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
5	**Y:**	Enter the value in the field	Set the Y coordinate in the vertical axis for the upper-left corner of the **Search in archive** interface box	% of the screen height	50	From 0 to 100. When more than one monitor is connected to the computer it is possible to use coordinates outside this range, but it is not recommended to use coordinates less than -200.
6	**W:**	Enter the value in the field	Sets width of he **Search in archive** interface box	% of the screen width	100	From 0 to 100. When more than one monitor is connected to the computer it is possible to use coordinates outside this range, but it is not recommended to use coordinates less than -200.
7	**H:**	Enter the value in the field	Sets height of he **Search in archive** interface box	% of the screen height	50	From 0 to 100. When more than one monitor is connected to the computer it is possible to use coordinates outside this range, but it is not recommended to use coordinates less than -200.

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
8	**Monitor**	Select from the list	Sets the number of the physical monitor which coordinates are specified. Monitors are numbered in physical order from left to right, top to bottom. Thus, number 1 corresponds to the top-left monitor, regardless of which monitor is the primary or first in the OS numbering. In the figure, the monitor numbers in the OS are highlighted in gray, and monitor numbers in *Intellect* are highlighted in red:  ***Attention! It is recommended to use the same resolution for all monitors in the system. Different resolutions are allowed only if each row of logical monitors is aligned to some sort of boundary (for example, to the top).***	Nonnegative integer	1	From 1 to 16
9	**Filter by owners**	Via the **Filter...** button	Displays selected pairs of users and owners	-	-	-

#	Name	Method for setting the parameter value	Description	Type	Default value	Value range
10	**Filter...**	Click the button	Opens a window for configuring the correspondence of owners to users	-	-	-

15.7 Settings panel of the Central Server of Control object

Settings panel of the **Central Server of Control** object is given on figure.



Description of the **Central Server of Control** object settings panel elements is given in table.

№	Name	Method for setting the parameter value	Description	Type	Default value	Value range
1	Identifier	Automatically	Shows the identification number of the **Central Server of Control** object in the system	Nonnegative integer	-	>=0
2	Name	Enter the value in the field	Shows the name of the **Central Server of Control** object in the system	Latin, Cyrillic letters and service characters	Central Server of Control	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	**Computer**	Select from the list	Assigns the parent **Computer** object for the **Central Server of Control** object	Name of the **Computer** objects registered in the system.	Name of the parent **Computer** object	Depends on the number of the **Computer** objects in the system.
4	**Restart**	Click the button	Restart of the **CentralNetServer** communication module	-	-	-
5	-	-	The table containing the monitored *Servers Of Control* or added *Additional workplaces of CSC*			
6	**Servers Of Control**	Click the tab	The tab for configuring and displaying the monitored *Servers Of Control*	-	-	-

№	Name	Method for setting the parameter value	Description	Type	Default value	Value range
7	**Additional CSC workplaces**	Click the tab	The tab for configuring and displaying the *Additional workplaces of CSC* which have the permission to be connected to the *Central Server of Control*	-	-	-
8	**Add**	Click the button	The settings window for adding the *Server Of Control/Additional workplace of CSC*	-	-	-
9	**Edit**	Click the button	The settings window for editing the parameters of added *Servers Of Control/ Additional workplaces of CSC*	-	-	-
10	**Delete**	Click the button	Deletes the selected *Server Of Control/Additional workplace of CSC*	-	-	-

