

AxxonSoft

Agent of Control

Installation and Configuration Guide

Version 1.5

Moscow 2014

CONTENTS

CONTENTS	2
1 INTRODUCTION.....	3
1.1 Document purpose	3
1.2 Purpose of Monitoring.....	3
1.3 Features of Monitoring.....	3
2 HARDWARE AND SOFTWARE REQUIREMENTS.....	4
2.1 Operating system requirements	4
2.2 Hardware requirements	4
3 INSTALLING AGENT OF CONTROL.....	5
3.1 Installer	5
3.2 Preparing for installation	5
3.3 Installation	5
4 CONFIGURING AGENT OF CONTROL	9
4.1 Creating necessary Agent of Control objects.....	9
4.2 Configuring the event log.....	11
4.3 Configuring the Partition Of Control object	13
4.3.1 Configuring the Partition Of Control unique ID.....	13
4.3.2 Configuring a port for incoming UPS messages	13
4.3.3 Configuring communication between Agent of Control and Control Server	14
4.3.4 Configuring sensors.....	16
4.3.5 Configuring captions	19
4.3.6 Configuring the camera list.....	21
4.3.7 Configuring alarm groups	23
4.4 Connecting to uninterrupted power supplies	27
4.4.1 Installing StateUPS	27
4.4.2 Installing the PowerChute plus utility	32
4.4.3 Example of configuration of event distribution	34
5 APPENDIX 1. SAMPLE SCRIPT FOR STOPPING CAMERA RECORDING	37

1 Introduction

1.1 Document purpose

This document, *Agent of Control: Installation and Configuration Guide*, is a reference aid for system administrators, configuration and installation specialists, and users with administrator rights on the Intellect PSIM.

This guide describes the following:

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

1.3 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, the module allows monitoring the actions of monitoring operators: recorded 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 for statistics and analysis generates reports on system operation: reports on alarms, downtime, statistics on security system operation, and more.

2 Hardware and software requirements

2.1 Operating system requirements

Agent of Control 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 *Administrator's Guide*).

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

2.2 Hardware requirements

Agent of Control 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

3 Installing Agent of Control

3.1 Installer

The Agent of Control installer is based on InstallShield 2010 and is found in the file setupAgentOfControl.exe (Fig. 3.1 – 1).

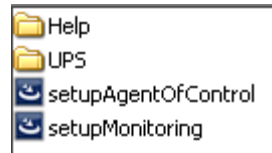


Fig. 3.1 – 1 Contents of the Monitoring installer kit

Documentation is included in the Help folder. The UPS folder contains the software components that are necessary for the Agent of Control to perform monitoring of UPS status.

3.2 Preparing for installation

Before beginning installation, copy the installation kit to a local disk and make sure that the indicated files are not marked as "read-only".

Before installing *Monitoring*, install *Intellect* in server mode.

Information on compatibility of *Monitoring* and *Intellect* software versions is given on the page [General information about product releases and versions compatibility](#).

The program key, intellect.sec, should contain the **Agent of Control** object.

Before starting the installer, quit Intellect. If Intellect is installed as a service, stop the service.

3.3 Installation

Installation of Agent of Control is performed in the following sequence:

1. From the installation kit, start the executable file setupAgentOfControl.exe. After an installation language is chosen, the window informs of the beginning of installation (Fig. 3.3 – 1).

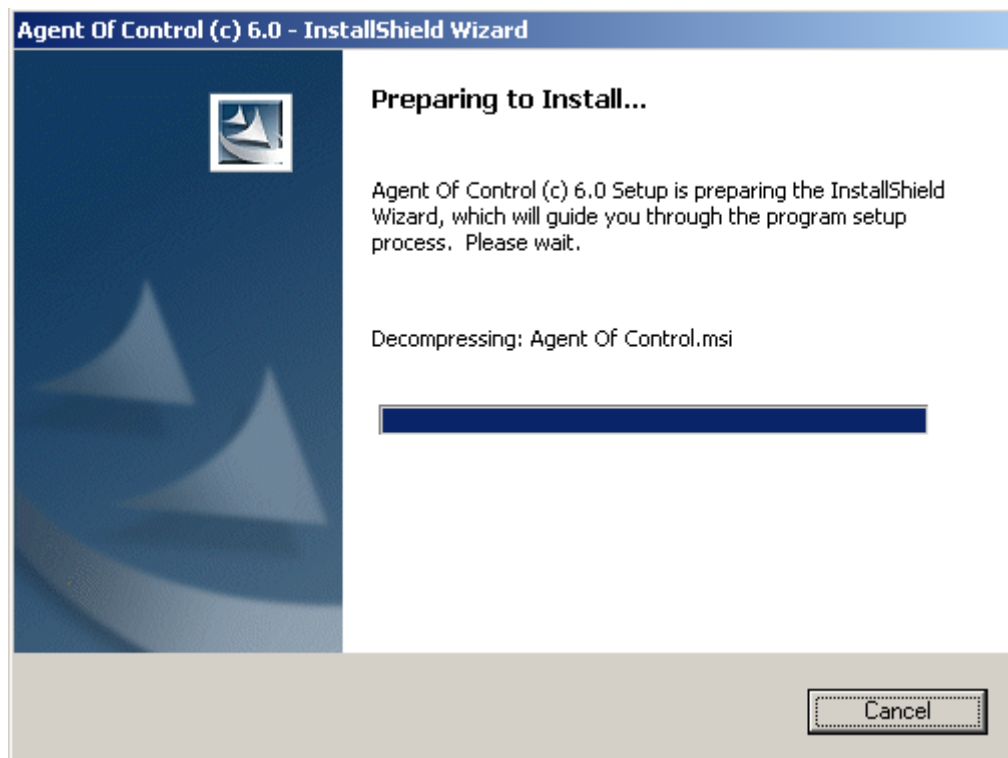


Fig. 3.3 – 1 Preparing for installation

2. A prompt to start installation then appears (Fig. 3.3 – 2). Click the **Next** button.

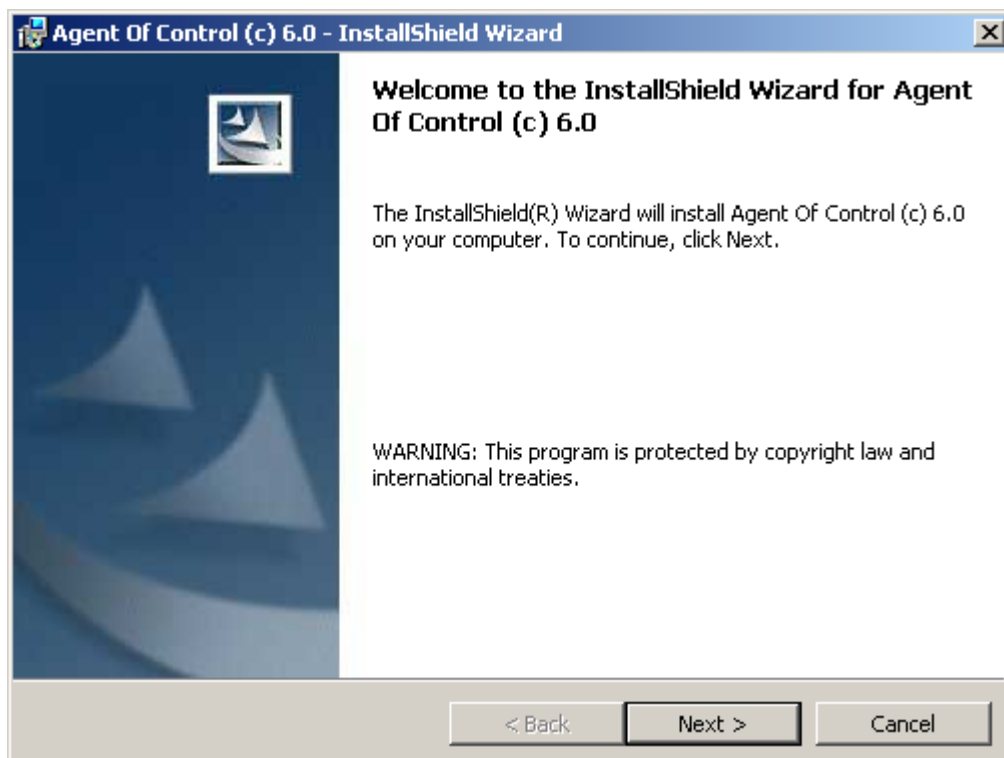


Fig. 3.3 – 2 Beginning installation

3. The **License Agreement** window presents the terms of the end user license agreement. Select **I accept the terms of the License Agreement** and click the **Next** button (Fig. 3.3 – 3).

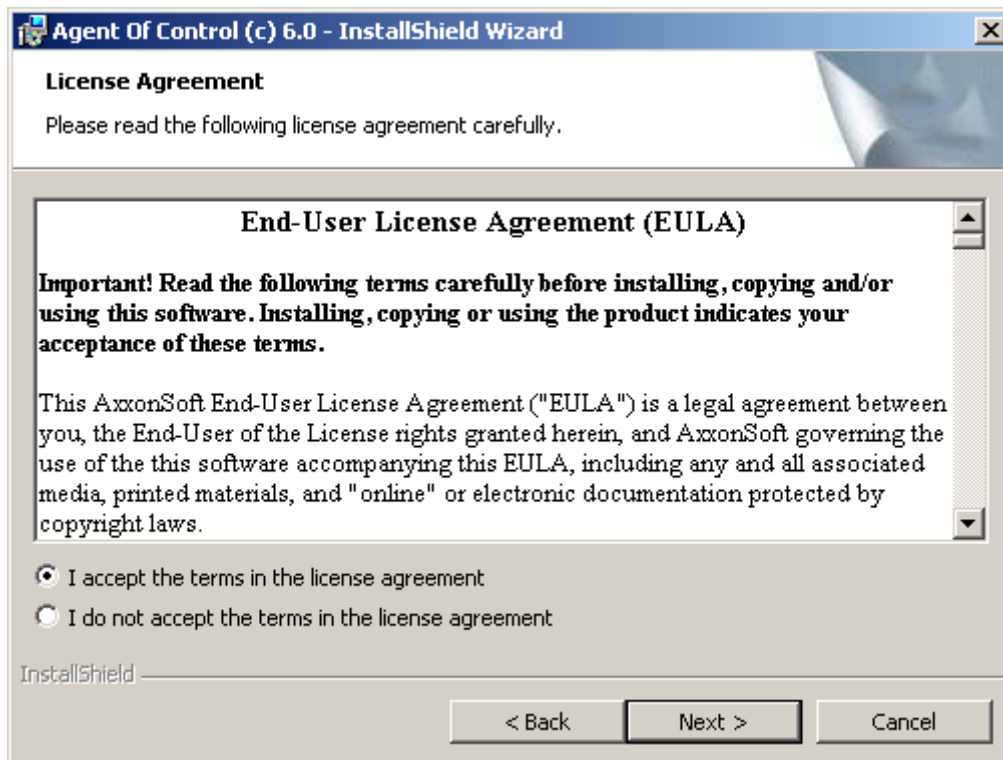


Fig. 3.3 – 3 License Agreement

4. In the window that appears, select the most appropriate installation type (Fig. 3.3 – 4). If Intellect is installed as a service, select the **Install Agent of Control (c) 4.8.3 as a service** check box. The ITV Monitoring VRecover service will be configured and added to the system. Otherwise, clear the check box.

