



# ADMINISTRATOR'S GUIDE



---

# Table of Contents

Customer support .....	5
Basic information .....	7
Scope and feature summary .....	8
System requirements .....	15
Video server .....	16
Selecting the number of disks for an archive .....	17
Compatible operating systems .....	18
Compatible IP equipment .....	19
Storage devices for the TRASSIR Lanser-4Mobile and the TRASSIR Lanser-Mobile II .....	20
Installation .....	21
Installing compression cards .....	22
TRASSIR Lanser IP-video server installation .....	23
Network settings for TRASSIR Lanser video servers .....	27
NAS Setup .....	30
Configuring a QNAP Turbo NAS .....	31
Connecting a network storage in a Windows OS .....	36
Installing Guardant USB keys .....	39
Windows OS settings .....	40
Installing TRASSIR server software .....	54
TRASSIR Server software installation as Windows service .....	58
Installing TRASSIR client software .....	63
PostgreSQL DBMS installation .....	66
Configuring the operating system to work with the PostgreSQL DBMS .....	69
Starting the PostgreSQL Database Server service .....	71
Moving a PostgreSQL database to a different server .....	74
Allowing external connections to the PostgreSQL DBMS .....	78
Connecting analog PTZ cameras .....	80
Working with the basic interface .....	82
Start the software and sign into the system .....	83
First launch of the TRASSIR Server software .....	84
Watchdog .....	85
System login .....	86
Main control panel .....	88
Settings window .....	90
Video monitor .....	91
Settings .....	92
Local server settings .....	93
Remote server settings .....	96
Client settings .....	97
Software Update .....	98
Logs and dumps .....	99
TRASSIR Cloud .....	100
Connecting server to TRASSIR Cloud .....	101
Client connection to TRASSIR Cloud .....	103
Cloud cameras in TRASSIR .....	105
Archive .....	106
Archive setup on the server .....	107
Archive setup on the client .....	110
Encrypting an archive .....	112
Creating and setting up RAID for archive record .....	114
Configuring a network storage connection in Linux-based TRASSIR OS .....	119
Recording network channels .....	121
Archive merge .....	122
Configuration of the archive merge session on the source server .....	125
Reviewing the archive merge session on the destination server .....	127



Screenshot management .....	128
Web server (SDK) .....	129
Configuring a server to work with the TRASSIR SDK .....	130
Access to TRASSIR WEB-interface .....	132
Map .....	134
Creating a map .....	135
Adding cameras .....	136
Adding floor to the map .....	138
Adding teleports .....	140
Reports .....	142
Report template settings .....	143
Database connection settings .....	144
Date and time .....	146
Network interfaces .....	147
Persons .....	149
Users .....	152
Adding users and user groups .....	153
Determining access rights .....	154
Determining access rights for a group .....	156
Per object rights .....	157
Examples of user rights settings .....	158
Audit .....	159
Devices .....	161
IP devices .....	162
Adding IP devices manually .....	164
Adding IP devices that use the ONVIF protocol .....	166
Adding IP devices using RTSP .....	168
Adding video files .....	169
Image dewarp into several channels .....	170
Boards .....	172
Configuring device settings .....	173
Serial port settings .....	178
Remote Controls Settings .....	180
Channels .....	181
Channel settings .....	183
Channel recording settings .....	187
Video capturing parameters .....	189
Black zones .....	190
Watermarks .....	191
Changing image rotation and aspect ratio .....	192
Audio channel settings .....	193
Motion detector settings .....	194
Hardware-based motion detector settings .....	196
Software-based motion detector settings .....	197
Fire/smoke detector settings .....	198
"Sabotage detector" module settings .....	199
Choosing an optics model and calibrating PTZ camera optics .....	201
Lost channels .....	203
Network .....	204
Connecting to a new server .....	206
Changing the connection settings .....	208
Connection through TRASSIR Cloud .....	210
Restrictions to connection to servers with TRASSIR 3.2 installed .....	211
Automation .....	212
Scripts .....	213
Python syntax .....	214
Integrated script editor .....	216
Activation .....	218
Working with settings .....	220

Working with objects .....	221
Interacting with the user .....	226
Events in scripts .....	227
Parameters and resources in scripts .....	228
Using ActivePOS in scripts .....	231
Using AutoTRASSIR in scripts .....	232
Rules .....	233
Schedules .....	236
Adding an email account .....	238
Examples of the rules and scripts .....	239
Plugins .....	256
ActiveDome - Automated PTZ-camera control .....	257
ActiveDome's manual and automatic operating modes .....	258
Creating an ActiveDome scene .....	259
Comparison of overview cameras and PTZ cameras .....	260
ActivePOS - Point-of-sale operations monitoring .....	262
ActivePOS features .....	263
Trading systems and equipment compatible with ActivePOS .....	264
ActivePOS incidents and detectors .....	266
Personal incidents and detectors creation .....	268
Configuring POS terminals .....	270
Configuring R-Keeper POS terminals .....	273
DSSL XML for ActivePOS .....	276
DSSL XML for trade objects .....	279
DSSL XML for hospitality business and public catering objects .....	285
DSSL XML for banknote counters and sorters .....	291
DSSL XML for warehouses .....	292
DSSL XML for gas stations .....	294
IP-video intercom .....	301
Connection to Asterisk server .....	302
SipPhone server settings .....	304
SipPhone on the client settings .....	305
AutoTRASSIR - Automated license plate recognition .....	306
Selecting, installing, and configuring cameras to work with the AutoTRASSIR module .....	308
AutoTRASSIR general settings .....	310
AutoTRASSIR settings .....	313
AutoTRASSIR (LPR5) setup .....	314
AutoTRASSIR settings (LPR3) .....	317
AutoTRASSIR settings (LPR1) .....	319
Maintaining internal lists of license plate numbers .....	323
Connecting external lists of license plate numbers from a text file .....	326
Creating an external ODBC data source for AutoTRASSIR .....	328
Connecting external lists of license plate numbers in TRASSIR for Windows .....	331
Connecting external lists of license plate numbers in TRASSIR OS .....	333
Creating an AutoTRASSIR template .....	335
SIMT software-based detector .....	337
SIMT detector settings .....	338
ActiveSearch - find motion .....	341
Floor mapping settings .....	342
Slow Down Detector .....	346
Common Slow Down detector settings .....	347
Configuration of the Advanced Slow Down detector .....	348
Face recognizer .....	350
Face recognizer basic settings .....	354
Face recognizer settings for the channel .....	359
Face recognizer 2.0 settings for the channel .....	361
Face database .....	364
Neural Empty Shelf Detector .....	366
Empty Shelf Detector .....	369

Queue detector and workplace detector .....	370
"Queue detector" module settings .....	371
Workplace detector module settings .....	373
Head Tracker .....	375
"Head Tracker" module settings .....	376
Neuro detector .....	378
Neuro detector setup .....	380
Classifier .....	385
ArUco Detector .....	386
ArUco Detection .....	387
ArUco Marker generator .....	390
Neural bags counter .....	391
Abandoned items neural detector .....	392
Pose detector .....	395
Analytics .....	398
Access monitoring control and security and fire alarm systems .....	399
TRASSIR Access Control .....	401
Devices .....	402
Areas of use .....	406
Personnel .....	407
Person access levels .....	410
Visitor templates .....	413
TRASSIR settings for operation with Orion Pro access monitoring and control system .....	415
Connecting a data source (ODBC) .....	417
TRASSIR settings for operation with Hikvision ACS panels .....	420
Connecting TRASSIR to Hikvision ACS panel .....	421
Typical TRASSIR settings for operation with access monitoring and control system and security and fire alarm system .....	422
FortNet ACS server settings features .....	423
"Gate" ACS server settings features .....	424
Sigur(Sphinx) ACS server settings features .....	425
Access monitoring and control system NeoGuard server settings features .....	426
Access monitoring and control system "Itrium" server settings features .....	427
Specific features of TRASSIR settings for operation with Schrack security and fire alarm system .....	428
Specific features of TRASSIR settings for operation with Spica access monitoring and control system server .....	429
Specific features of TRASSIR settings for operation with Paradox access monitoring and control system panels .....	430
Stemax system server settings features .....	432
TRASSIR settings features for operation with "MaxLogic" panels .....	433
AMCS or security and fire alarm system objects settings tree .....	434



## Customer support

TRASSIR pays great attention to the customer support. We offer the following informational resources as a part of the information support:

- Technical support for issues regarding the installation and configuration of the TRASSIR system;
- A [special section](#) of the company website, which contains a collection of technical documentation for the TRASSIR system, drivers and utilities, instructions, and reference materials;

Please direct your questions and requests related to the TRASSIR system as follows:

- by phone to +7 (495) 783-72-87,
- via [helpdesk@trassir.com](mailto:helpdesk@trassir.com),
- via the [feedback form](#) on the company website.

You must indicate your USB-key number, which is printed on the key itself, when contacting technical support. This helps us serve you faster and maintain a record of your requests.

## Type Codes

Information blocks used in the document:



Warning about the features of the function, requiring mandatory reading and/or execution.



Important information, which should be noted when working with the described function.



Note to the text, which is indicative and/or recommendatory.



References to other sections of the documentation related to the section described.

## Basic information

The manual is designed for video surveillance system administrators.

This document is a manual on how to install, configure, and use TRASSIR software.

The purpose of the document is to:

- Help administrators to independently install TRASSIR on video surveillance system servers and workstations, and to start and configure TRASSIR according to their needs;
- Provide reference information about TRASSIR features and ways to receive technical support;
- provide quickly accessible information about how to install, configure, and use TRASSIR.



- [\*Scope and feature summary\*](#)

## Scope and feature summary

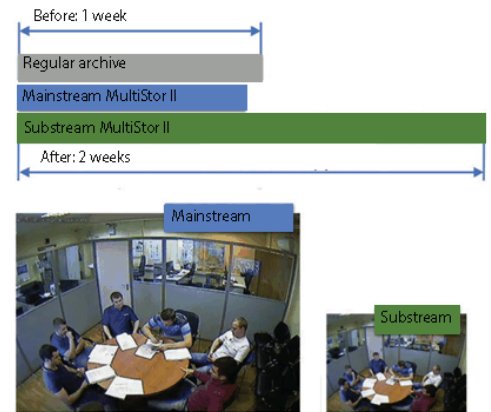
TRASSIR software is a modern automated system intended to arrange video surveillance, smart processing and storage of video information, and to provide access to video data for operating and dispatching personnel.