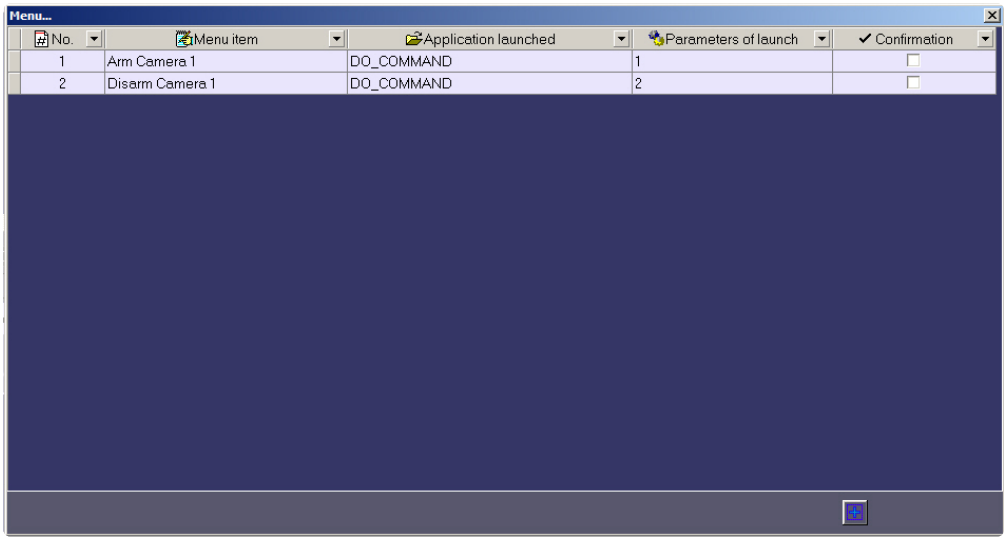
16 Appendix 2. Sample scripts

16.1 Sample script for processing Server of Control command on Agent of Control

In the *Monitoring* software package one can configure ad hoc command sending by the Operator of the *Server of Control* to the *Agent of Control*. Information on how to configure commands on the *Server of Control* can be found in the Executing ad hoc command on the Agent of Control by the operator of Server of Control section of Operator's Guide.

A script for processing incoming commands is to be created on the *Agent of Control*.

Extra menu items are created on the Server of Control – “Arm camera 1” and “Disarm camera 1”. They send a command with parameter 1 or 2 correspondently.



The sample of program in *Intellect* embedded language for processing the incoming command is shown below:

```
OnEvent("VIDEOSRV_C_DVC","1","DO_COMMAND")
{
    if (strequal(param0,"1"))
    {
        DoReact("CAM","1","ARM");
    }
    if (strequal(param0,"2"))
    {
        DoReact("CAM","1","DISARM");
    }
}
```

16.2 Sample script for setting custom filter in the Log Panel

Custom filter on the Log Panel can be changed with a script or macro. For more details on the filter and its configuration in the user interface, see Custom filter in the Log Panel.

Use APPLY_FILTER reaction of the VIDEOSRV_M object to create or change the custom filter in the Log Panel:

```
DoReact("VIDEOSRV_M","","APPLY_FILTER","computer<>,query<>");
```

Parameters:

computer<> – NetBIOS name of the computer to execute the command on.

query<> – filter condition.

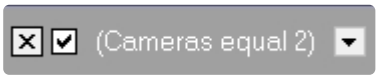
The query<>parameter syntax:

query<TotalExpressions;BoolOperatorKind;Expression[;Expression]>

- **TotalExpressions** — number of expressions in the condition
  Example:
  TotalExpressions = 1 for condition (Cameras equal 2)
  TotalExpressions = 3 for condition (Cameras equal 2) and ((Disks equal 1) or (Disks equal 2))
- **BoolOperatorKind** — boolean operator for main expression. Possible values:
  – and
  – or
  Example:
  BoolOperatorKind = and for condition (Cameras equal 2)
  BoolOperatorKind = and for condition (Cameras equal 2) and ((Disks equal 1) or (Disks equal 2))
  BoolOperatorKind = or for condition (Cameras equal 1) or (Cameras equal 2)
- **Expression** — one or several expressions
  Format: Field;Expressions;LocalBoolOperator;OperatorKind;Value
  - *Field* — name of the field in the DB table.
    Possible values:
    – ID
    – Name
    – Region
    – Province
    – City
    – CamCnt
    – ArcMax
    – HddCnt
    – IpAddress
    – FirstRecord
    – TemperHdd
    – AvailMemory
    – WorkingTime
    – VerSoft
  - *Expressions* — number of expressions in a subcondition.
    Example:
    Expressions = 1 for condition (Cameras equal 2) and ((Disks equal 1) or (Disks equal 2))
    Expressions = 2 for condition (Cameras equal 2) and ((Disks equal 1) or (Disks equal 2))
  - *LocalBoolOperator* — boolean operator for subconditions. Possible values:
    – and
    – or
    Example:
    LocalBoolOperator = and for condition (Cameras equal 2)
    LocalBoolOperator = or for condition (Cameras equal 2) and ((Disks equal 1) or (Disks equal 2))
  - *OperatorKind* — operator type.
    Possible values:
    – Equal
    – NotEqual

  - Less
  - LessOrEqual
  - Greater
  - GreaterOrEqual
  - Like
  - NotLike
- *Value* — value to compare with.