After selecting an installation method, click the **Next** button.

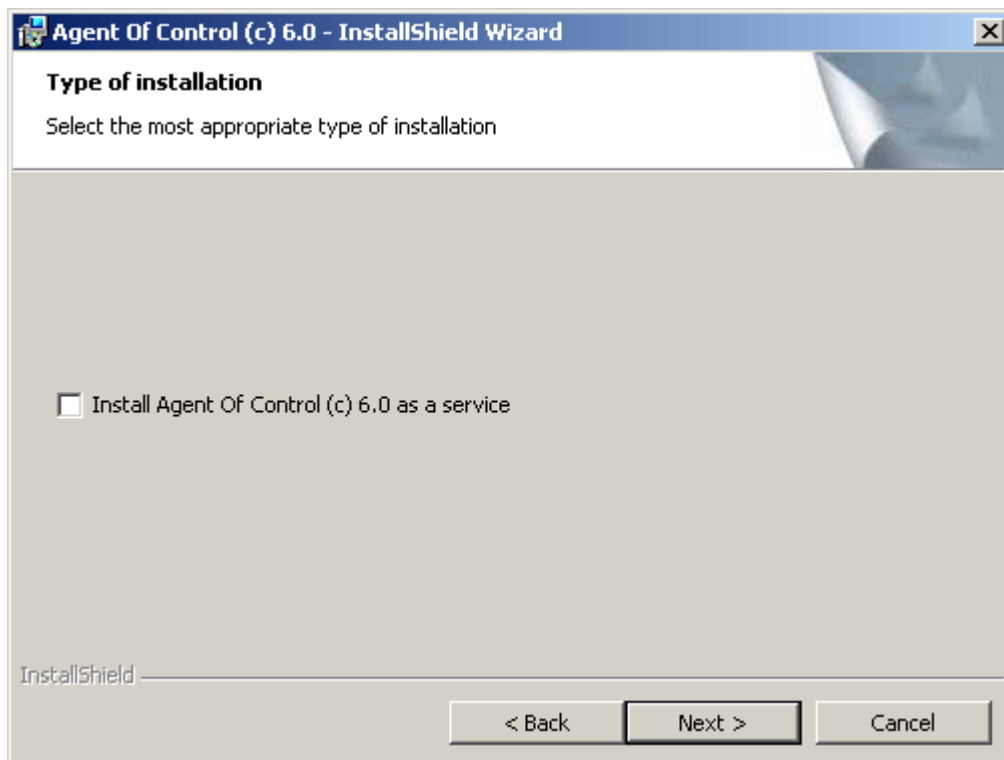


Fig. 3.3 – 4 Selecting an installation type

5. The installation process is started (Fig. 3.3 – 5).

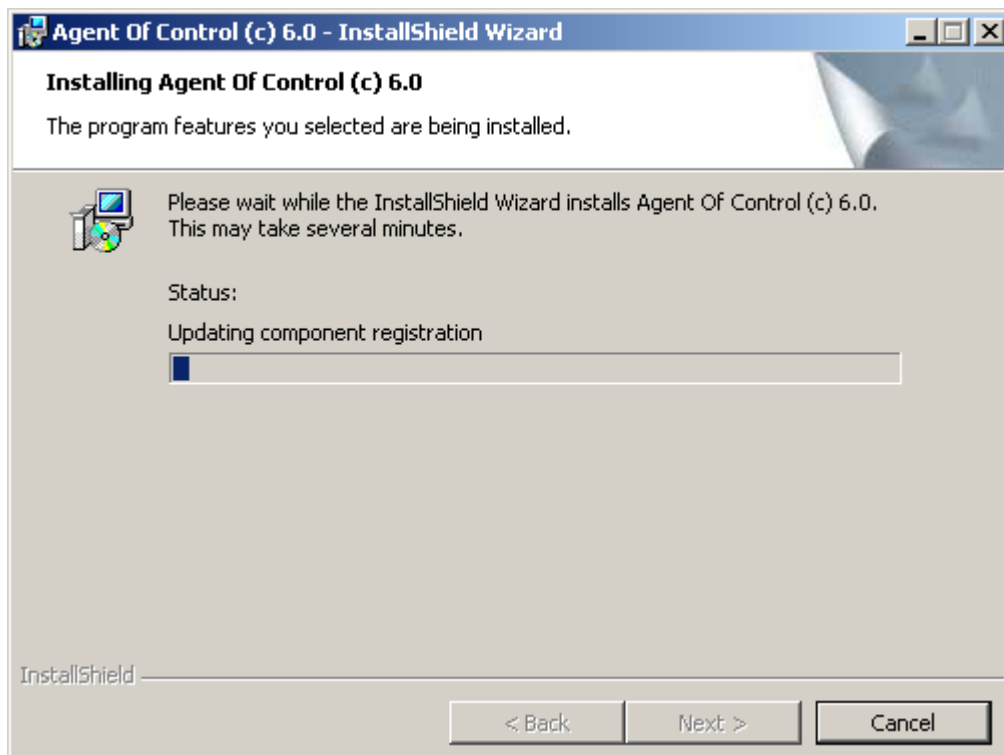


Fig. 3.3 – 5 Installation progress

6. When installation is complete, a wizard page appears with a message about successful installation (Fig. 3.3 – 6). Click the **Finish** button.

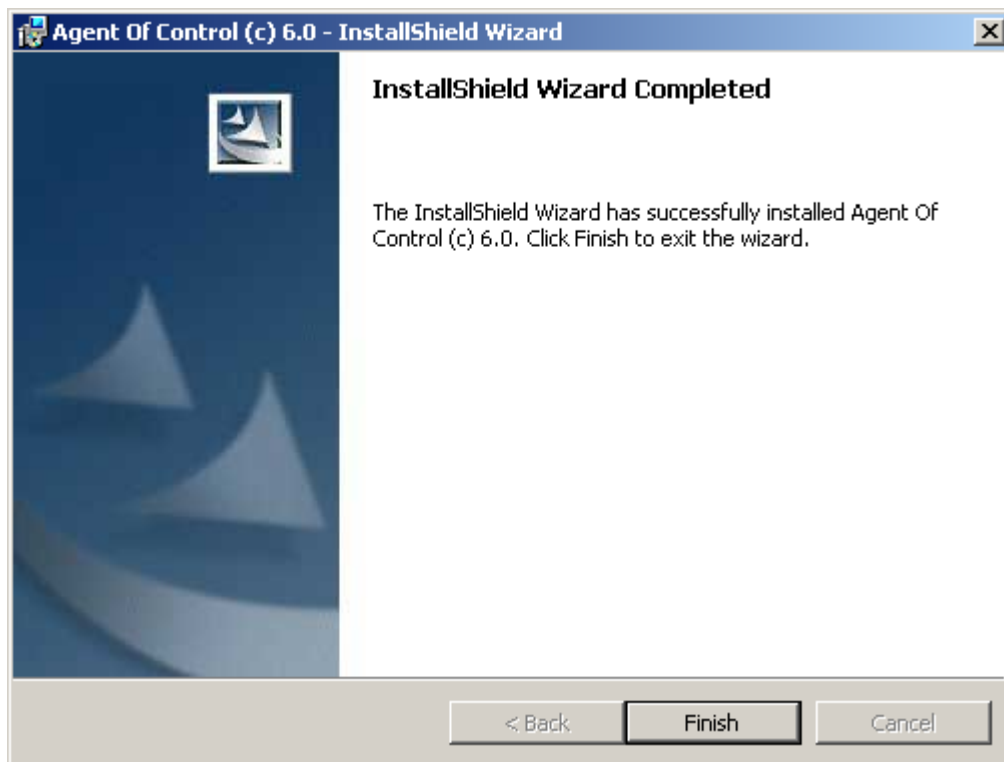


Fig. 3.3 – 6 End of installation

Installation of Agent of Control is now complete.

4 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*.

4.1 Creating necessary Agent of Control objects

Note. Agent of Control, as well as Server of Control, can operate in distributed architecture of the digital video surveillance system. In this case both Server of Control and Agent of Control shall be configured locally, not remotely.

Important: 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. Do not delete this folder.

To create an Agent of Control object in the device tree:

1. In the **System settings** window, go to the **Hardware** tab (Fig. 4.1 – 1, 1).
2. Create an **IIDK interface** object based on a **Computer** object (Fig. 4.1 – 1, 2). The ID of the **IIDK interface** object should be larger than 100 (Fig. 4.1 – 1, 3).



Fig. 4.1 – 1 IIDK interface object

3. Create an **Agent of Control** object based on a **Computer** object (Fig. 4.1 – 2).

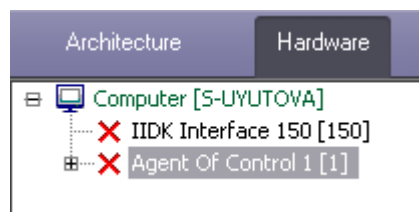


Fig. 4.1 – 2 Agent of Control object

4. After an **Agent of Control** object is created in the right part of the **System settings** window, a panel appears for configuring the object (Fig. 4.1 – 3).



Fig. 4.1 – 3 Configuration panel for the Agent of Control object

5. In the **IIDK Interface No.** field, enter the object ID for the **IIDK interface** created in step 2 (see Fig. 4.1 – 3).
6. Create one or more child **Partition Of Control** objects based on the Agent of Control object (Fig. 4.1 – 4).



Fig. 4.1 – 4 Partition Of Control object

7. After the **Partition Of Control** object is created in the right part of the **System settings** window, a panel appears for configuring the object (Fig. 4.1 – 5).