TRASSIR covers a wide range of tasks and is the reliable base for both centralized and decentralized video surveillance systems.

The software is implemented in a web-based distributed IGMP architecture: it can run both on a single server or as a part of complex solutions consisting of multiple machines. The Clients run on separate workstations using data coming from video surveillance system and can connect to TRASSIR servers via local network or via the Internet.

TRASSIR is an up-to-date software with the following features and technologies:

## TRASSIR technologies ensuring data storage reliability



**MultiStor II** technology increases archive depth several times by minor reduction of the archive volume in the main stream while gaining significant increase of the archive depth in the additional stream. An additional feature of MultiStor II technology is parallel recording to multiple hard drives at the same time to avoid total data loss when any of them fails.



**EdgeStorage** technology effectively doubles the reliability of the operation with the video archive due to the use of two independent archives in a single system.

Modern IP-devices (Network Video Recorders and IP-cameras) support archive recording to the internal HD or SD-card. TRASSIR can manage each archive separately and in case of server malfunction or communication failure the data on the device will not be lost. After the network recovery, TRASSIR will provide access to archive on IP-devices.

**Video archiving.** TRASSIR supports an unlimited number of hard disks for recording, making it possible to create archives with sizes in the tens of terabytes. Additionally, it supports hot-plugging of various types of digital storage devices: CDs, USB-drives and FireWire.

For each drive, there is a diagnostic system and statistics about disk space available for video archive recording; there are also a number of [settings](#) that let an administrator specify which drives are to be used and how, and how much hard disk space an archive can occupy.

Recording to the archive can be done continuously: by operator command, by schedule or by motion detector. The video archive can be securely [encrypted](#), if necessary.

**Lost channels.** This function allows you to make work with the archive much easier. You can view it on any computer without any additional actions and settings. You can record the archive from the video server to an external drive, then connect it to any computer where TRASSIR is installed - and work with the archive as on a video server. You can also view this archive using free TRASSIR Client application, which requires no USB key with a license to run it.

For the channels to be created to view the archive on another computer, a term "lost" is used. [Lost channels](#) are the channels for which only the archive is available and there is no video register device (grabber).

**All events of video camera surveillance system are recorded and stored in a [database](#)**, which can be both on local and remote server. Data retention time is determined by TRASSIR settings.





**TRASSIR Cloud** is a set of free WEB services from DSSL that provide 24/7 monitoring for your servers. In addition, TRASSIR Cloud allows you to control servers from personal account and display their status on the map.

## TRASSIR network features

**MultiStream** is a multi-thread technology allowing to significantly reduce the requirements towards the video server or customer's remote computer. The technology consists in a simultaneous receipt of two video streams from the video camera with independent settings of resolution, degree of compression and frame rate.

The first stream of maximum resolution will be used to record to archive or display on screen while full screen viewing of the video from this camera. Second stream of low resolution and decreased frame frequency will be displayed on the screen (both customer and server) in multiscreen mode. Both streams can be set up independently and the system will switch between them imperceptibly, significantly saving server and network resources for the user.



**Tier** is the unique feature of TRASSIR allowing you to combine servers into networks on the tree-structured principle. TRASSIR architecture allows you to build distributed video surveillance system of any scale: unrestricted number of network clients can connect to single server, both through local network and through Internet. In addition, it is possible *to combine unrestricted number of servers into single network*, herewith servers can operate both independently and exchange data with each other; remote servers set up is possible through the network. And the unrestricted network administration allows you to control any TRASSIR server through the customer's software or through WEB. When you access the system via web-browser, it will be sufficient to run TRASSIR *web-server* and there would be no need to install any software to arrange operators' workplaces.

## Ergonomic and management features



**TRASSIR open user interface** allows customize your workspace using ready templates of screen separators and camera arrangement. Arrange any object at monitor screen the way you need: [plans of the premises](#), video cameras arrangement, Access Monitoring and Control System and Operations Service event logs, [AutoTRASSIR](#) license plate recognition or [ActivePOS](#) cash control.

**TRASSIR multitask operation mode** performs all operations (monitoring, archive recording, archive view, settings, access via network, remote viewing of the video archive along with interaction with integrated safety systems) simultaneously in a single interface. Thus, the staff will be able to perform all necessary actions simultaneously without interruption of the other components of video surveillance system operation.



**Easy navigation** accelerates user operation by times.

A built-in video player is provided to review archive in TRASSIR, enabling to review fragments in any order, scroll them forward and backward, increase and reduce view speed, review frame-by-frame. It is also possible to export archive fragments to video file and make screenshots.

**ActiveSearch II** is an intelligent technology of motion detection in the video archive which makes operator's work much easier. At the objects with round-the-clock recording to archive, in order to search for an event, you need to review the entire video archive. With ActiveSearch it is enough to select the area in which you want to find the desired fragment and select time interval of search and in a few seconds TRASSIR will output the list of segments at which any movement had happened in the selected area.

**MultiSearch** significantly increases the search for events in the archive. Select the region and in a second you'll get in one scene segments from various time points of archive.

**TRASSIR ActiveDome** accelerates PTZ camera control 20 times. It allows performing automatic monitoring of the vast territories and zoom objects with single click.

TRASSIR has **built-in search engines** allowing to find the required event and if necessary immediately start reviewing the corresponding archive. Besides, the possibility to create filters for the current events is provided allowing to reduce the scope of the output data. Using filters one can achieve output of only those events that are worth operator's attention.

A mechanism of **video surveillance system flexible settings** is implemented in TRASSIR, using [schedules](#), [rules](#) and [scripts](#). Any equipment or video channel in TRASSIR can be both source of event and a performer of actions. The schedules, rules and scripts ensure management of video surveillance system response to any occurring events.

**Multi-level rights distribution system** is implemented in TRASSIR, allowing to prevent unauthorized access. Administrator can create user accounts with various combinations of access rights, for example: "current events

review", "archive review", "archive export", "administration" (capability to change system settings), etc. up to possibility to control other user accounts.

## TRASSIR integration



**Broad range of supported devices.** Different types of devices can operate together in a single video surveillance system: *Hardware/software-based compression cards* and *IP devices*. Additionally, TRASSIR works correctly with the majority of modern hardware platforms, and the *list of supported devices* is constantly growing.

**The use of efficient H. 264 compression standard.** This standard provides for unprecedented frame size under perfect quality. For example at 704 x 576 resolution and slight movement color frame size is 3 Kb and black-and-white half-frame - 1 Kb. H.264 provides for huge saving of disk space and allows long-term storage archives for lesser costs.



**ActivePOS - integration with POS-systems.** The widest possibilities of the cash control system are provided through event integration with leading trading systems. ActivePOS creates scenarios for detecting violations of any complexity, and a powerful reporting system with cash analytics will not leave scammers any chance.

**Integration with Access Monitoring and Control System and Security and Fire Alarm** allows you to get complete list of events from AMCS. It will provide possibility to adjust response rules, manage objects using TRASSIR maps, conduct photo and video verification and view the status of all the objects.

**AutoTRASSIR automatic license plate recognition system** which can be used to control the entry/exit of vehicles to/from the territory of enterprises as well as traffic control service, at the checkpoints and at any other inspection points. TRASSIR provides interaction with access control systems, video and audio surveillance systems and execution units (for example, rising arm barriers).



- [Basic information](#)

## System requirements

This section presents the main requirements for the equipment used to build a video surveillance system:

1. [Video server](#) - The computer that TRASSIR will use to process video, store video archives, and control the entire video surveillance system.  
You can use the list of the ready-made configurations on [our website](#) to complete a video server quickly.
2. [Compatible IP devices](#) - A list of manufacturers whose equipment is compatible with TRASSIR. Refer to this section if you plan to deploy a video surveillance system based on IP devices.
3. [Storage devices for Lanser](#) - If you're going to use IP video records from the Lanser family of devices, you can find in this section a list of compatible hard drives that can be installed in these devices.



- [Windows OS settings](#)

## Video server

When designing a video surveillance system, special attention must be given to the selection of components in your future video surveillance system. The most important aspects of the system are listed below.

1. **Video card.** In case you plan to display video directly on the video surveillance server, you should use a discrete video card. TRASSIR supports almost all up-to-date ATI Radeon and nVidia video cards. You can find recommendations on selecting video card in our [knowledge base](#).
2. **Disk subsystem.** The disk array for archive recording must be selected based on both the total volume of disk space and the required archive recording speed. During simultaneous recording, reading, and deleting of archives, the actual speed of an array of hard disks may differ significantly from the manufacturer's claimed maximum speed. You can read more about this in the subsection of the manual entitled [Selecting the number of disks for an archive](#).
3. **Operating system** - TRASSIR works with the majority of modern Microsoft Windows operating systems. A full list of the supported operating systems can be found in the subsection of the manual entitled [Compatible operating systems](#). Note that in order for TRASSIR to work properly, several changes must be made to the [operating system settings](#).



You can use one of the ready-made video server configurations published on [our website](#). You should also review the lists of equipment that we [recommend](#) and [do not recommend](#).



- [Selecting the number of disks for an archive](#)
- [Compatible operating systems](#)
- [Compatible IP equipment](#)
- [Storage devices for the TRASSIR Lanser-4Mobile and the TRASSIR Lanser-Mobile II](#)

## Selecting the number of disks for an archive

When selecting the number of disks for a video server, consider the archive depth required, i.e. how many disks will be needed to store the total volume of data.

The required number of disks is always calculated based on the total data stream. The size of the stream ("bitrate") depends directly on a number of factors, including: the number of cameras, picture resolution, number of recorded frames per second, compression codec used by an IP camera or video capture card, etc. In a running system you can check the total rate on the [channels](#) tab. In order to calculate the capacity of disks and their number, you can use the calculator on [our website](#).

Number of disks	Rate for upgrade from versions 2 and 3 (fragmented disks)	Rate for formatted disks
1	5 MB/s	50 MB/s
2	7 MB/s	50 MB/s
3	15 MB/s	100 MB/s
4	20 MB/s	150 MB/s
5+	25 MB/s	200 MB/s



You can check the list of recommended for use HDDs in our [knowledge base](#).