Examples:




```
query<1;and;CamCnt;1;and;Equal;2>
```

With main expressions:


```
query<2;and;CamCnt;1;and;Less;5;CamCnt;1;and;Greater;3>
```

With subquery:


```
query<2;and;CamCnt;2;and;Less;5;CamCnt;2;and;Greater;3>
```


```
query<3;and;CamCnt;2;and;Greater;1;CamCnt;2;and;Less;5;HddCnt;1;and;Greater;0>
```


```
query<1;and;Name;1;and;Like;%47>
```

16.3 Sample script for stopping camera recording

If you want for a JPEG still frame to be attached to an alarm message or video fragment when a sensor is activated (**Sensor** object), remember that this is possible only after the current archive file has been written to disk. To reduce the waiting time (the **Delay (sec.)** parameter, see the section Configuring sensors) and be assured of camera recording, you can create a **Program** object on the **Programming** tab of *Intellect* software package.

These programs are written for a camera with an ID of 1 and for a **Sensor** object whose ID is also equal to 1. Thanks to these programs, the value of the **Delay** parameter can be set equal to 7 seconds.

Attention!

To get several video fragments, you can specify several repeated commands "REC" and "REC_STOP" in the script. If "rollback" is used, and the prerecording time in the settings of the **Camera** object is greater than or equal to the time between subsequent "REC_STOP" and "REC" commands, then this video fragment will be combined with the next video fragment.

Option 1. The camera is disarmed:

```
OnEvent("GRAY","1","ALARM")
{
[
    if( !CheckState("CAM","1","DETACHED") )
    {
        DoReact("CAM","1","REC","rollback<1>");
        Wait(5);
        DoReact("CAM","1","REC_STOP","priority<2>");
    }
]
}

OnEvent("GRAY","1","ALARM")
{
[
    Wait(2);
    DoReact("GRAY","1","CONFIRM");
    Wait(2);
    DoReact("GRAY","1","ARM");
]
}
```

Option 2. Camera is armed:

```
OnEvent("GRAY","1","ALARM")
{
[
    if( !CheckState("CAM","1","DETACHED") )
    {
        DoReact("CAM","1","DISARM");
        Sleep(50);
        DoReact("CAM","1","REC","rollback<1>");
        Wait(5);
        DoReact("CAM","1","REC_STOP","priority<2>");
        Sleep(2050); // Prerecording time in the Camera settings = 2 sec.
        DoReact("CAM","1","ARM");
    }
]
}

OnEvent("GRAY","1","ALARM")
{
[
    Wait(2);
    DoReact("GRAY","1","CONFIRM");
```

```
    Wait(2);
    DoReact("GRAY","1","ARM");
]
}
```

Option 3. Continuous recording:

```
OnEvent("GRAY","1","ALARM")
{
[
    if( !CheckState("CAM","1","DETACHED") )
    {
        Wait(5); // Specifies the time after which the recording should be stopped in
order to get the required video fragment or number of frames
        DoReact("CAM","1","REC_STOP","priority<2>");
        Sleep(2050); // Prerecording time in the Camera settings = 2 sec.
        DoReact("CAM","1","REC","rollback<1>"); // Start recording with 2 sec
rollback (during prerecording). Thus, data in the archive is not lost.
    }
]
}

OnEvent("GRAY","1","ALARM")
{
[
    Wait(2);
    DoReact("GRAY","1","CONFIRM");
    Wait(2);
    DoReact("GRAY","1","ARM");
]
}
```

16.4 Sample scripts for processing alarm confirmations

The **Partition of Control** object (VIDEOSRV_C_DVC) sends the «Confirmed: Monitoring events» (CONF_MON) message to *Intellect* core when an alarm is confirmed.

When the confirmation type is **Simple**, then param0<> has the same value as the ID of event that is confirmed (see Configuration for associating events with certain alarm groups section). When **param1<>** is **0**, it means that a Simple confirmation is used.