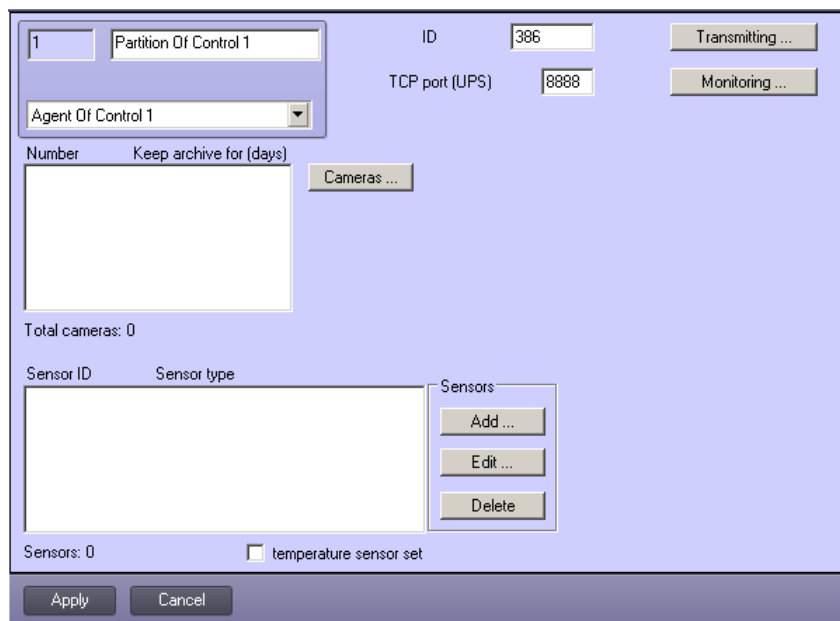


Fig. 4.1 – 5 Configuration panel for the Partition Of Control object

*Note: It is also necessary to create **Video input device**, **Camera**, and **Sensor** objects in the device tree that correspond to the connected hardware. Creation and configuration of these objects is described in the document *Intellect Software Package: Guide to Installation and Configuration of Security System Components*.*

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

4.2 Configuring the event log

The event log allows configuring the detail level at which the activity of Agent of Control is recorded.

To configure the event log:

1. Go to the configuration panel for an **Agent of Control** object (Fig. 4.2 – 1).

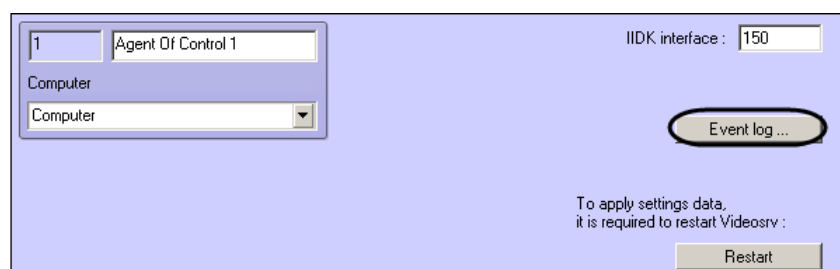


Fig. 4.2 – 1 Event log... button

2. Click the **Event log...** button (see Fig. 4.2 – 1).
3. In the dialog box that opens, specify the following parameters (Fig. 4.2 – 2):

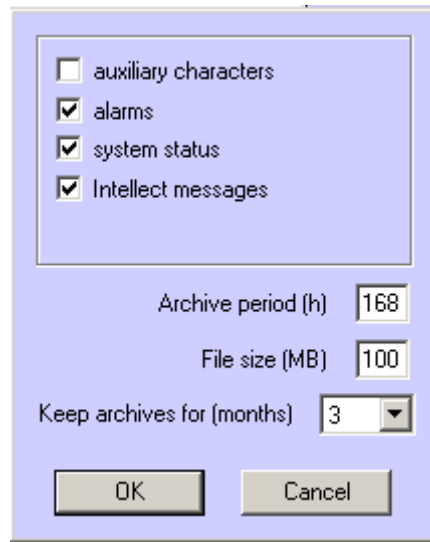


Fig. 4.2 – 2 Configuring the event log

3.1. **Auxiliary characters** . To log transport-level auxiliary characters, select this check box.

3.2. **Alarms** . To log alarms (activation of vibration sensor, temperature sensor, or forcible entry sensor), select this check box.

3.3. **System state** . To log events related to the system state, select this check box.

3.4. **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.

3.5. **Archive frequency (hrs)**.: Allows archiving the event log at the specified interval (in hours). Archives are saved in the DATA subfolder, with the following name format: namelog_yymmddhhmmss.gz, where

3.5.1. namelog is the name of the event log being archived

3.5.2. yy is the year of archive creation

3.5.3. mm is the month of archive creation

3.5.4. dd is the day of archive creation

3.5.5. hh is the hour of archive creation

3.5.6. mm is the minute of archive creation

3.5.7. ss is the second of archive creation

3.6. **File size (MB)**: Sets the threshold size (in megabytes) for the event log after which the file is archived. This setting overrides the value in the **Archive frequency** field.

4. **Store archives for (months)**: Sets the length of time for which to store the event log, in months (between 1 and 24). Archives that are older than the specified number of months are deleted.

The main event log 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 event log is now complete.

4.3 Configuring the Partition Of Control object

4.3.1 Configuring the Partition Of Control unique ID

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

1. Go to the configuration panel for the **Partition Of Control** object (Fig. 4.3 – 1).

Fig. 4.3 – 1 Configuring a unique Partition Of Control ID

2. In the **ID** field, enter a unique number for the object on which Agent of Control is being installed (see Fig. 4.3 – 1). The number can be from 3 to 9 digits long.
3. To save settings, click the **Apply** button.

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

4.3.2 Configuring a port for incoming UPS messages

To configure a port for accepting messages from an uninterrupted power supply unit:

1. Go to the configuration panel for the **Partition Of Control** object (Fig. 4.3 – 2).

Fig. 4.3 – 2 Configuring a port to accept incoming UPS messages

2. In the **TCP port (UPS)** field, enter the number of the port on which to "listen" for UPS messages (see Fig. 4.3 – 2).
3. To save settings, click the **Apply** button.

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

4.3.3 Configuring communication between Agent of Control and Control Server

To configure communication between Agent of Control and Control Server:

1. Go to the configuration panel for the **Partition Of Control** object (Fig. 4.3 – 3).

Fig. 4.3 – 3 Transport... button

- Click the **Transmitting...** button (see Fig. 4.3 – 3). A dialog box opens with settings for configuring the communication method between Agent of Control and Control Server (Fig. 4.3 – 4).

Connection to Control Server

Connection mode: Client mode

Connection type: TCP/IP

RS232

COM port: Com1

COM port speed: 9600

COM port format: 8N1

TCP/IP

TCP port: 7777

IP address: 0 . 0 . 0 . 0

I/O buffer (bytes): 4096

Ping frequency (sec): 120

OK Cancel

Fig. 4.3 – 4 Configuring communication

- In the **Connect to Control Server** drop-down list select the **Client mode** as the methods for connecting Agent of Control to Control Server (see Fig. 4.3 – 4, 1).
- Note. The **Server mode** is not used.*
- In the **Link type** drop-down list, select one of the possible values for the transport level (see Fig. 4.3 – 4, 2): **TCP/IP** or **RS232**.
 - If **RS232** is selected in the **Link type** field, specify values in the **Number**, **Bit rate**, and **COM port shorthand notations** fields (see Fig. 4.3 – 4, 3).
 - If **Client mode** is used to connect to Control Server and **TCP/IP** is selected in the **Link type** field, in this dialog box you should indicate the **IP address** and **TCP port** of Control Server (see Fig. 4.3 – 4, 4).
 - When still frames or video is sent to Control Server, the data is transferred in packets. The packet size is specified by the setting named **Transfer buffer (bytes)** (see Fig. 4.3 – 4, 5). For maximum data transfer speed, you are advised to use the value 4096. For poor connections, such as if a GSM modem is used, you are advised to use the value 800.
 - In the **Ping frequency (sec.)** field, enter the time interval at which Agent of Control will send messages about its technical state to Control Server (if **Client mode** is selected) (see Fig. 4.3 – 4, 6). The value in the **Ping frequency (sec.)** field does not affect short-term alarms. Messages about short-term alarms are transmitted from *Agent of Control* to *Server of Control* immediately after corresponding sensors triggering.
 - Click **OK** (see Fig. 4.3 – 4 , 7).

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

4.3.4 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. There is also a separate additional device, "temperature array".

*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 *Guide to Installation and Configuration of Security System Components*.*

Important: Sensor IDs must be whole numbers.

Attention! 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 Appendix 1. 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 (Fig. 4.3 – 5).

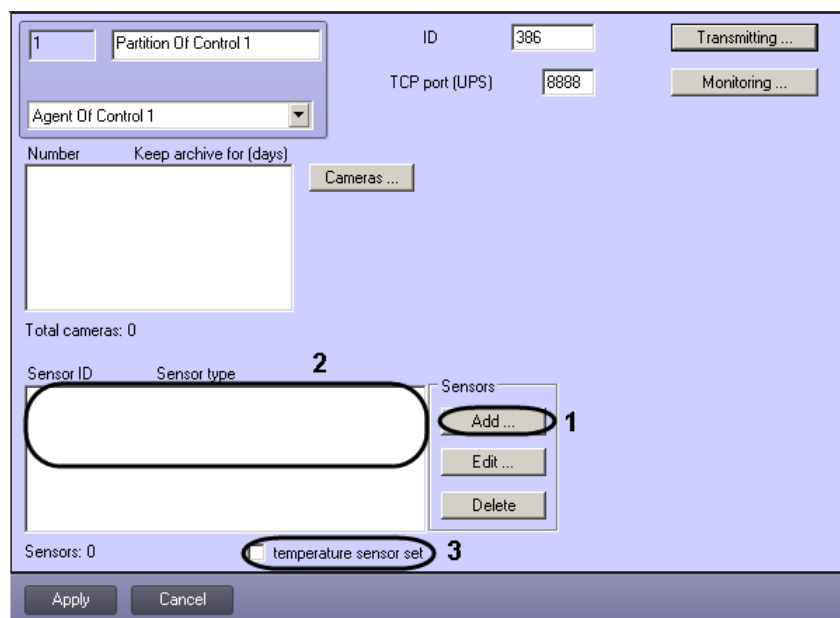


Fig. 4.3 – 5 Adding a sensor

2. Click the **Add** button (see Fig. 4.3 – 5, 1). A dialog box for adding a sensor appears (Fig. 4.3 – 6).

Fig. 4.3 – 6 Configuring a sensor

3. In the **Type** drop-down list, select the type of sensor from the sixteen types described previously (see Fig. 4.3 – 6, 1).
4. In the **Name** field, enter the text that will be sent to Control Server together with the alarm message. This text will be overlaid on the video during the captioning process (Fig. 4.3 – 6, 2).
5. In the **ID** drop-down list, select a **Sensor** object that has been previously created in the Intellect device tree (see Fig. 4.3 – 6, 3).
6. In the **Attach to camera** drop-down list, select a **Camera** object that has been previously created in the Intellect device tree (see Fig. 4.3 – 6, 4).
7. To enable sending video frames to Control Server when a sensor is activated, select the **transmit snapshots** check box (see Fig. 4.3 – 6, 5). In the **Attach to camera** field, specify the camera from which you want video frames to be sent (see Fig. 4.3 – 6, 4).