When using network storage devices, keep in mind that:

- It may take up to 20 minutes to connect certain iSCSI drives after losing a connection for more than one minute due to outages in the local network.
- When using RAID arrays (for example, RAID5), if one of the disks fails, the data transmission rate will drop by more than a factor of two.



**To optimize hard disk use and ensure maximum speed for archive recording, the size of the hard disks' logical partitions must not vary by more than a factor of 2.**

For example, if you use a local disk with a logical partition of 1 TB in a video recorder, when a new hard disk is installed to the server or when network storage is connected to the TRASSIR server, the logical partitions on them must not exceed 2 TB.



- [Video server](#)
- [Archive setup on the server](#)
- [Archive](#)
- [Compatible operating systems](#)



## Compatible operating systems

TRASSIR 4 works with all modern versions of the Windows operating system, both 32-bit and 64-bit. When choosing between the 32-bit and 64-bit version of an operating system, preference should be given to the 64 bit version.

TRASSIR is compatible with the following operating systems:

- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows Server 2012
- Windows 10



A number of operating system settings must be changed for TRASSIR to work properly. A list of the settings required for each operating system is given in the [Operating system settings](#) subsection.



- [Video server](#)
- [Windows OS settings](#)

## Compatible IP equipment

TRASSIR fully supports IP equipment manufactured by TRASSIR and third party integrations. The list of supported equipment manufacturers and models is constantly growing. You can find a full list of compatible IP equipment as well as a list of the IP equipment that uses the RTSP and ONVIF protocols in TRASSIR [on our website](#).

Our website also contains detailed information about the specifications and features of IP equipment supported by TRASSIR 4. To get the latest information about compatible specifications and features of IP equipment, [download this MS Excel file](#).



- [Video server](#)
- [Storage devices for the TRASSIR Lanser-4Mobile and the TRASSIR Lanser-Mobile II](#)
- [System requirements](#)

## Storage devices for the TRASSIR Lanser-4Mobile and the TRASSIR Lanser-Mobile II

TRASSIR Lanser-4Mobile and TRASSIR Lanser-Mobile II models may be equipped with their own hard disks for data storage. Installing a hard disk makes it possible to record a video archive directly on the Lanser, i.e. to use it as an extra (backup) archive.

The full list of hard disk models that are compatible with the TRASSIR Lanser-4Mobile and the TRASSIR Lanser-Mobile II is given [on our website](#).



After installing a hard disk in a Lanser, it must be formatted. The hard disk is formatted using the Lanser's web interface while the device is connected to the network, or through the device's internal interface while a VGA monitor and mouse are connected to the Lanser.



- [Video server](#)
- [Compatible IP equipment](#)
- [System requirements](#)

# Installation

The number of installation screens and their content may vary depending on the configuration of the video surveillance system you want to deploy (number video servers, number of channels, number and type of video-recording devices used).



All software and drivers must be installed using an administrator account.

We recommend deploying your video surveillance system in the following order:

1. Install video surveillance equipment. Generally speaking, your video surveillance system may include the following video-recording equipment:
  - *Compression cards.*
  - *Lanser IP devices.*
  - *Analog PTZ cameras.*If your video surveillance system won't use one of the device types listed, then skip the corresponding screen. Moreover, installation of IP cameras (including PTZ cameras) is not considered at this stage, because the entire installation process consists of connecting the camera to the local network and setting up an IP address for it.
2. *Configure the servers' operating system* for TRASSIR to work properly.
3. *Install drivers for Guardant USB keys on all servers.* USB keys are used to protect licensed copies of TRASSIR and are required to run it.
4. *Install the PostgreSQL DBMS on the server.* Later, a database for recording and storing events will be automatically created on the server. If your video surveillance system will have a heavy stream of a large number of events, we recommend installing the PostgreSQL DBMS on a dedicated server (not used for processing and recording video) for proper operation.
5. Install TRASSIR Server software on all servers as *a separate application* or *Windows service*.
6. *Install TRASSIR Client* all workstations that will be used for video surveillance.

Note that both TRASSIR Client and TRASSIR Server may be used for video surveillance. Alternatively, you can altogether decline to install TRASSIR on operators' workstations. To do this, you will need to configure a *TRASSIR web server*. Then all the video surveillance functions will be available using an ordinary browser. A workstation only needs to have the Mozilla Firefox browser installed, as well as the video surveillance plug-in.

## Installing compression cards

A compression card is an electronic device for converting an analog video signal into a digital video stream. The card has a PCI or PCI-E socket, and can process a signal from one or more analog video cameras.

Depending on the nature of the signal processing, a compression card may have hardware-based or software-based compression.

Hardware-based compression implies the processor on the card, which performs all of the routine work of video compression and preprocessing. First of all, this makes it possible for even a weak processors to write up to 64 channels of video at high-resolution at 25 frames per second for each channel. Secondly, the central processing unit is free for other tasks, such as video analysis, face recognition, and servicing network clients.

Software-based compression is performed directly on the server using its central processing unit. A card of this type places a heavy load on the server, but it also possesses a wide range of capabilities.

TRASSIR supports the use of both hardware-based and software-based compression in a single video surveillance system.

To install a compression card in a computer:

1. Read the compression card manufacturer's instructions.
2. Turn off and unplug the computer.
3. Open the computer case.
4. Install the compression card(s) in an available PCI slot(s) on the motherboard and securely fasten it (them) with screws.
5. Close the computer case.
6. Connect an interface cable to the compression card.
7. Connect the camera signals to the interface cable.
8. Plug the computer back in.
9. Turn on the computer.
10. Wait for the operating system to load and discover the new hardware.
11. Install the drivers for the discovered hardware (supplied together with TRASSIR).

## TRASSIR Lanser IP-video server installation

TRASSIR supports the following IP video servers:

### TRASSIR Lanser IP-4P

Rear panel:



1	1 ... 4	Network interfaces to connect IP-cameras
2	AUDIO INPUT	RCA connector - audio input
3	AUDIO OUTPUT	RCA connector - audio output
4	VGA MONITOR	DB15 port for VGA monitor
5	HDMI	HDMI port
6	LAN	Network interface for connecting a video recorder to the local network
7	USB	USB slot for mouse connection (it is used to control the internal interface and flash drive (to reflash the device)
8	48V	Power source 48V DC
9	POWER	Switch to turn device on/off

### TRASSIR Lanser 960H

TRASSIR Lanser 960H-4 rear panel:



TRASSIR Lanser 960H-8 and TRASSIR Lanser 960H-8 Hybrid rear panel:



TRASSIR Lanser 960H-16 and TRASSIR Lanser 960H-16 Hybrid rear panel:

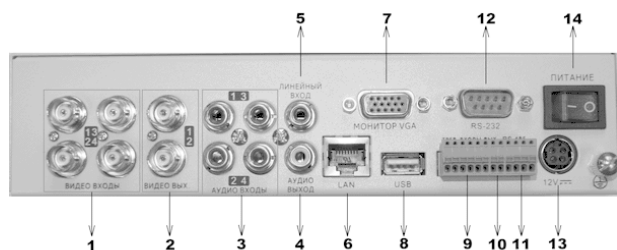


1	VIDEO IN	Video signals BNC inputs
---	----------	--------------------------

2	VIDEO OU	BNC output for analogue monitor
3	USB interface	It is used to connect USB mouse or USB Flash
4	HDMI	HDMI port
5	VGA	DB15 port for VGA monitor
6	AUDIO IN	RCA connector - audio input
7	AUDIO OUT	RCA connector - audio output
8	LAN interface	Network interface
9	RS-485	Port to connect devices through RS-485
10	12V	Power source 12V DC
11	POWER	Switch to turn on / off the device
12	GND	Grounding (must be conducted upon video recorder start)
13	ALARM IN	Alarm inputs
14	ALARM OUT	Alarm outputs

### TRASSIR Lanser-Mobile II

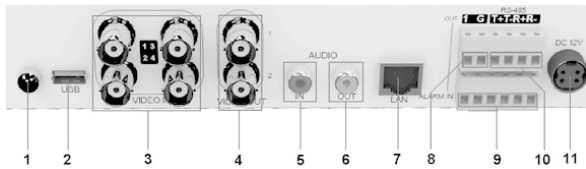
Rear panel:



1	Video inputs	Video inputs for connecting the cameras
2	Video outputs	Analog video outputs. These outputs are used to connect to an analog video monitor for viewing and configuration. The second output can be used for viewing cameras in SPOT mode.
3	Audio inputs	Audio inputs to connect active (amplified) microphones.
4	Audio output	RCA jack to connect the active speakers or headphones. Used to listen to voice messages.
5	Line in	RCA jack to connect an active (amplified) microphone. Used to broadcast voice messages.
6	LAN	RJ-45 jack to connect a device to a network using TCP/IP.
7	VGA monitor	D-sub socket to connect to a VGA monitor.
8	USB	USB slot to connect a USB mouse (used to control the internal interface).
9	Alarm inputs	Alarm inputs (4 inputs)
10	Alarm output	Alarm output (1 output)
11	RS-485	RS-485 serial port
12	RS-232	RS-232 serial port
13	12V	Camera power jack (12 V, current draw of at least 3.33 A)
14	Power	The device's power on/off switch

### TRASSIR Lanser-4Mobile

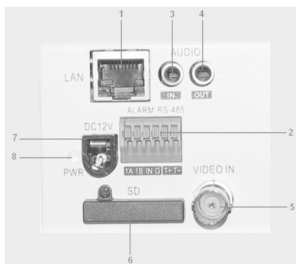
Back panel:



1	-	Grounding.
2	USB	Mouse USB slot (is used to control the internal interface and flash drive, which is used for the device reflashing).
3	VIN1-VIN4	Camera connectors.
4	Video output	Analog video output signal. It is used to connect to an analog video monitor.
6	Video SPOT	Analog video out. It is used to review cameras.
7	LAN	RJ-45 jack to connect to a network using TCP/IP.
8	OUT	Alarm output (1 output).
9	IN	Alarm inputs (4 inputs).
10	RS-485	RS-485 serial port. Used to control PTZ devices.
11	DC 12V	Camera power jack (12 V, current draw of at least 3.33 A)
12	RS-232	RS-232 serial port. It is used to configure the TRASSIR Lanser-4Mobile using a computer's serial port.