Below you will find a sample program that can be written on the *Agent of Control* in order to process a received simple confirmation. As a result a camera is armed.

```
OnEvent("VIDEOSRV_C_DVC","1","CONF_MON")
{
  if (strequal(param0,"1"))
  {
    DoReact("CAM","1","ARM");
  }
}
```

When the confirmation type is **Complex**, then param0<> has the value of the ID of event that is confirmed (see Configuration for associating events with certain alarm groups section). If param1<> is **1**, it means that the operator has clicked the **OK** button in the confirm box. If the operator clicked the **Cancel** button, then param1<> would be **2**.

Below you will find a sample program that can be written on the *Agent of Control* in order to process a received complex confirmation. As a result a camera is armed only when the operator clicks the **OK** button in the confirm box.

```
OnEvent("VIDEOSRV_C_DVC","1","CONF_MON")
{
  if (strequal(param0,"1")&&strequal(param1,"1"))
  {
    DoReact("CAM","1","ARM");
  }
}
```

16.5 Sample script to export filtered data from the Log Panel to .xls

Before executing this command, apply filter in the Log Panel. It can be done from the user interface (see Custom filter in the Log Panel) or by a script (see Sample script for setting custom filter in the Log Panel).

Export filtered Log Panel data to the test.xls file on disk C:

```
DoReact("VIDEOSRV_M","","EXPORT_EXCEL","computer<NamePC>,file<c:\test.xls>");
```

16.6 Sample script to show and hide Search license plates window

Show **Search license plates** window with 70% screen width and 50% screen height in the upper left of the display:

```
DoReact("VIDEOSRV_M","","SHOW_AUTO","computer<NamePC>,x<0>,y<0>,w<70>,h<50>");
```

Hide **Search license plates** window:

```
DoReact("VIDEOSRV_M","","HIDE_AUTO","computer<NamePC>");
```

Parameters:

computer<> – name of the computer to execute command on.

x<> – X-axis coordinate of upper left corner the window.

y<> – Y-axis coordinate of upper left corner the window.

w<> – window width as a percentage of the screen width.

h<> – window height as a percentage of the screen height.

16.7 Sample scripts for the special mode of Monitoring operation with ACFA Intellect

16.7.1 Sample script for configuring the interaction between the Monitoring and the Rovalant (A6, A16) integration module

This script records the users from the *Server Of Control* side into the *Rovalant (A6, A16)* FSA, which is installed on the *Agent Of Control* side.

> **Attention!**
>
> The configuration guide for the *Rovalant (A6, A16)* integration module is available only in the Russian documentation for *ACFA Intellect*. This script can be modified for any other integration module that supports user entry into the controller.

> **Note**
>
> For details, see Configuring the special mode of Monitoring operation with ACFA Intellect.

```
function SetPersons(srcDepartment, destTable, destTableSize, msg)
{
    var users = CreateMsg();
    users.StringToMsg(GetObjectIds("PERSON"));
    var userCount = users.GetParam("id.count");
    var i;
    var index;
    for(i = 0, index = 1; (index <= destTableSize) && (i < userCount); ++i)
    {
        var user = users.GetParam("id." + i);
        if(GetObjectParentId("PERSON", user, "DEPARTMENT") == srcDepartment)
        {
            msg.SetParam("USERS.user_id." + Itv_var("counter"), user);
            msg.SetParam("USERS.number." + Itv_var("counter"), index);
            msg.SetParam("USERS.key_type." + Itv_var("counter"), destTable);
            index++;
            Lock();
            Itv_var("counter")++;
            Unlock();
        }
    }
}
if(Event.SourceType == "VIDEOSRV_C" && Event.Action == "SPR_DATA_UPDATED")
{
    var ROVALANT_TYPE = "ROVALANT_DEVICE";
    var ROVALANT_ID = "1.1";
    var WRITE_CONFIG_REACT = "WRITE_CONFIG";
    Itv_var("counter") = 0;
    var msg = CreateMsg();
    msg.SourceType = "CORE";
```

```
    msg.SourceId = "";
    msg.Action = "UPDATE_OBJECT";
    msg.SetParam("objtype", ROVALANT_TYPE);
    msg.SetParam("objid", ROVALANT_ID);
    var type = GetObjectParam(ROVALANT_TYPE, ROVALANT_ID, "type");
    if(type == "A6")
    {
        SetPersons("1", "USER", 79, msg);
    }
    else
    {
        SetPersons("1", "USER", 255, msg);
    }
    SetPersons("2", "POLICE", 15, msg);
    SetPersons("3", "ELECTRIC", 15, msg);

    msg.SetParam("USERS.user_id.count", Itv_var("counter"));
    msg.SetParam("USERS.number.count",  Itv_var("counter"));
    msg.SetParam("USERS.key_type.count",  Itv_var("counter"));
    NotifyEvent(msg);
    NotifyEventStr(ROVALANT_TYPE, ROVALANT_ID, WRITE_CONFIG_REACT, "");
}
```