Note: The settings for sending video frames and for sending video fragments are different.

8. If you want for a video fragment to be sent to Control Server when a sensor is triggered, select the **transmit video** check box (see Fig. 4.3 – 6, 6). In the **Attach to camera** field, specify the camera from which you want video frames to be sent (see Fig. 4.3 – 6, 4).
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 (see Fig. 4.3 – 6, 7). The default value is 20 seconds.
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 (see Fig. 4.3 – 6, 8). This allows obtaining video frames depicting not only the very moment at which an alarm occurs, but a short time before.
11. In the **Number of frames** drop-down list, select the quantity of video frames to be transferred when a sensor is triggered (for **video frame transmission** mode) (see Fig. 4.3 – 6, 9).

12. In the **Interval (sec.)** field, enter the length of time, in seconds, between video frames if more than one frame is to be sent (see Fig. 4.3 – 6, 10). Thus when an alarm occurs, it is possible to send to Control Server an entire sequence of frames that represent different points in time, which increases the chance of viewing the most valuable frames (for **video frame transmission** mode).

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 Appendix 1. Sample script for stopping camera recording)

Important: When specifying the Lookback, 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 time setting (Fig. 4.3 – 7).

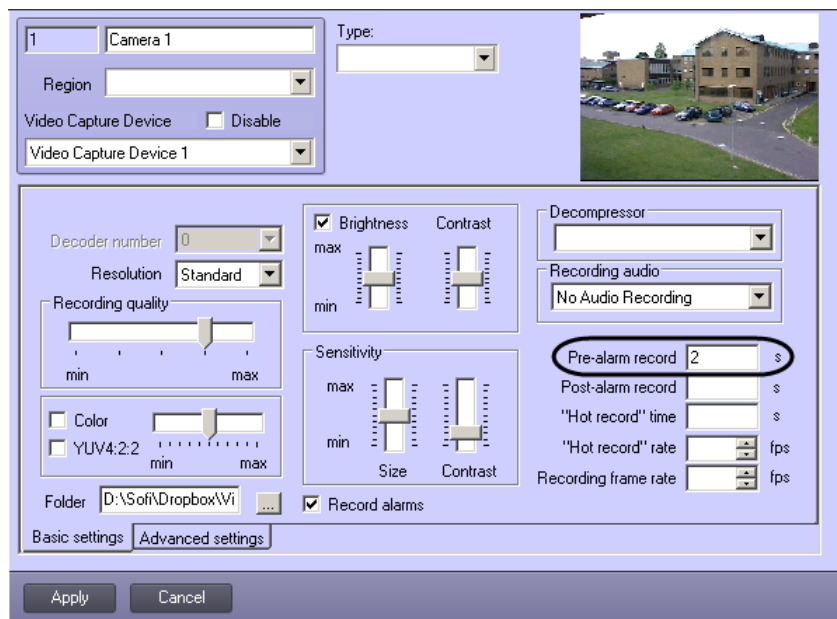


Fig. 4.3 – 7 The Pre-Alarm time setting on the configuration panel of the Camera object

13. In the **Length (sec.)** field, specify the length of the video fragment to send (for **video fragment transmission** mode).

Attention! This setting is unavailable in the current version (Fig. 4.3 – 8, 1). 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 Appendix 1. Sample script for stopping camera recording).

Fig. 4.3 – 8 Length and Rate settings

14. In the **Rate (KB/sec.)** field, enter the transmission rate for the video fragment (for **video fragment transmission** mode) (see Fig. 4.3 – 8, 2).
15. To overlay captions on video when a sensor is triggered, select the **captioning** check box (). In the **Attach to camera** field, specify the camera on whose video you want to overlay captions (see Fig. 4.3 – 6, 11).
16. In the **Show (sec.)** drop-down list, select the amount of time for which you want captions to be displayed on video, in seconds (see Fig. 4.3 – 6, 12).
17. Click **OK** (see Fig. 4.3 – 6 , 13).
18. To perform monitoring to ensure that temperatures do not deviate from an allowed range, select the **Temperature array** check box (see Fig. 4.3 – 5, 3). A set of DS18S20-type temperature sensors is used for temperature monitoring. Temperature sensors are connected via a two-wire MicroLAN to a MicroLAN network adapter, which in turn connects to the COM port of the computer on which Agent of Control is installed. The MicroLAN network adapter can be connected to the USB port of the computer on which Agent of Control is installed, by adding a RS232–USB adapter.

Configuration of the list of used sensors is now complete.

4.3.5 Configuring captions

To use and configure captions, for each camera on which you want to use captions you must create a **Captioner** object (Fig. 4.3 – 9).

***Important:** If multiple captioners have been created for a single camera, Agent of Control uses the captioner with the lowest ID number.*

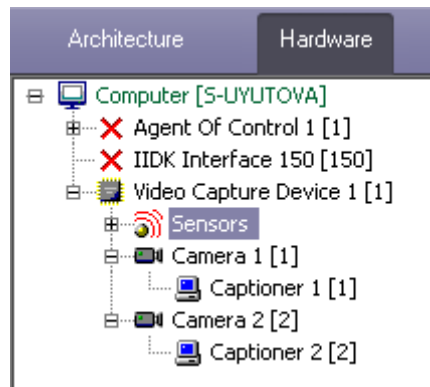


Fig. 4.3 – 9 Captioner objects in the device tree

To configure the font and display area used for captions:

1. In the device tree, click the relevant **Captioner** object. On the right side of the **System settings** dialog box, the configuration panel of the **Captioner** object is displayed (Fig. 4.3 – 10).

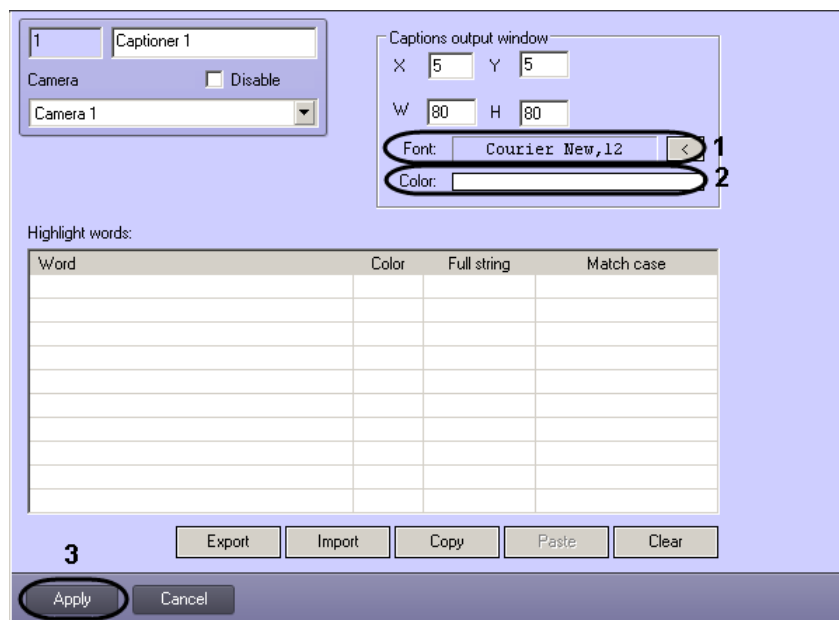


Fig. 4.3 – 10 Configuring caption color and font

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 (see Fig. 4.3 – 10, 1).

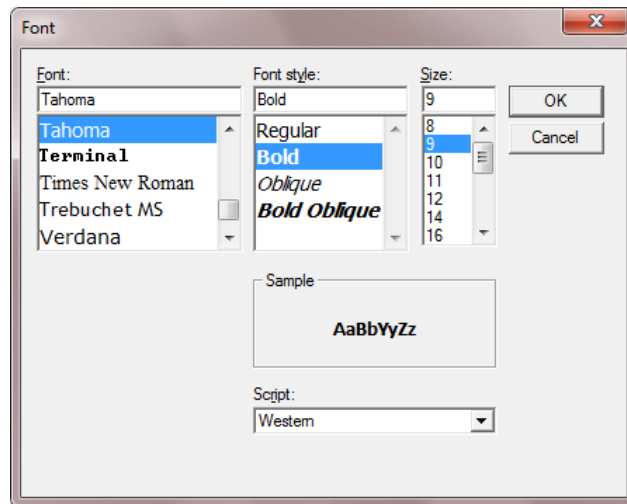


Fig. 4.3 – 11 Configuring the font

3. To configure the color of captions, double-click the area to the right of **Color**. A dialog box for configuring color appears (see Fig. 4.3 – 10, 2).

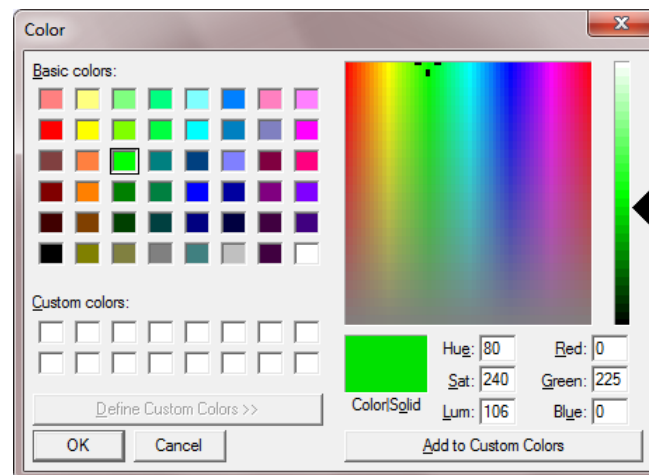


Fig. 4.3 – 12 Configuring colors

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

4.3.6 Configuring the camera list

The list of cameras specified in the configuration panel for the **Partition Of Control** object defines the cameras whose archives can be accessed through the **Search in Archive** interface object (see the document *Monitoring Software Package: User's Guide*). In addition, this list defines 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. Control Server receives information about the number of cameras, disks, disk volume, etc.
2. If no cameras are specified in the list, Agent of Control checks for the presence of a **Long-term Archive** object in the system and gets information about disks from this object. In this case,

Control Server will receive information only for the disks marked in the **Long-term Archive** object. Access to the archive is not performed from the **Search in Archive** interface object during this process.