### TRASSIR Lanser-1Real

Rear panel:



1	LAN	RJ-45 jack, used for network connection.
2	1A 1B IN G T+ T-	Alarm output (pins A and B). Alarm input (pins IN and G). Half-duplex RJ-485 serial port (pin T+ and T-).
3	IN	Audio input, used to connect an active (amplified) microphone.
4	OUT	Audio output, used to connect headphones. For high-volume listening, i.e. when connected to speakers or a notification system, and external audio amplifier is required.
5	VIN	Analog video input from the camera.
6	SD	SD-card slot.
7	DC12V	Power supply jack (12 V, current draw of at least 700 mA).
8	PWR	Power-on indicator.

These instructions will assist in preparing IP-videoserver to connect it to TRASSIR.





Switch off power supply before performing any activities on the device.



Before connecting any device to IP-videoserver it is strongly recommended getting acquainted with IP-videoserver guidelines and the list of the compatible devices.

Before connecting to IP-videoserver, do the following:

1. Install hard drive into the device and fix it.
2. Connect network cable to RJ-45 (UTP) slot on the device. In case the device is directly connected to computer it is necessary to use cable with crossover crimping scheme.
3. Connect one or several cameras to the relevant ports:
  - RJ-45 - for IP-cameras
  - BNC - for analogue cameras
4. Connect audio devices to the corresponding RCA-ports on the device.
5. Connect contacts for alarm inputs/outputs operation.
6. Connect RS-485 port contacts for work with PTZ cameras.
7. Fix IP-videoserver steadily and connect power supply.
8. Open WEB-interface of the device and format the hard drive.
9. Set up IP-videoserver using *SADP utility software*.

After that you'll be able to *add the device to TRASSIR*.



Besides the above named devices, TRASSIR will also operate properly with old-fashioned IP-videoservers: Lanser-4M, Lanser-4HDD, Lanser-4Real. Please note that you can not order such devices (for example to expand video surveillance system).

## Network settings for TRASSIR Lanser video servers

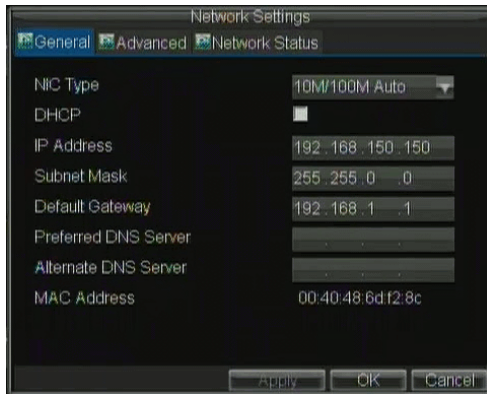
After *IP-videoserver preparation* and before *adding* to TRASSIR, device parameters should be set up: *IP-address*, *subnet mask* and *gateway*.

Parameters can be set in two ways:

- in *SADP* utility;
- in the device's interface.

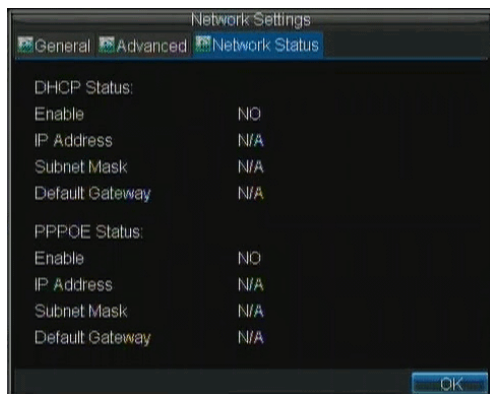
## TRASSIR Lanser settings with the help of your own interface

1. Connect monitor and mouse to the device.
2. Turn on the TRASSIR Lanser.
3. Open network settings menu by selecting **Menu > Settings > Network**.
4. Select the **General** tab in the opened menu.



5. Select one of the two following variants of settings:
  - **Automatic settings receipt** - in case DHCP server operates in the network and you need to receive network settings for this device, check **DHCP** box.

You can check the status of the DHCP server in **Network status** tab:

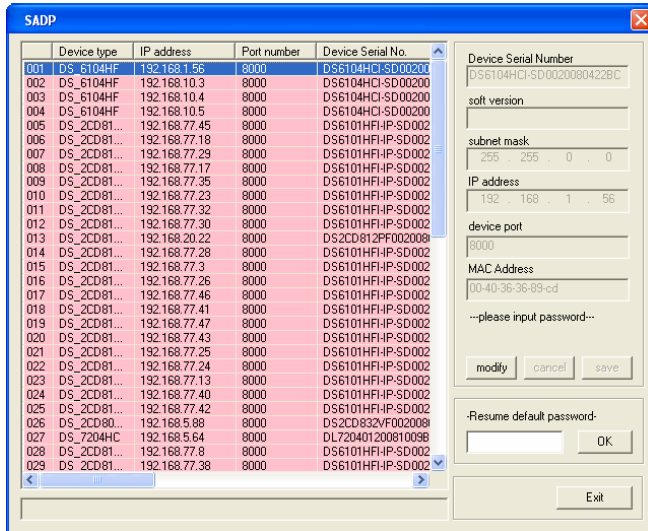


- **Manual network settings** -set the following values:
  - **IP address** - The address that is to be assigned to the device;
  - **Mask** - The subnet mask;
  - **Gateway** - The IP address of the gateway (this is usually your router);
  - **Primary DNS server, Secondary DNS server** - The primary- and secondary DNS servers to be used with your device.

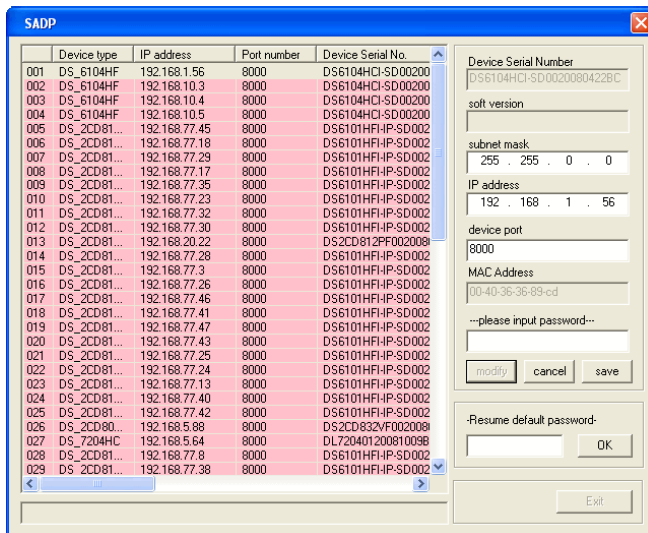
6. Press **OK** button to save the settings.

## TRASSIR Lanser setting using SADP utility

1. Download SADP utility from our [web-site](#).
2. Extract the archive and install the utility.
3. Restart your PC, if necessary.
4. Run the utility `sadpdlg.exe`.
5. In the opened window click **Enter**.
6. In the list of the discovered devices, select the device. Click **Modify**.



7. In the **Subnet mask** field, enter your subnet mask.
8. In the **IP address** field, enter the device's required IP address.
9. In the **Please input password** field, enter your password (the default password is "12345").



10. Click **Save**.



• [TRASSIR Lanser IP-video server installation](#)

## NAS Setup

A network-attached storage (NAS) is a device with a disk array that is connected to the local network. To ensure data storage reliability, the hard disks in the network storage are part of a RAID array.

Virtually any network storage that uses iSCSI can be used in TRASSIR as an archive for video data.



Before a network storage is connected, it must first be *configured*.

The configuration of a network storage's connection in TRASSIR depends on the operating system being used:

- *Windows operating systems*
- *"Linux-based TRASSIR OS"*



- *[Configuring a QNAP Turbo NAS](#)*
- *[Connecting a network storage in a Windows OS](#)*
- *[Configuring a network storage connection in Linux-based TRASSIR OS](#)*
- *[Archive setup on the server](#)*

## Configuring a QNAP Turbo NAS

As an example, let us consider the configuration of a QNAP Turbo NAS.

1. To connect to the network storage, launch a browser and enter the following into the address bar

`http://IP-address:8080`

where **IP-address** is the network storage's address.

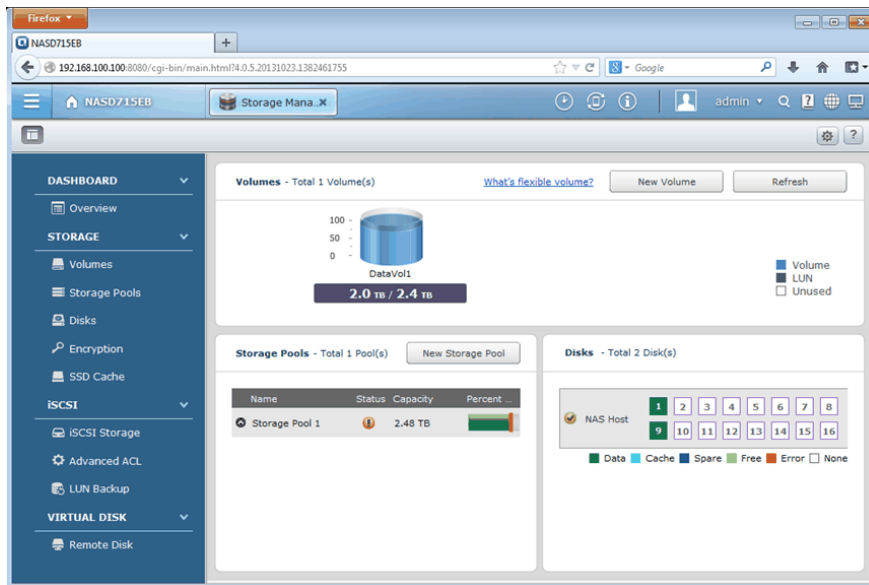
If the connection is successful, a sign-in window will appear in the browser.



2. To sign in, enter your username and password. If the authentication is successful, the network storage control panel will open.