16.7.2 Sample scripts for determining the current state of the zones of the Rovalant (A6, A16) object on the Agent of Control side

This script determines the current state of the zones on the *Agent Of Control* side with the configured *Rovalant (A6, A16)* FSA. Also, when the **GET_OBJECT_STATE** event is received, this script generates the **OBJECT_STATE_INFO** event. The zones are configured and assigned to the corresponding loops when configuring the *Rovalant (A6, A16)* integration module.

> **Attention!**
>
> The configuration guide for the *Rovalant (A6, A16)* integration module is available only in the Russian documentation for *ACFA Intellect*. This script can be modified for any other integration module that supports user entry into the controller.

> **Note**
>
> For details, see Configuring the special mode of Monitoring operation with ACFA Intellect.

```
function GetStateByCounts(armedCount, disarmedCount)
{
    /* If there are both armed and disarmed zones, then we consider that arming is
partially completed */
    if(armedCount > 0 && disarmedCount > 0)
    {
        return "PART_ARMED";
    }
```

```
    /* If there are only armed zones, then we consider that the controller is armed
*/
    else if(armedCount > 0)
    {
        return "ARMED";
    }
    /* We consider that the controller is disarmed */
    return "DISARMED"
}
function ZoneIsUsed(params, id)
{
    var count = params.GetParam("TABLE.zone.count");
    var number = GetObjectParam("ROVALANT_ZONE", id, "number");
    var i;
    for(i=0; i < count; ++i)
    {
        if(params.GetParam("TABLE.zone." + i) == number)
        {
            return "true";
        }
    }
    return "false";
}
function GetControllerState(id, zones)
{
    /* Get the controller configuration*/
    var params = CreateMsg();
    params.StringToMsg(GetObjectParams("ROVALANT_DEVICE", id));
    /* Get the number of zones used by the controller */
    var count = params.GetParam("TABLE.zone.count");
    /* If the controller uses the zones */
    if(count > 0)
    {
        /* The number of armed and disarmed zones */
        var armedCount = 0;
        var disarmedCount = 0;
        var zoneCount = zones.GetParam("id.count");
        var j;
        for(j = 0; j < zoneCount; ++j)
        {
            /* Determine if the zone belongs to the current controller
               and determine whether this zone is used by the current controller */
            var zone = zones.GetParam("id."+j);
            if(GetObjectParentId("ROVALANT_ZONE", zone, "ROVALANT_DEVICE") == id &&
ZoneIsUsed(params, zone) == "true")
            {
                /* Check the state of the zone */
                var state = GetObjectState("ROVALANT_ZONE", zone);
                switch(state)
                {
                case "ARMED":
                case "ALARM_ARMED":
                case "TROUBLE_ARMED":
```

```
                    armedCount++;
                    break;
                case "DISARMED":
                case "TROUBLE_DISARMED":
                    disarmedCount++;
                    break;
                }
            }
        }
    }

    /* Check the state of the object */
    return GetStateByCounts(armedCount, disarmedCount, msg);
}
function GetSkdStateMsg(type, id, action)
{
    var devices = CreateMsg();
    devices.StringToMsg(GetObjectIds("ROVALANT_DEVICE"));
    var count = devices.GetParam("id.count");
    var zones = CreateMsg();
    zones.StringToMsg(GetObjectIds("ROVALANT_ZONE"));
    /* The number of armed and disarmed zones */
    var armedCount = 0;
    var disarmedCount = 0;
    var i;
    for(i = 0; i < count; ++i)
    {
        var device = devices.GetParam("id."+i);
        var state = GetControllerState(device, zones);
        switch(state)
        {
            case "PART_ARMED":
                disarmedCount++;
            case "ARMED":
                armedCount++;
                break;
            case "DISARMED":
                disarmedCount++;
                break;
        }
    }
    var msg = CreateMsg();
    msg.SourceType = type;
    msg.SourceId = id;
    msg.Action = action;

    msg.SetParam("state", GetStateByCounts(armedCount, disarmedCount));
    msg.SetParam("card", "");
    return msg;
}
if(Event.SourceType == "VIDEOSRV_C" && Event.Action == "GET_OBJECT_STATE")
{
```

```
    NotifyEvent(GetSkdStateMsg(Event.SourceType, Event.SourceId, "OBJECT_STATE_INFO")
);
}
else if(Event.SourceType == "ROVALANT_DEVICE" &&
(Event.Action == "A06_CLOSE" ||
Event.Action == "A16_CLOSE" ||
Event.Action == "A06_OPEN" ||
Event.Action == "A16_OPEN" ||
Event.Action == "A06_POLICE" ||
Event.Action == "A16_POLICE" ||
Event.Action == "A06_ELECTRIC" ||
Event.Action == "A16_ELECTRIC" ||
Event.Action == "A06_ENTRY" ||
Event.Action == "A16_ENTRY"))
{
    var card = Event.GetParam("key_code");
    var msg = GetSkdStateMsg("VIDEOSRV_C", "1", "OBJECT_STATE_INFO");
    msg.SetParam("card", card);
    NotifyEvent(msg);
}
```