3. If no cameras are indicated in Agent of Control settings and there is no **Long-term Archive** object in the configuration, information about disks is taken from the **Computer** object; the disks indicated 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 **Long-term Archive** object is described in the document **Intellect Software Package: Administrator's Guide**.*

To configure the list of cameras in use:

1. Go to the configuration panel for the **Partition Of Control** object (Fig. 4.3 – 13).

Number	Keep archive for (days)
1	60

Sensor ID	Sensor type
-----------	-------------

Fig. 4.3 – 13 Adding a camera

2. Click the **Cameras...** button (see Fig. 4.3 – 13). The **Add/edit cameras** window opens (Fig. 4.3 – 14).

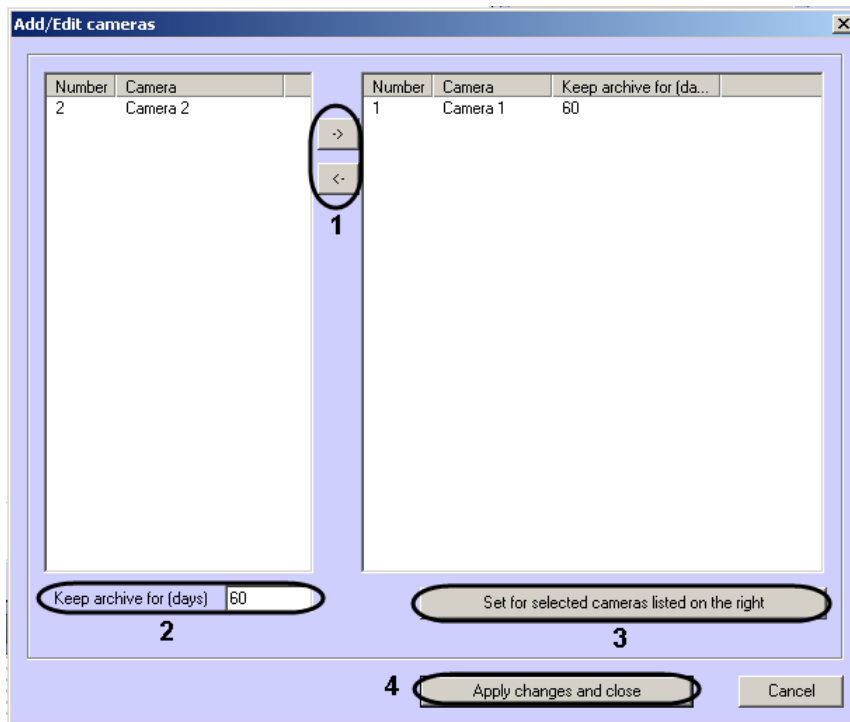




Fig. 4.3 – 14 Adding/editing cameras

3. Configure the necessary cameras by clicking the  and  buttons to move cameras from the left list to the one on the right (see Fig. 4.3 – 14, 1).
4. Select cameras in the list on the right.
5. Specify the time for video archive storage, in days (see Fig. 4.3 – 14, 2).
6. Click the **Set for cameras selected in the right list** button.
7. Repeat steps 4 to 6 for all necessary cameras.
8. Click the **Apply changes and close** button (see Fig. 4.3 – 14, 3). The selected cameras will be added to the list on the configuration panel of the **Security Site** object.
9. Click the **Apply** button.

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

Configuration of the camera list is now complete.

4.3.7 Configuring alarm groups

For the **Access Control** and **Detection Tools** alarm groups, by default 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 (Fig. 4.3 – 15) and configure it (select the **Abandoned Object Detection Tool**

type, specify the detection area and sensitivity, etc.; for more details, see the document *Intellect Software Package: Administrator's Guide*.

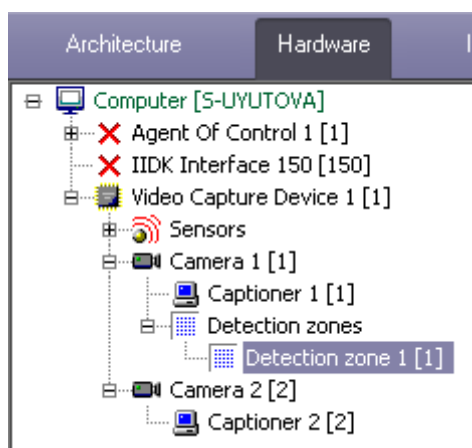


Fig. 4.3 – 15 Detector Zone object

To associate various events with particular alarm groups:

1. Go to the configuration panel for the **Partition Of Control** object (Fig. 4.3 – 16).

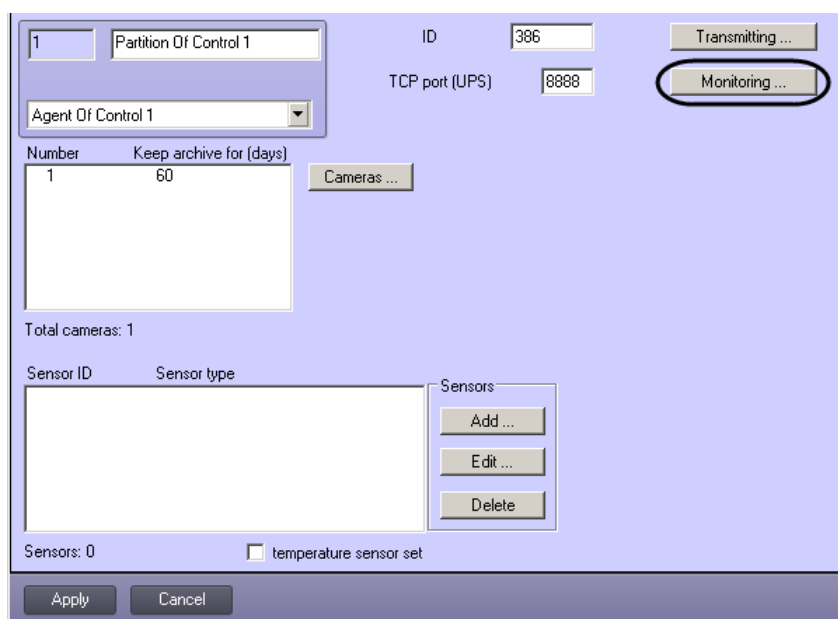


Fig. 4.3 – 16 Monitoring button...

2. Click the **Monitoring** button (see Fig. 4.3 – 16). The **Add/Remove Monitoring Events** window opens (Fig. 4.3 – 17).

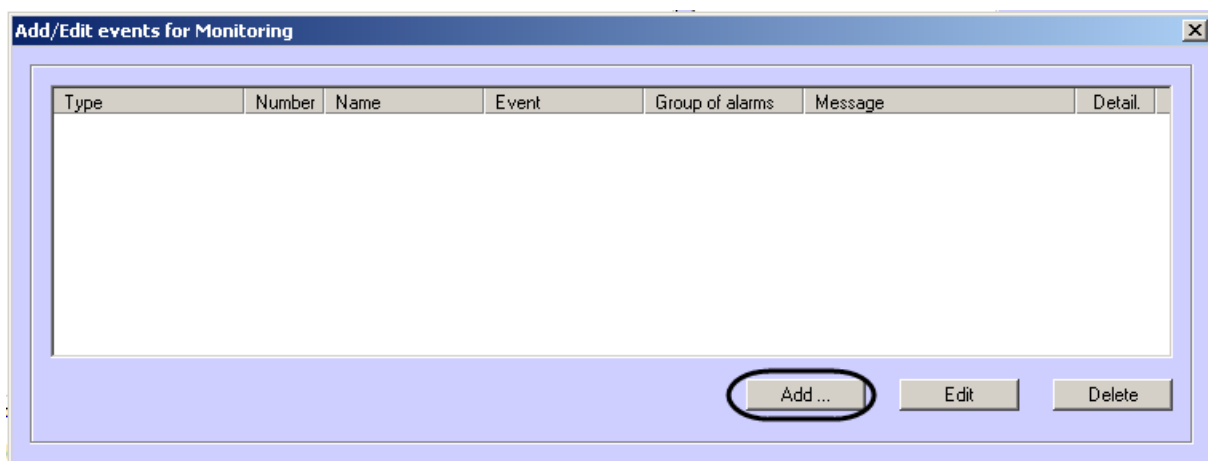


Fig. 4.3 – 17 Adding/removing events for Monitoring

3. To add an event, click the **Add...** button (see Fig. 4.3 – 17). The event configuration window opens (Fig. 4.3 – 18).

Fig. 4.3 – 18 Event configuration

4. In the form that appears, in the **Type** drop-down list, select the type of device (see Fig. 4.3 – 18, 1). 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. Select an ID number for the object of the selected type from which you want to get events (see Fig. 4.3 – 18, 2). If you want to get events from all devices of this type, leave this field blank.
6. In the **Event** drop-down list, select an event type (see Fig. 4.3 – 18, 3). The available event types depend on the selected object type.
7. In the **Alarm group** drop-down list, select an alarm group and indicate in which alarm group you want for Monitoring to display alarms for this event (see Fig. 4.3 – 18, 4).

8. Enter text in the **Message** field (see Fig. 4.3 – 18, 5). The text entered in this field will appear in the **Device** column of the **Alarm Reaction** dialog form (see the document *Monitoring Software Package: User's Guide*).
9. To search for additional information in messages from a device of this type (for the substring "param0<>"), select the **Intercept detail** check box (see Fig. 4.3 – 18, 6).

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 **Intercept detail**, the following text may appear in the **Device** column of the **Alarm Reaction** dialog form: "Motherboard (CPU cooler)".

Example of how to configure the message for the Abandoned Object Detection Tool (Fig. 4.3 – 19).