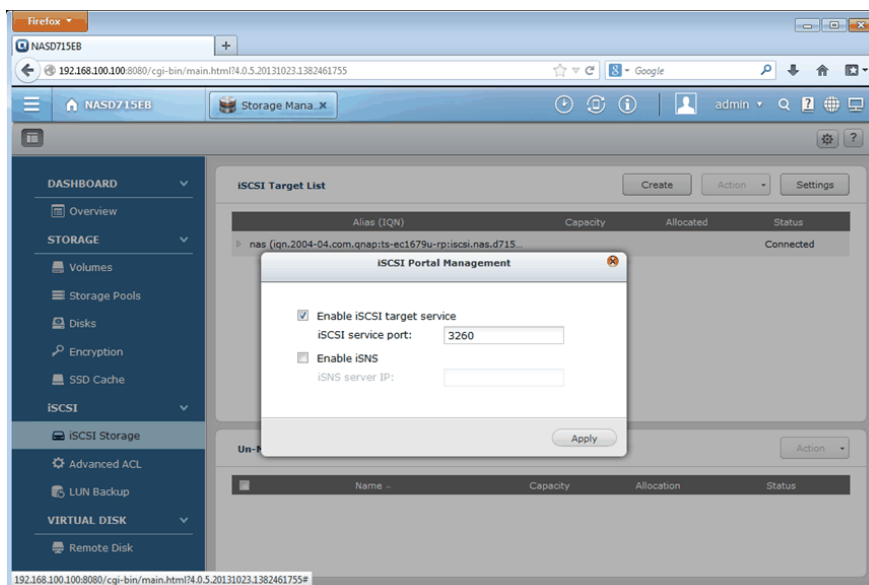


3. Run **Storage Manager** and click the **Dashboard** -> **Overview** link. This page contains information about the hard disks installed in the network storage, their state, and size.

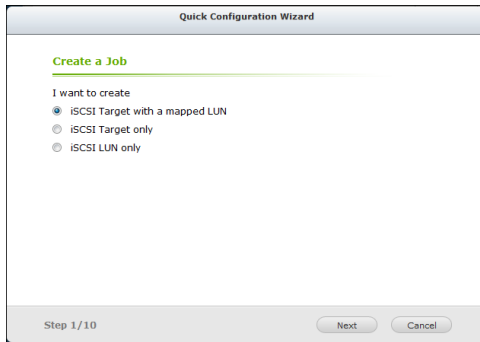


To use the network storage as an archive for TRASSIR video data, create one or more volumes. Note that all logical disks to which the archive will be written must be approximately the same size and must absolutely not differ in size by more than a factor of 2. You can use a RAID array to ensure data storage reliability.

- To allow and configure an external connection to the network storage via iSCSI, click the **iSCSI** -> **iSCSI Storage** link and click the **Settings** button. In the window that opens, set the **Enable iSCSI target service** checkbox and enter the **iSCSI service port**.



- To create and configure a new iSCSI storage, click the **Create** button. This will launch the Quick Configuration Wizard. If you are creating an iSCSI storage for the first time, select **iSCSI Target with a mapped LUN** and click **Next**.



Quick Configuration Wizard

Create a Job

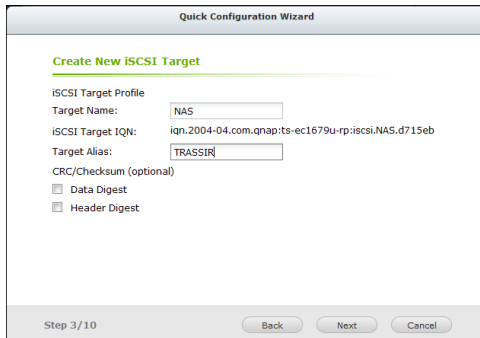
I want to create

- ☒ iSCSI Target with a mapped LUN
- ☐ iSCSI Target only
- ☐ iSCSI LUN only

Step 1/10

Next Cancel

6. In step 3, enter the target's name and alias.



Quick Configuration Wizard

Create New iSCSI Target

iSCSI Target Profile

Target Name:

iSCSI Target IQN:

Target Alias:

CRC/Checksum (optional)

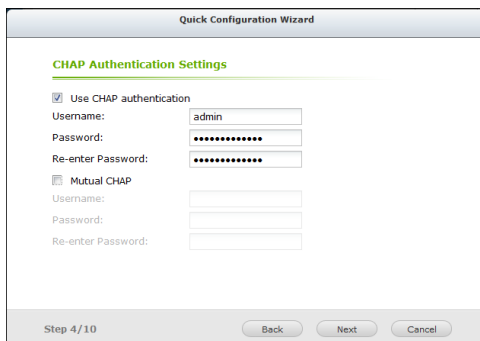
- ☐ Data Digest
- ☐ Header Digest

Step 3/10

Back Next Cancel

Click **Next** to continue.

7. In step 4, specify the CHAP authentication settings. If needed, set the **Use CHAP authentication** and enter the username and password.



Quick Configuration Wizard

CHAP Authentication Settings

☒ Use CHAP authentication

Username:

Password:

Re-enter Password:

☐ Mutual CHAP

Username:

Password:

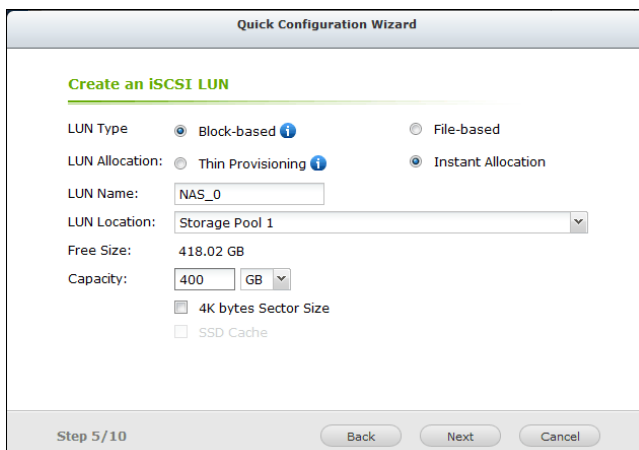
Re-enter Password:

Step 4/10

Back Next Cancel

Click **Next** to continue.

8. In step 5, create an iSCSI LUN. To do this, select a LUN type, enter the LUN name, and specify its location and capacity.



Quick Configuration Wizard

Create an iSCSI LUN

LUN Type: ☒ Block-based ☐ File-based

LUN Allocation: ☐ Thin Provisioning ☒ Instant Allocation

LUN Name:

LUN Location:

Free Size: 418.02 GB

Capacity:

☐ 4K bytes Sector Size

☐ SSD Cache

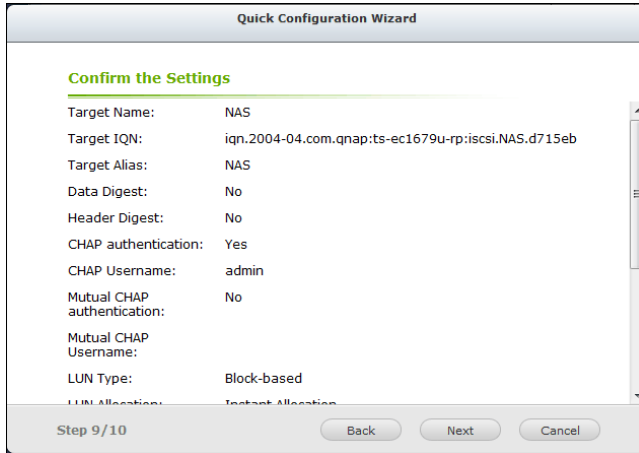
Step 5/10

Back Next Cancel

Click **Next** to continue.



9. In step 9, confirm the selected settings.



**Quick Configuration Wizard**

**Confirm the Settings**

Target Name: NAS

Target IQN: iqn.2004-04.com.qnap:ts-ec1679u-rp:iscsi.NAS.d715eb

Target Alias: NAS

Data Digest: No

Header Digest: No

CHAP authentication: Yes

CHAP Username: admin

Mutual CHAP authentication: No

Mutual CHAP Username:

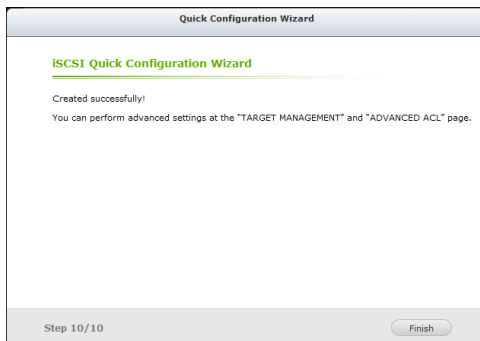
LUN Type: Block-based

LUN Allocation: Instant Allocation

Step 9/10

Back Next Cancel

10. In step 10, the iSCSI target and LUN are created.



**Quick Configuration Wizard**

**ISCSI Quick Configuration Wizard**

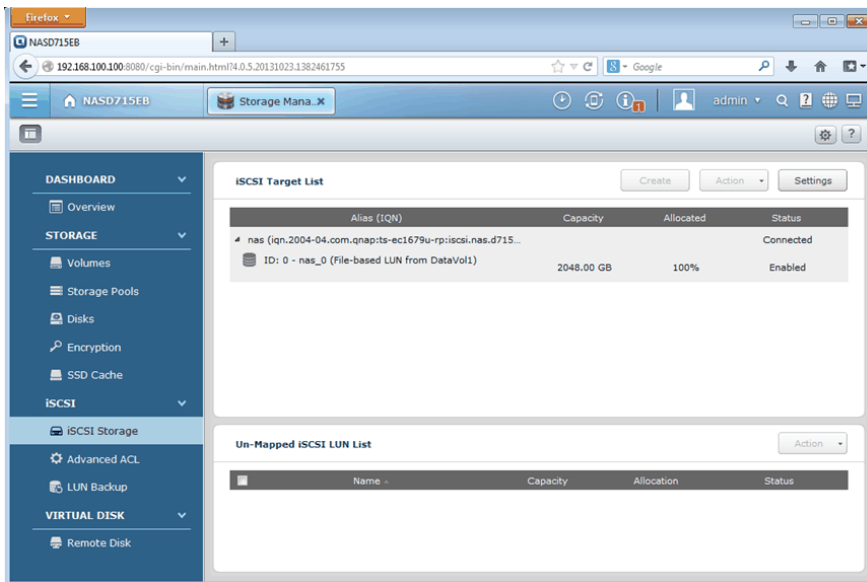
Created successfully!

You can perform advanced settings at the "TARGET MANAGEMENT" and "ADVANCED ACL" page.