16.8 Sample scripts for determining the current state of the relay on the Agent of Control side

This script determines the current state of the relay on the *Agent of Control* side. Also, when the **GET_OBJECT_STATE** event is received, this script generates the **OBJECT_STATE_INFO** event (for details, see Configuring alarms for monitoring the object state on the Agent Of Control side). Using the **card** parameter from the *Agent of Control*, it is possible to transfer any additional information to the *Server of Control*. This information will be displayed in the **Event Log** (see Event log).

```
function GetReleStateMsg(type, id, action, card)
{
  var state = GetObjectState("GRELE","1");
  var msg = CreateMsg();
  msg.SourceType = type;
  msg.SourceId = id;
  msg.Action = action;
  msg.SetParam("state",(state=="OFF")?"DISARMED":"ARMED");
  msg.SetParam("card",card);
  return msg;
}

if(Event.SourceType=="VIDEOSRV_C" && Event.SourceId=="1" && Event.Action=="GET_OBJECT
_STATE")
{
  NotifyEvent(GetReleStateMsg(Event.SourceType, Event.SourceId,"OBJECT_STATE_INFO","")
);
}
else if(Event.SourceType=="GRELE" && (Event.Action=="ON" || Event.Action=="OFF"))
{
```

```
  NotifyEvent(GetReleStateMsg("VIDEOSRV_C", "1","OBJECT_STATE_INFO",""));
}
```

16.9 Sample script for creating a hardware failures report

A **Hardware failures report** (see Hardware failures reports) can be automatically generated using a script that uses the REPORT_FAILURES reaction of the VIDEOSRV_R object:

```
DoReact("VIDEOSRV_R","","REPORT_FAILURES","computer<>,file<>,export<>,object<>,region
<>,district<>,city<>,type<>,fromTime<>,toTime<>,sorting<>,comment<>");
```

Parameters description is given in the table below:

Parameter	Description
computer<>	Specifies the NetBIOS name of the computer on which the report is to be created. Required parameter.
file<>	The full path to the file where the report will be saved. Required parameter.
export<>	Format of the export file. 0 - Excel, 1 - HTML, 2 - RTF, 3 - CSV. Optional parameter. If this parameter is absent, the file is exported in Excel format.
object<>	The object on which the report is created. This parameter specifies the "Object code", which is displayed on the Log Panel of the **Monitoring** interface object (see Information about an object). Optional parameter. If this parameter is absent, a report is created for all objects.
region<>	Filter by the Region. It is necessary to specify the indexing numbers of the options to be used separated by commas in the **Region** drop-down list. For example: (region<1,3>) (see Hardware failures reports). Optional parameter. If this parameter is absent, a report is created for all regions.
district<>	Filter by the District. It is necessary to specify the indexing numbers of the options to be used separated by commas in the **District** drop-down list. For example: (district<2,3,5>) (see Hardware failures reports). Optional parameter. If this parameter is absent, a report is created for all districts.