Fig. 4.3 – 19 Configuring message for the Abandoned Object Detection Tool

*In the example shown with the Abandoned Object Detection Tool, when the detection tool is triggered a indicator corresponding to the **Detection Tools** alarm group becomes red in the Control Panel (Fig. 4.3 – 20).*



Fig. 4.3 – 20 Reaction to triggering of detection tool in the Control Panel

*Click this indicator to view the **Alarm Reaction** window, which indicates that the Abandoned Object Detection Tool has been triggered (Fig. 4.3 – 21).*

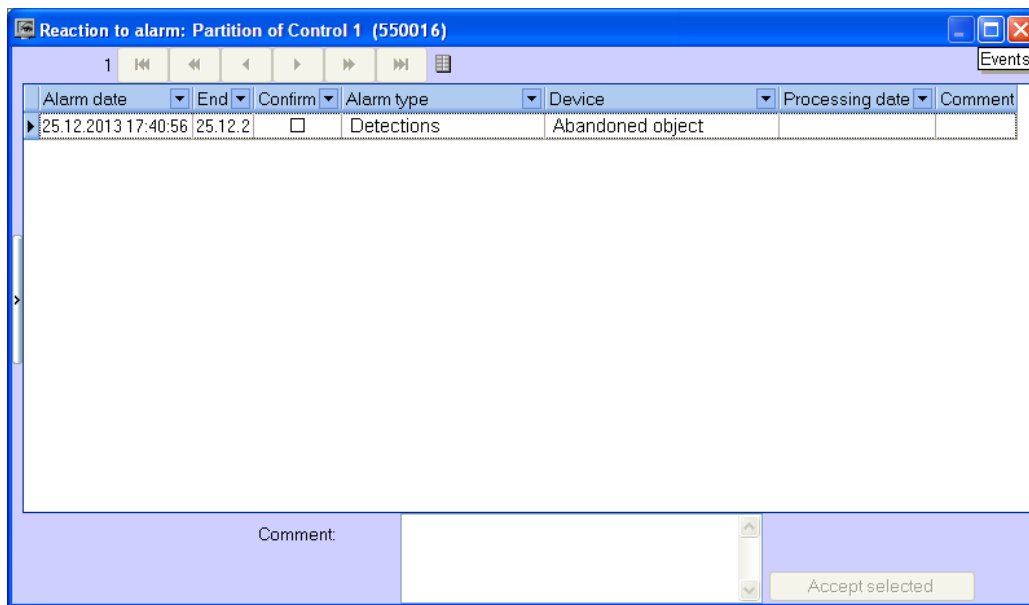


Fig. 4.3 – 21 Alarm Reaction window for the Abandoned Object Detection Tool

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

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

4.4 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 Control Server.

Configuration of a UPS is performed in the following order:

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

4.4.1 Installing StateUPS

To start, configure the StateUPS auxiliary utility.

1. Create a folder on disk, such as C:\EVUPS. To this same location, copy the file StateUPS.exe from the UPS folder in the installation kit.
2. Configure the file StateUPS.ini, which is also in the UPS folder of the installation kit:
 - 2.1. 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.
 - 2.2. 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*).

3. After the file StateUPS.ini is configured, it must be copied to the system folder of the operating system (OS). For example, if Windows is installed in the folder C:\WINNT, the file StateUPS.ini must be copied to the folder C:\WINNT\System32\.
4. Then install the software from the UPS vendor. Before starting installation, make sure that the interface cable is connected to the UPS.
 - 4.1. 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 (Fig. 4.4 – 1).

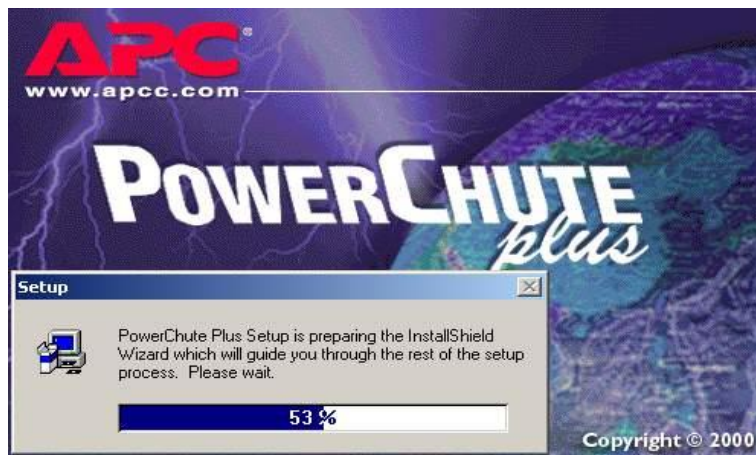


Fig. 4.4 – 1 Preparing for installation

- 4.2. On the following wizard page, select the option **Continue with the installation now** and click the **Next** button (Fig. 4.4 – 2).

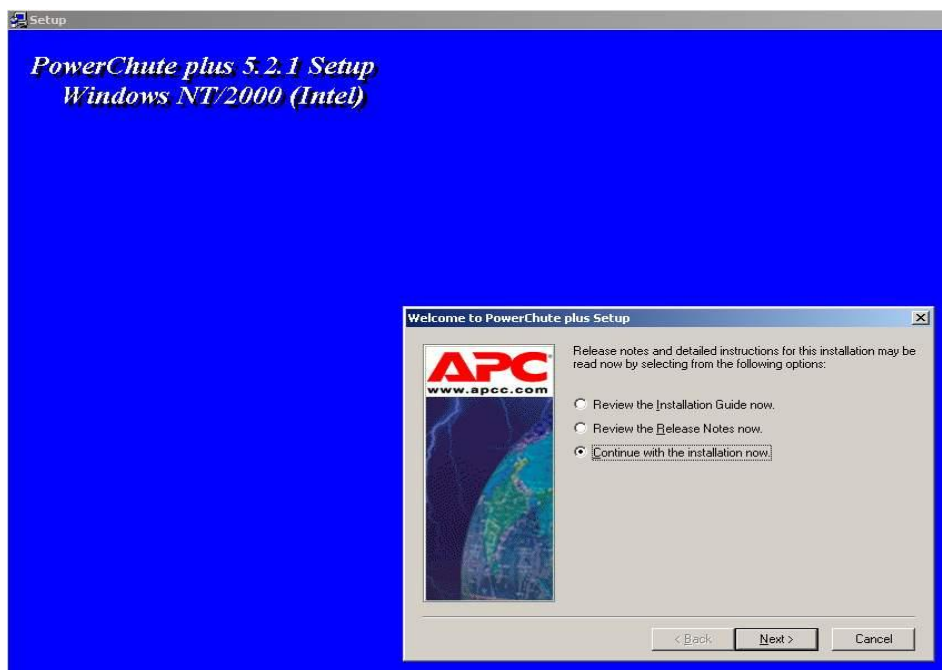


Fig. 4.4 – 2 Selecting an installation method

- 4.3. On the following wizard page, click the **Yes** button to accept the license agreement (Fig. 4.4 – 3).

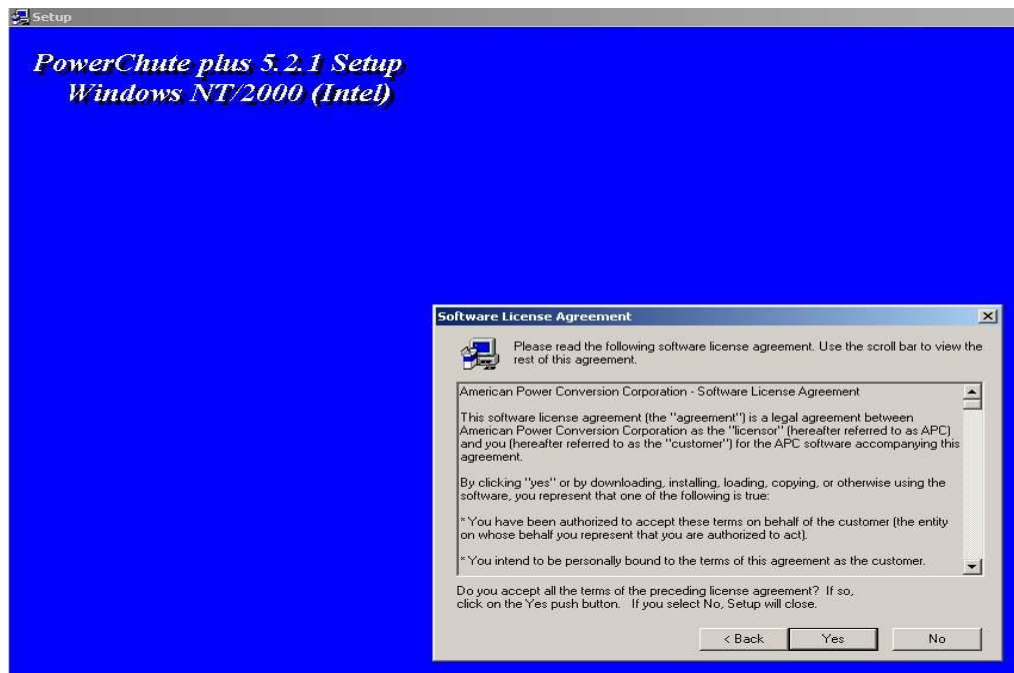


Fig. 4.4 – 3 License Agreement

4.4. On the following wizard page, select the **Typical** installation type and indicate the path at which you want to install the software (Fig. 4.4 – 4).