Step 10/10

Finish

When the Quick Configuration Wizard is finished, the iSCSI target should be created with a connected LUN:



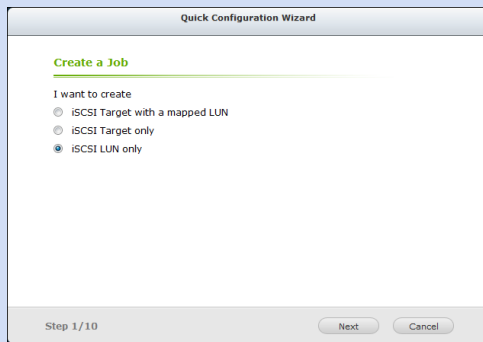
The screenshot shows the web interface of a NASD715EB device. The left sidebar contains a navigation menu with sections: DASHBOARD, STORAGE, and VIRTUAL DISK. The main content area displays the "iSCSI Target List" table, which shows a single target named "nas" with a capacity of 2048.00 GB and a status of "Connected". Below this, there is an "Un-Mapped iSCSI LUN List" section, which is currently empty.

Alias (IQN)	Capacity	Allocated	Status
nas (iqn.2004-04.com.qnap:ts-ec1679u-rp:iscsi.nas.d715eb)	2048.00 GB	100%	Connected

ID: 0 - nas\_0 (File-based LUN from DataVol1)



If you need to connect one or more LUNs to an existing iSCSI target, select the **iSCSI LUN only** option in the Quick Configuration Wizard.



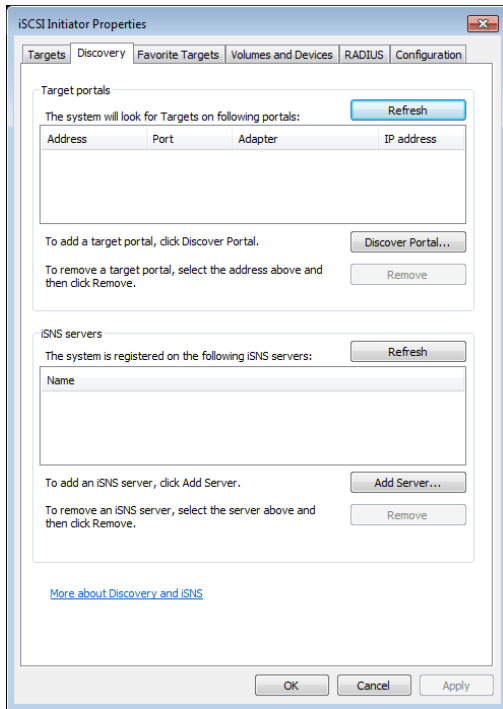
- [NAS Setup](#)
- [Connecting a network storage in a Windows OS](#)
- [Configuring a network storage connection in Linux-based TRASSIR OS](#)
- [Archive setup on the server](#)

## Connecting a network storage in a Windows OS

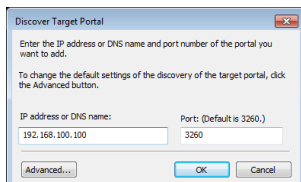
Volumes that were configured on the network storage when connecting in a Windows OS will be displayed as logical disks. In other words, all commands that apply to logical disks can be used when working with these disks.

Network storage connection procedure and settings in a Windows OS:

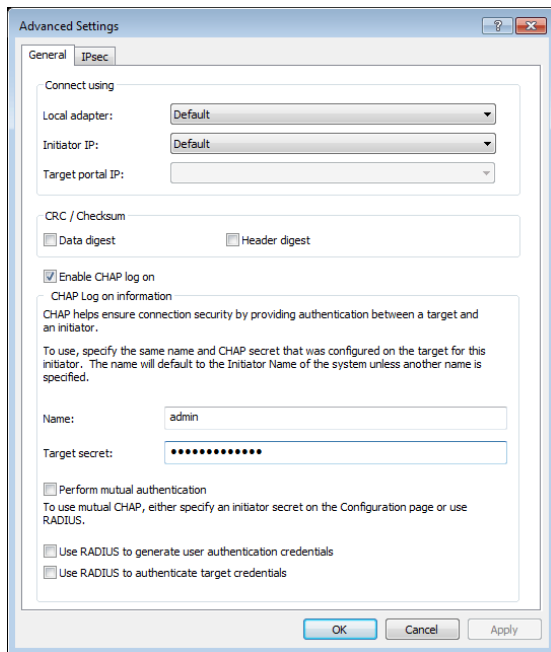
1. Open **Start -> Control Panel -> Administration -> iSCSI Initiator**



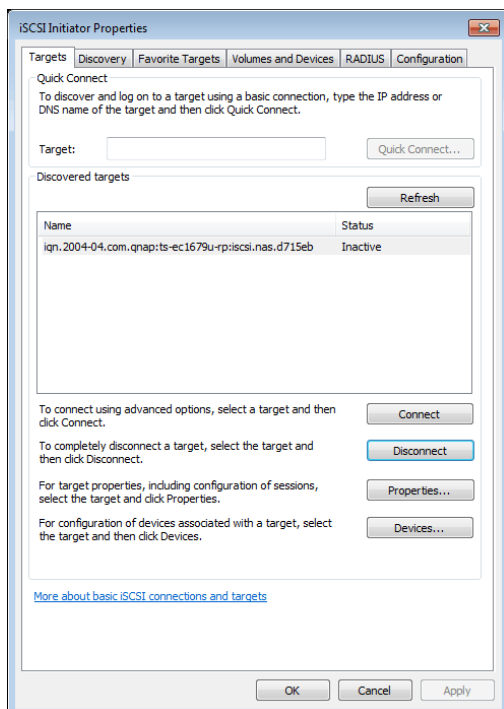
2. Go to the **Discovery** tab and click the **Discover Portal...** button to connect to the network storage
3. Enter the IP address of the network storage and specify the iSCSI service port that was entered during *configuration of the network storage*.



4. If you enabled CHAP authentication while configuring the network storage, click **Advanced** to enter the corresponding parameters.

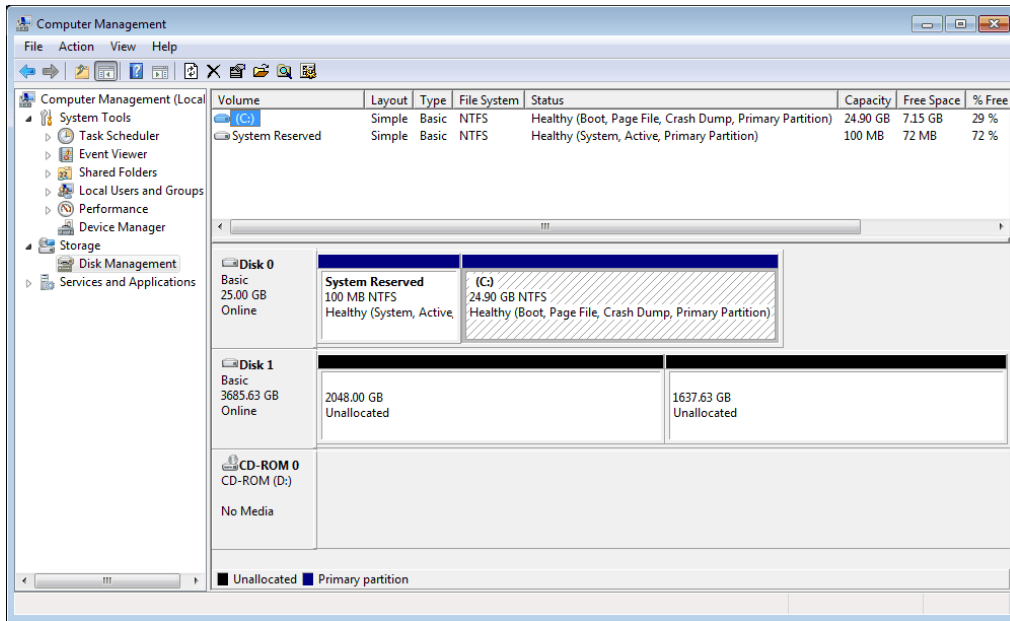


5. If there the network storage successfully connects, its identifier will appear in the **Targets** tab. And it's status will be "Inactive".



6. To start working with the network storage, it must be activated. To do this, select it in the list and click the **Connect** button. The network storage's status will change to "Connected".

If all of these steps were successful, the new disk will appear in the OS. To locate it, open **Computer -> Manage -> Disk Management**



Format disk before using it in TRASSIR. Please remember that all logical disks whereon the archive is going to be recorded should be of similar capacity and their capacity should not in any way differ 2 times or more in their size.



- [NAS Setup](#)
- [Configuring a QNAP Turbo NAS](#)
- [Configuring a network storage connection in Linux-based TRASSIR OS](#)
- [Archive setup on the server](#)

## Installing Guardant USB keys

A Guardant USB key is a device designed to protect TRASSIR and associated data from unauthorized use and copying. Each TRASSIR license contains the number of a USB key that must be used to start and run the software. You will not be able to work with TRASSIR if:

- The USB is not connected to the computer on which TRASSIR is installed;
- The drivers for the USB key are not installed or there were errors when installing them;
- The USB key's physical number and the number specified in the TRASSIR license do not match.

To install drivers for Guardant USB keys:

1. Be sure you have administrator rights. Otherwise, you will not be able to install the drivers.
2. Download the drivers for the Guardant USB key from the manufacturer's website or the [DSSL website](#). Additionally, drivers for the keys can be found on the TRASSIR CD. When downloading drivers for the USB keys, you must bear in mind your operating system's version and bus width (32-bit or 64-bit).
3. Disconnect all other keys (if there are any connected). The Guardant USB key should be connected to the port only after installing the drivers. The a key is connected before the drivers are installed and the standard Windows device installation wizard starts up, remove the key from the port and terminate the wizard.
4. Close all applications to avoid file-sharing errors.
5. Run `GrdDriversRU.msi` or `Setup.exe` and follow the installation program's instructions.
6. After completing the installation procedure, verify that the Guardant USB key works. To do this:
  - Connect the Guardant USB key.
  - Be sure that the key's network indicator is constantly lit.
  - Be sure that the Guardant USB key is in the Windows device manager's list of hardware.



You can install drivers for Guardant keys at the same time you install TRASSIR, because the TRASSIR distribution includes the required drivers.