Parameter	Description
city<>	Filter by the City. It is necessary to specify the indexing numbers of the options to be used separated by commas in the **City** drop-down list. For example: (city<1>) (see Hardware failures reports). Optional parameter. If this parameter is absent, a report is created for all cities.
type<>	Filter by the Failure type. It is necessary to specify the indexing numbers of the options to be used separated by commas in the **Failure type** drop-down list. For example: (type<1,3,5>) (see Hardware failures reports). Optional parameter. If this parameter is absent, a report is created for all failure types.
fromTime<>	Date and time of the report beginning in the DD-MM-YY HH:MM:SS format. Required parameter.
toTime<>	Date and time of the report ending in the DD-MM-YY HH:MM:SS format. Required parameter.
sorting<>	Sorting mode. 0 - by event, 1 - by time. Optional parameter. If this parameter is absent, sorting by event is used.
comment<>	Show comment. 0 - do not show, 1 - show. Optional parameter. If this parameter is absent, comments are not shown.

Sample script that will automatically create a **Hardware failures report** every day at 20:00 and save it to the C:\report.html file:

```
OnTime(W,D,X,Y,"20","00","00")
{
DoReact("VIDEOSRV_R","","REPORT_FAILURES","computer<MONITORING>,file<c:
\report.html>,export<1>,fromTime<" + date + " 00:00:00>,toTime<" + date + " " + time
+ ">");
}
```

16.10 Sample script for creating an alarms report

An **Alarms report** (see Alarms reports) can be automatically generated using a script that uses the REPORT_ALARMS reaction of the VIDEOSRV_R object:

```
DoReact("VIDEOSRV_R","","REPORT_ALARMS","computer<>,file<>,export<>,object<>,region<>
,district<>,city<>,type<>,fromTime<>,toTime<>,sorting<>,comment<>,filter<>");
```

Parameters description is given in the table below:

Parameter	Description
computer<>	Specifies the NetBIOS name of the computer on which the report is to be created. Required parameter.
file<>	The full path to the file where the report will be saved. Required parameter.
export<>	Format of the export file. 0 - Excel, 1 - HTML, 2 - RTF, 3 - CSV. Optional parameter. If this parameter is absent, the file is exported in Excel format.
object<>	The object on which the report is created. This parameter specifies the "Object code", which is displayed on the Log Panel of the **Monitoring** interface object (see Information about an object). Optional parameter. If this parameter is absent, a report is created for all objects.
region<>	Filter by the Region. It is necessary to specify the indexing numbers of the options to be used separated by commas in the **Region** drop-down list. For example: (region<1,3>) (see Alarms reports). Optional parameter. If this parameter is absent, a report is created for all regions.
district<>	Filter by the District. It is necessary to specify the indexing numbers of the options to be used separated by commas in the **District** drop-down list. For example: (district<2,3,5>) (see Alarms reports). Optional parameter. If this parameter is absent, a report is created for all districts.
city<>	Filter by the City. It is necessary to specify the indexing numbers of the options to be used separated by commas in the **City** drop-down list. For example: (city<1>) (see Alarms reports). Optional parameter. If this parameter is absent, a report is created for all cities.

Parameter	Description
type<>	Filter by the Alarm type. It is necessary to specify the indexing numbers of the options to be used separated by commas in the **Alarm** drop-down list. For example: (type<1,3,5>) (see Alarms reports). Optional parameter. If this parameter is absent, a report is created for all alarm types.
fromTime<>	Date and time of the report beginning in the DD-MM-YY HH:MM:SS format. Required parameter.
toTime<>	Date and time of the report ending in the DD-MM-YY HH:MM:SS format. Required parameter.
sorting<>	Sorting mode. 0 - by event, 1 - by time. Optional parameter. If this parameter is absent, sorting by event is used.
comment<>	Show comment. 0 - do not show, 1 - show. Optional parameter. If this parameter is absent, comments are not shown.
filter<>	Text filter by messages of monitored alarms (see Configuring alarm groups). Optional parameter.

Sample script that will automatically create an **Alarms report** every day at 20:00 and save it to the C:\report.html file:

```
OnTime(W,D,X,Y,"20","00","00")
{
DoReact("VIDEOSRV_R","","REPORT_ALARMS","computer<MONITORING>,file<c:
\report.html>,export<1>,fromTime<" + date + " 00:00:00>,toTime<" + date + " " + time
+ ">");
}
```