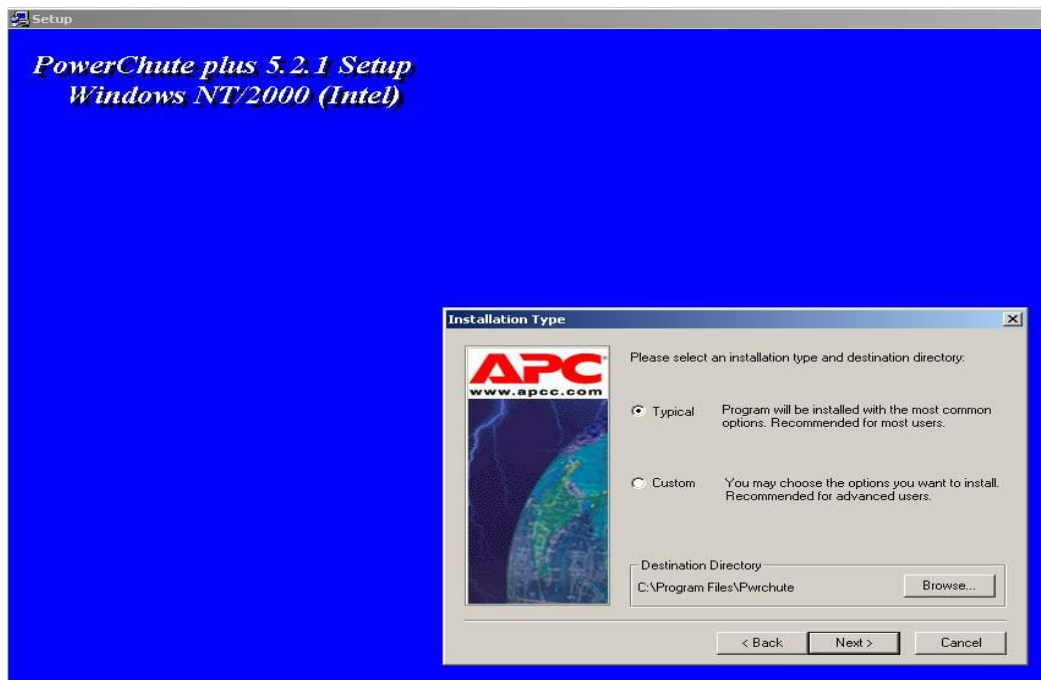


Fig. 4.4 – 4 Selecting the installation type and path

4.5. Copying begins of the necessary files (Fig. 4.4 – 5).

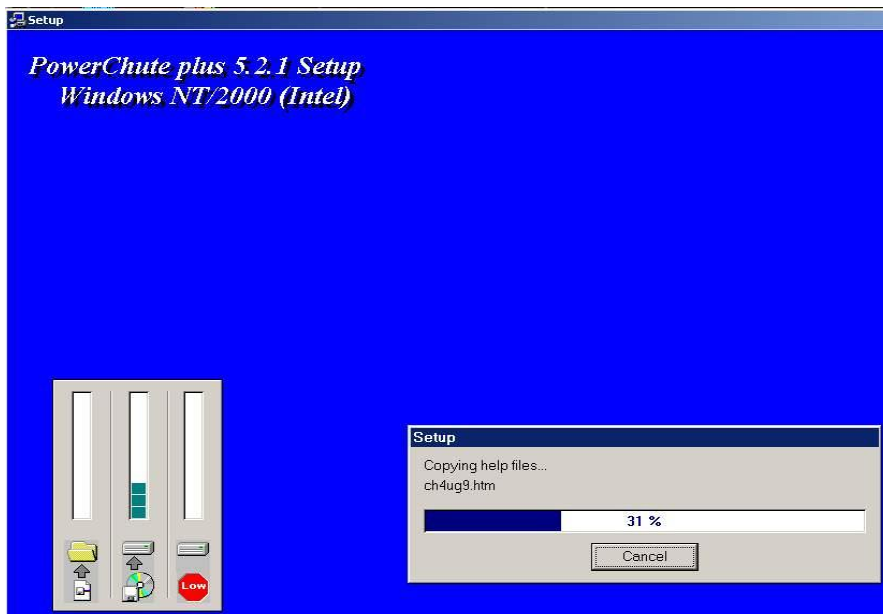


Fig. 4.4 – 5 Process of copying program files

- 4.6. When copying is complete, a dialog box appears with a request to automatically determine the COM port on which the UPS is located (Fig. 4.4 – 6). Click the **Yes** button.

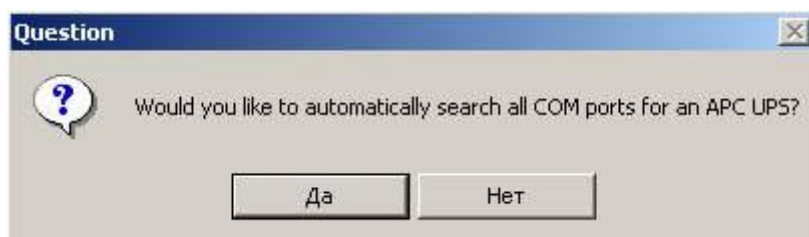


Fig. 4.4 – 6 Request for automatic UPS search

- 4.7. The search process begins (Fig. 4.4 – 7).



Fig. 4.4 – 7 Searching for UPS

- 4.8. When the search is complete, the program will show what type of UPS it found and on which COM port (Fig. 4.4 – 8). Click the **Next** button.

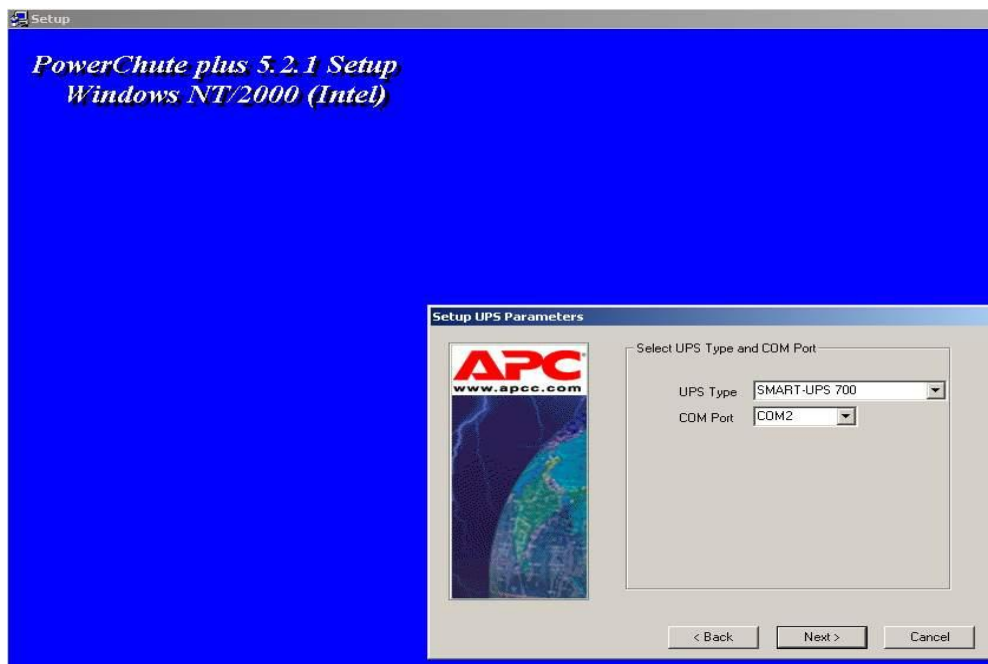


Fig. 4.4 – 8 Found UPS units

- 4.9. On the next wizard page, clear the **Enable PowerChute plus remote monitoring** check box and click the **Next** button (Fig. 4.4 – 9).

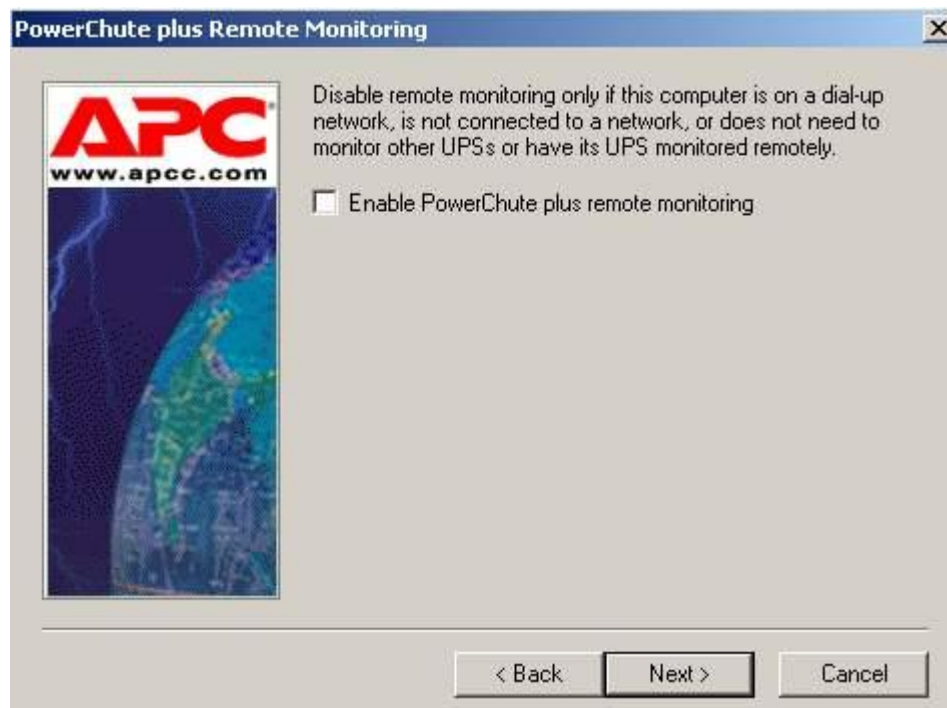


Fig. 4.4 – 9 Configuring remote monitoring

- 4.10. The two following wizard pages complete the installation process (Fig. 4.4 – 10, Fig. 4.4 – 11).

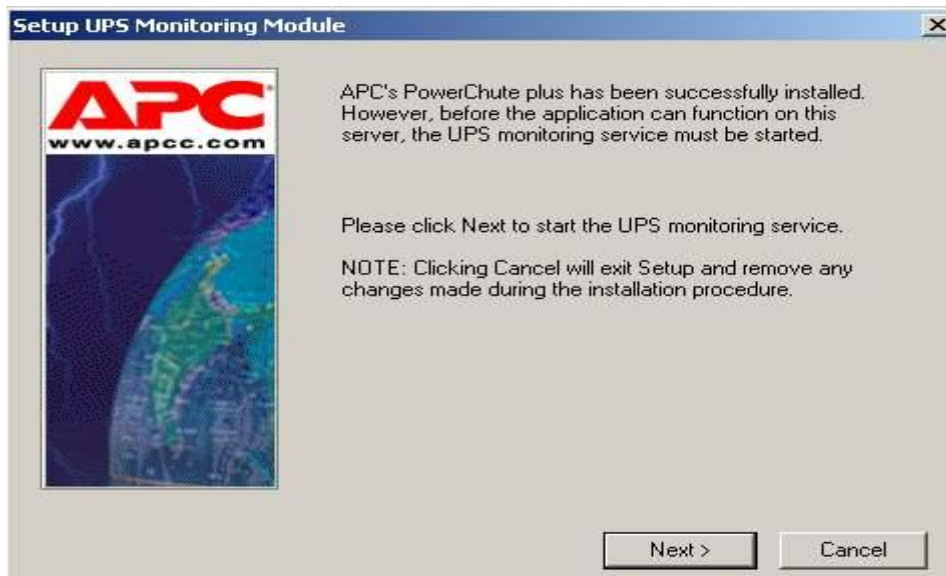


Fig. 4.4 – 10 End of installation



Fig. 4.4 – 11 Confirmation of end of installation

Installation of the StateUPS utility is now complete.