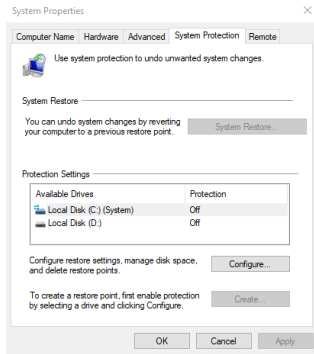
## Windows OS settings

This section contains the description of Windows operating system parameters settings procedure at the server.

### Windows 10 settings

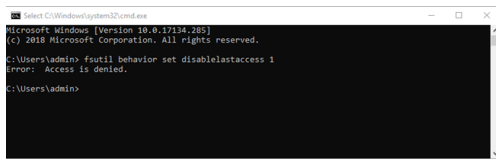
For the correct TRASSIR operation win Windows 10, the following parameters should be set up:

1. Disable system recovery on all the drives.



2. Enable parameter `disablelastaccess` (deactivate last access time) to enhance access rate to the folders and files.

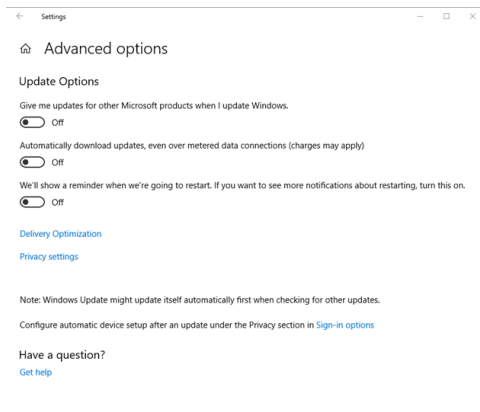
Run **CMD.exe** and enter: `fsutil behavior set disablelastaccess 1` and press **OK**.



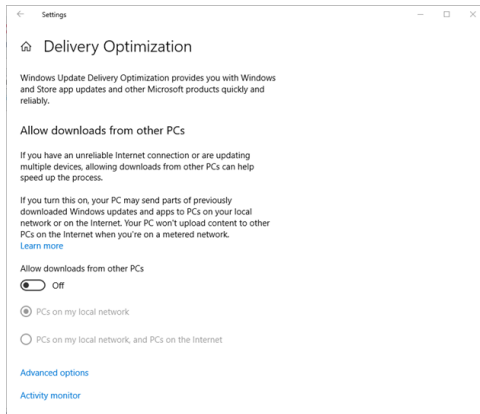
Restart your computer.

3. Disable automatic Windows update.

Open **Parameters > Update and security > Additional parameters** and check **Postpone component updates receive** box.



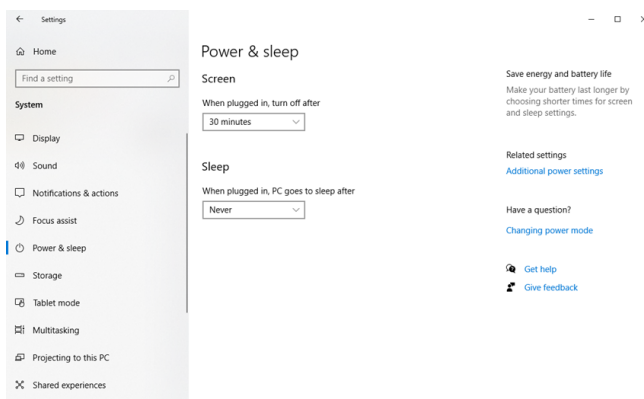
Open **Parameters > Update and security > Additional parameters > Select when and how to receive updates** and check **Off** box.



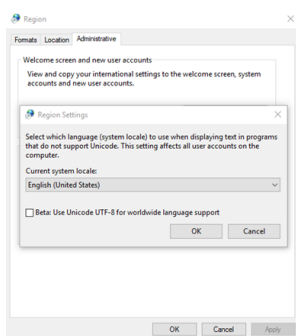
4. Disable Windows start screen, set display switch off parameters.

Open **Parameters** > **Personalization** and in the **Background** parameter select **No**.

Open **Parameters** > **System** > **Power and sleep mode** and in the parameter **Disconnect in..**, select **Never**.



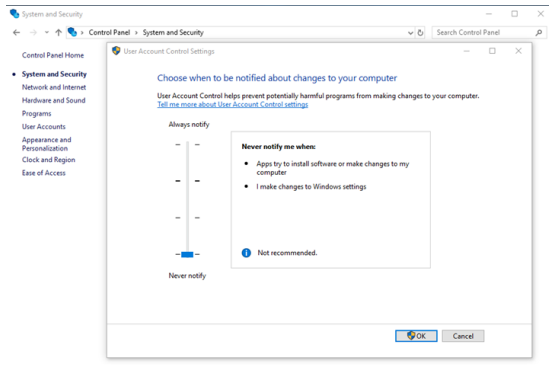
5. Open **Parameters** > **Time and language** > **Additional parameters of the date and time, regional parameters** > **Language** > **Additional parameters** and click **Apply language parameters to welcome screen, system user accounts and new accounts of users**. Tabpage **Additionally** in the setting **Language of programs not supporting Unicode** should have **English (United States)** selected.



6. Disable user account control (UAC).

Open **Control panel** > **User accounts** > **Change user accounts control parameters** and select **Never**.

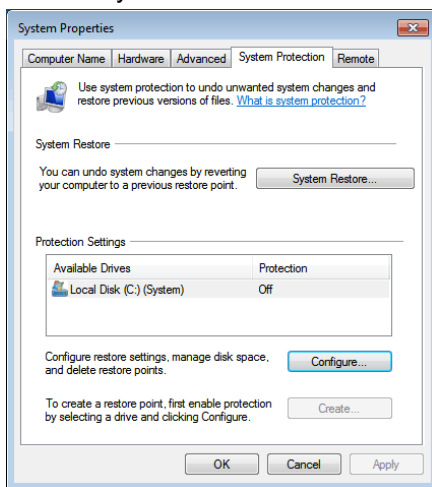




## Windows 7 settings

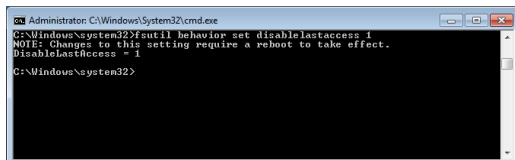
In order for TRASSIR to work properly on Windows 7, perform the following configuration:

### 1. Disable system restore on all disks.



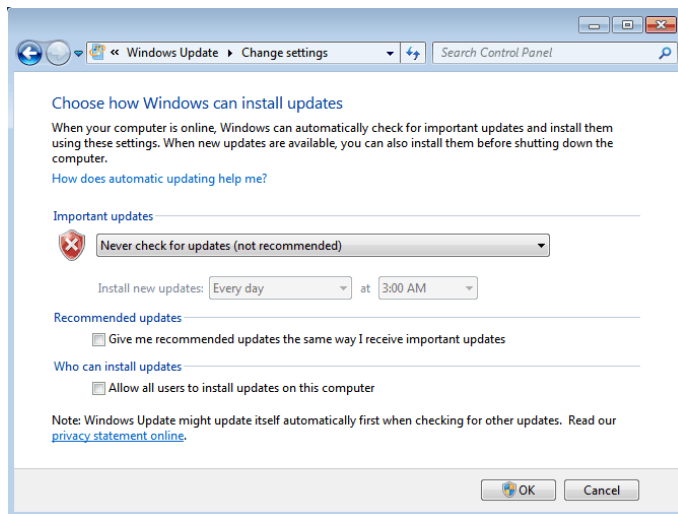
### 2. Enable `disablelastaccess` (disable the time of last access). This can help accelerate access to folders and files. To enable the setting:

- Open the **Start** menu;
- In the input field, enter: `fsutil behavior set disablelastaccess 1` and click **OK**;
- restart the computer for the changes to take effect.

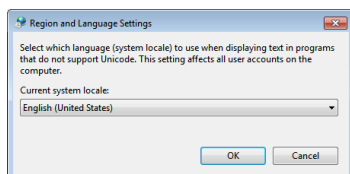


### 3. Disable automatic updating of Windows. To do this:

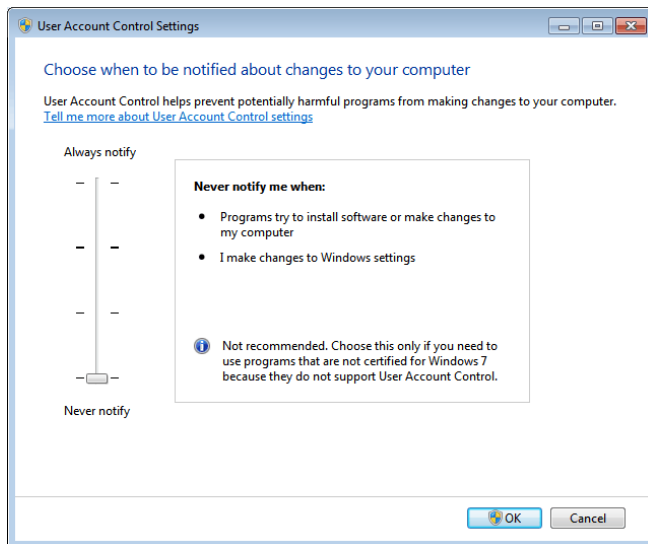
- Open **Control Panel > Windows Update**;
- In the left menu, select **Change settings**;
- In the settings window, select **Never check for updates (not recommended)** and click **OK**.



4. Disable the Windows screensaver and prevent the display from being turned off To do this:
- right-click anywhere on the desktop to bring up the context menu and select **Personalization**;
  - Click the **Screensaver** link;
  - In the Screensaver dropdown list, select **None** and click **Apply**;
  - click the **Change plan settings...** link;
  - Specify the following settings for all power plans that are used:
    - **Dim the display** - "Never";
    - **Turn off the display** - "Never";
    - **Put the computer to sleep** - "Never";
    - **Turn off hard disk after** - "Never".
5. Be sure that English is selected on the **Administrative** tab of the **Region and Language** window.