4.4.2 Installing 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** (Fig. 4.4 – 12).

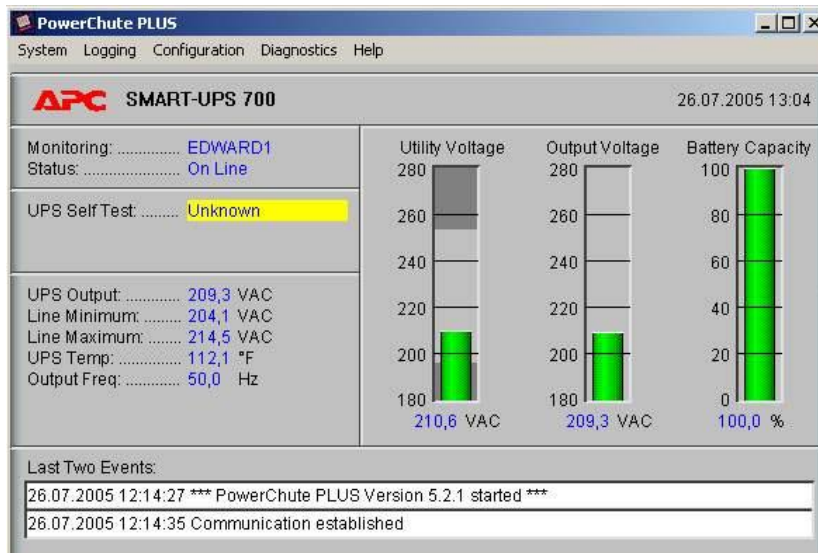


Fig. 4.4 – 12 Program window

2. Select the menu item **Configuration -> Event Actions...** A dialog box appears (Fig. 4.4 – 13), 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.

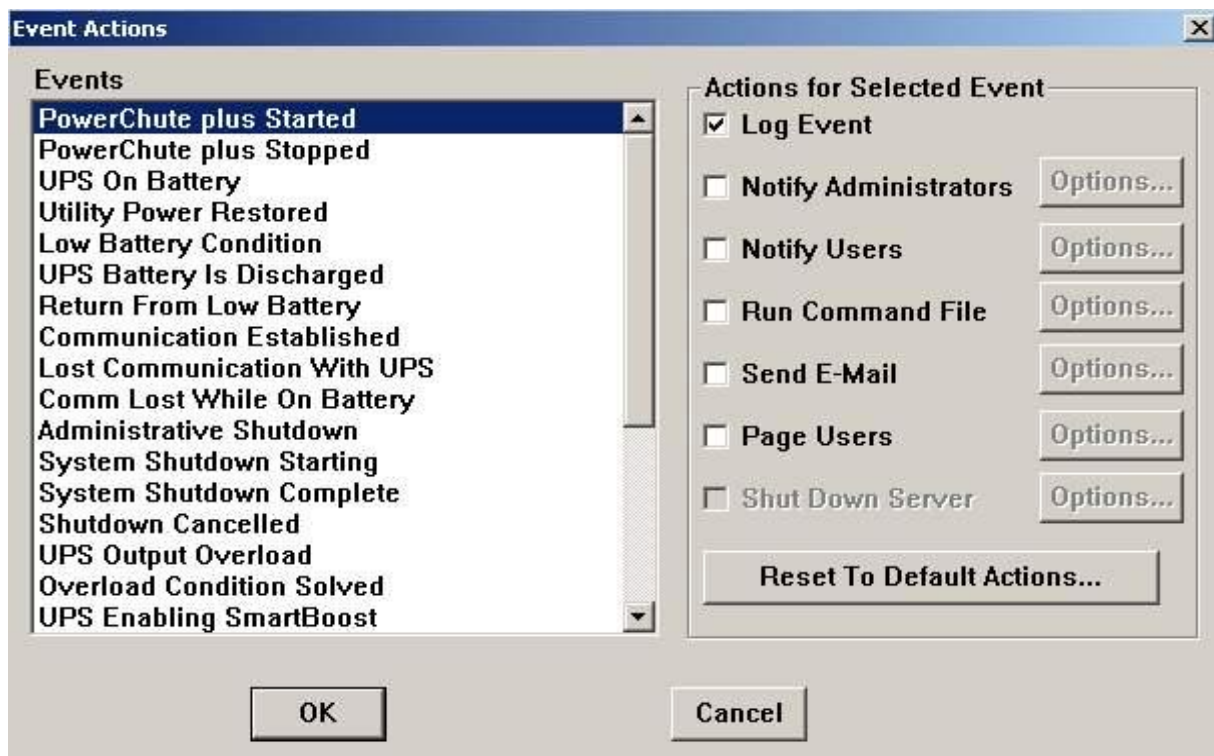


Fig. 4.4 – 13 Utility events and reactions

A more detailed list of events is given in Tab. 4.4 – 1.

Tab. 4.4 – 1 Description of UPS events

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	Battery 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 Control Server.

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

The installation package 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 from the command line.

4.4.3 Example of configuration of event distribution

Let us imagine that we are interested in situations when 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).

1. In the list of events, select the event **UPS On Battery** and, for this event, select the **Run Command File** check box (Fig. 4.4 – 14).

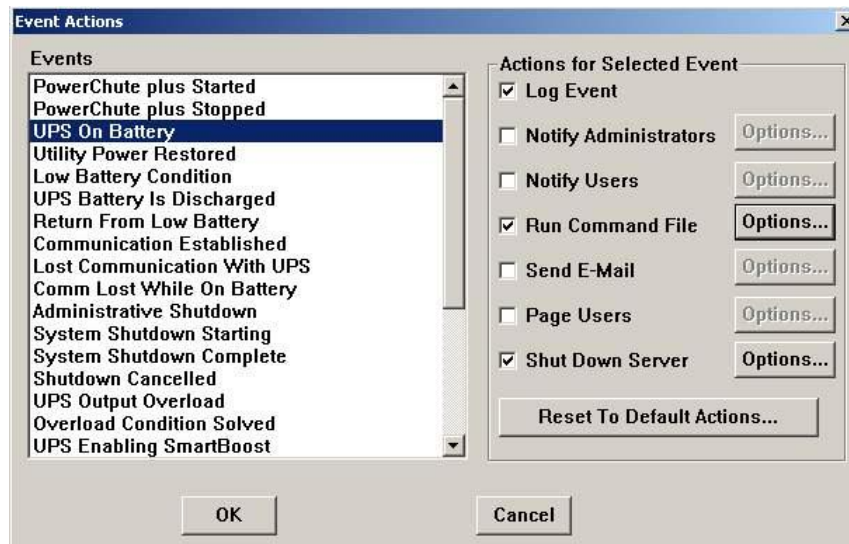


Fig. 4.4 – 14 Configuring UPS On Battery events

2. To the right of **Run Command File**, click the **Options...** button (see Fig. 4.4 – 14).
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 (Fig. 4.4 – 15).

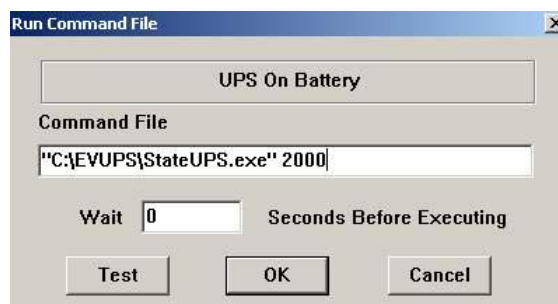


Fig. 4.4 – 15 Path to the StateUPS utility for the UPS On Battery event

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 (see Tab. 4.4 – 1).

4. Similar actions for the **Utility Power Restored** event are shown in Fig. 4.4 – 16 and Fig. 4.4 – 17.

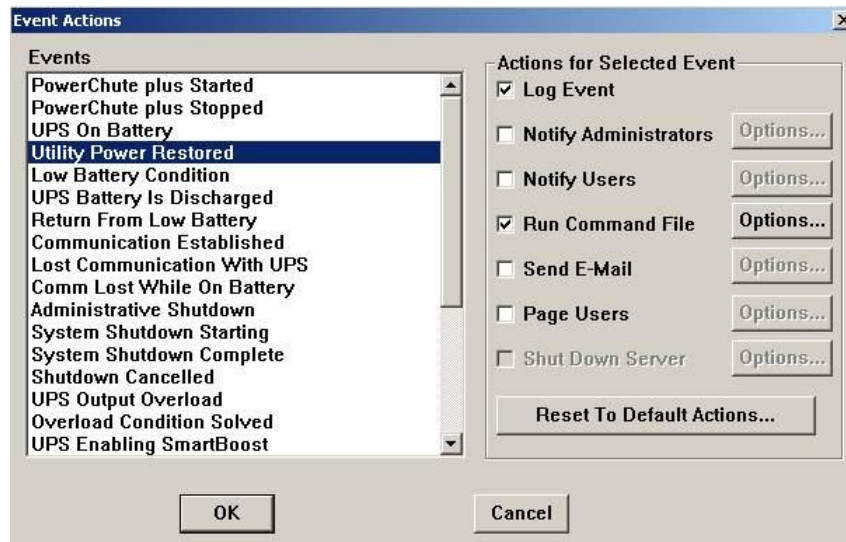


Fig. 4.4 – 16 Configuring the Utility Power Restored event

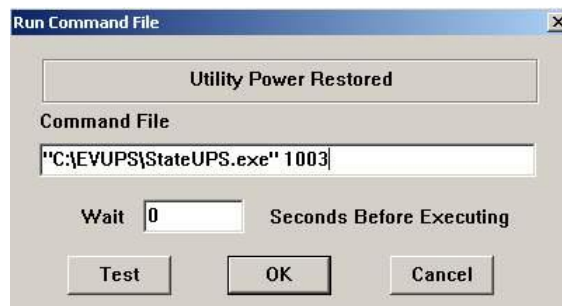


Fig. 4.4 – 17 Path to the StateUPS utility for the Utility Power Restored event

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 OS system folder (System32) with a name of the following format:

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

5 Appendix 1. 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 on the **Programming** tab of the **System settings** window in Intellect, based on the example below.

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

```
OnEvent("GRAY","1","ALARM")

{
[
    DoReact("CAM","1","REC_ROLLBACK");

    Wait(5);

    DoReact("CAM","1","REC_STOP");
]
}

OnEvent("GRAY","1","ALARM")

{
[
    Wait(2);

    DoReact("GRAY","1","CONFIRM");

    Wait(2);

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

When continuous recording is in use, the following program should be used:

```
OnEvent("GRAY","1","ALARM")

{

[

    Wait(5); // Specifies the time after which the recording should be stopped in order to get the
required clip length or number of frames

    DoReact("CAM","1","REC_STOP");

    Wait(2); // Pre-alarm record time in the camera settings = 2 sec.

    DoReact("CAM","1","REC_ROLLBACK"); // Start recording with pre-alarm recording of 2 seconds.
This allows us not to lose data in the archive

]

}
```