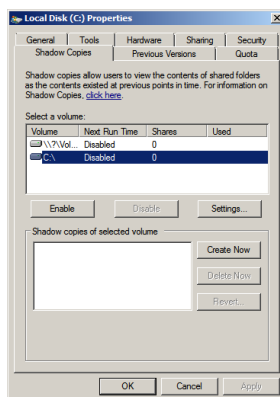
6. Disable user account control (UAC). To do this:
- open the **Control Panel** and select **User accounts**;
  - click the **Change User Account Control settings** link>;
  - In the settings window, select "Never notify" and click **OK**.



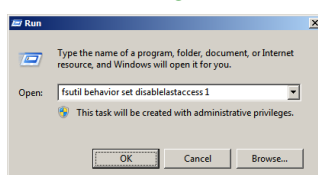
## Windows 2008 R2 settings

In order for TRASSIR to work properly on Windows 2008, perform the following configuration:

1. Be sure that shadow copying is disabled on all disks. To do this:
  - Open **My computer**.
  - Select a disk and right-click to bring up its context menu.
  - In the context menu, select **Properties**.
  - In the window that opens, go to the **Shadow copies** tab.
  - Be sure that for each of the computer's disks the value of the **Time of next launch** setting is "Disabled".



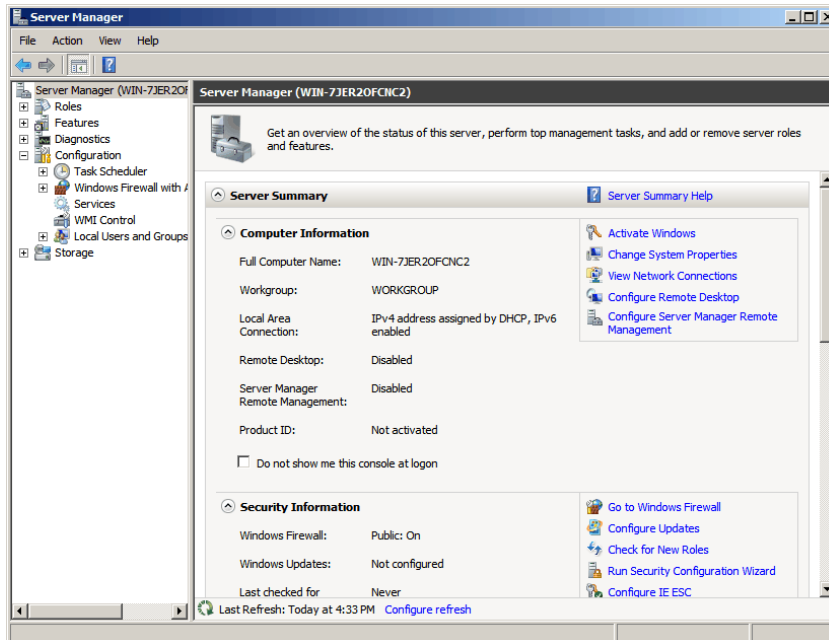
- If shadow copying is enabled, it must be disabled by clicking **Disable**.
2. Enable `disablelastaccess` (disable the time of last access). This can help accelerate access to folders and files. To enable the setting:
    - Use the **Start** menu to bring up the **Run** window.
    - In the **Run program** window that opens, enter the following: `fsutil behavior set disablelastaccess 1` and click **OK**.



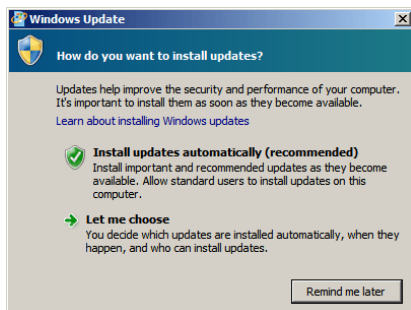
Restart the computer for the changes to take effect.

### 3. Disable automatic updating of Windows:

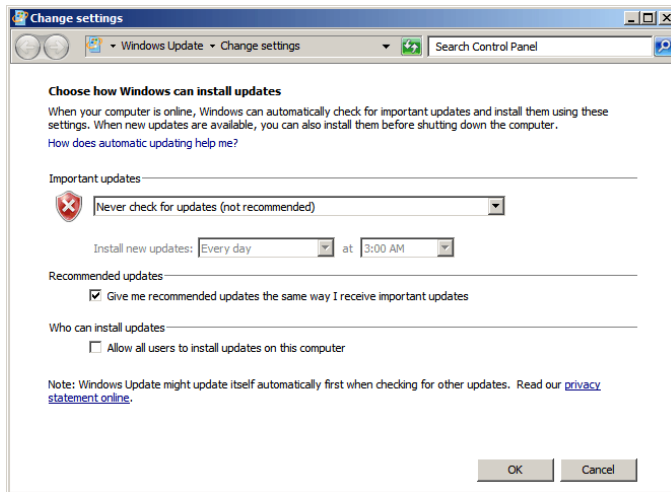
- Open **Start > Administrative Tools > Server Manager**.
- In the window that opens, go to the **Security system information** section and click on the **Configure updates** link on the right.



- In the **How updates are installed** window, select **Ask me**.

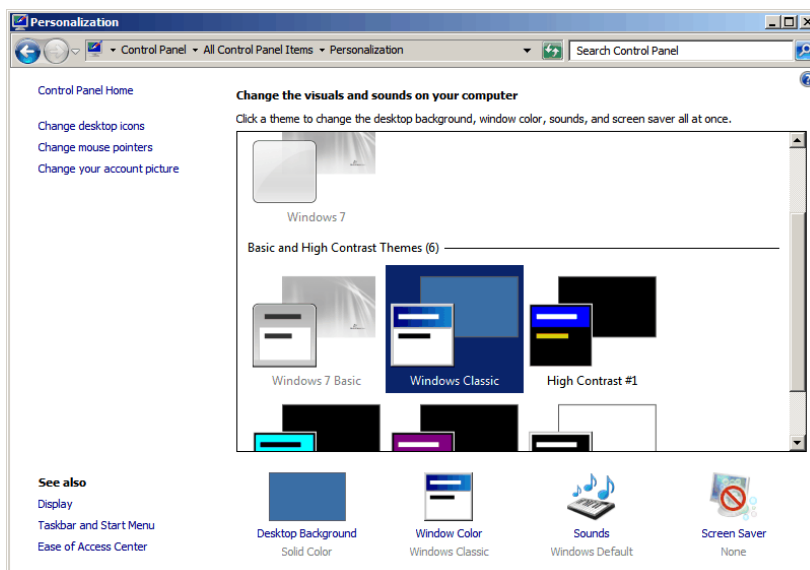


- In the **Change settings** window:
  - In the **Important updates** dropdown list, select **Never check for updates (not recommended)**;
  - Set the **Receive recommended updates the same way as important updates** checkbox;
  - Clear the **Allow all users to install updates on this computer** checkbox;
  - Click **OK**.

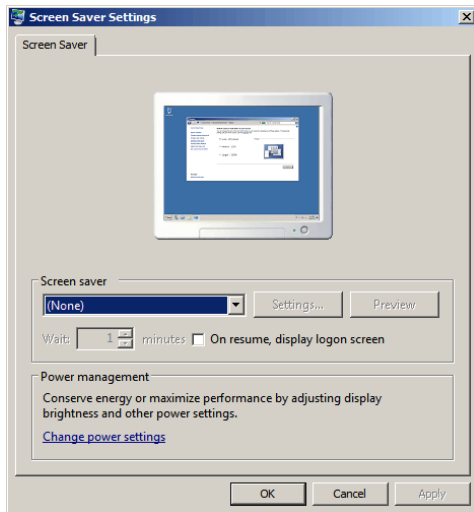


4. Be sure the screensaver is disabled:

- Right-click anywhere on the desktop to bring up the context menu.
- In the context menu, select **Personalization**.
- In the opened window, make sure that the value of the **Screensaver** parameter is set to "Never".

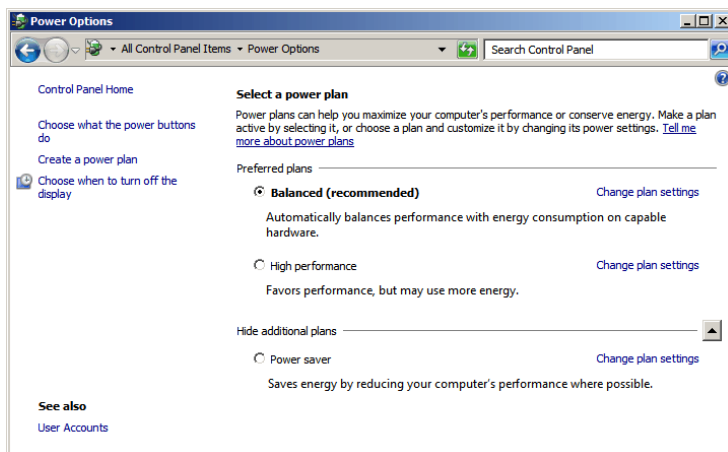


- If there is a screensaver, disable it:
  - Click the **Screensaver** link;
  - In the Screensaver settings window, select "None" in the **Screensaver** dropdown list;
  - Click **OK**.

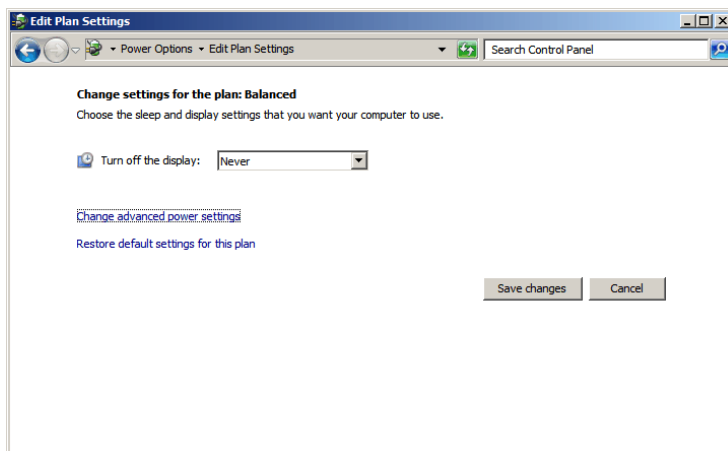


5. Disable turning off the display and sleep mode:

- Open **Control Panel > Power Options**.
- In the settings window, click the **Change plan settings** link opposite of the currently selected plan.



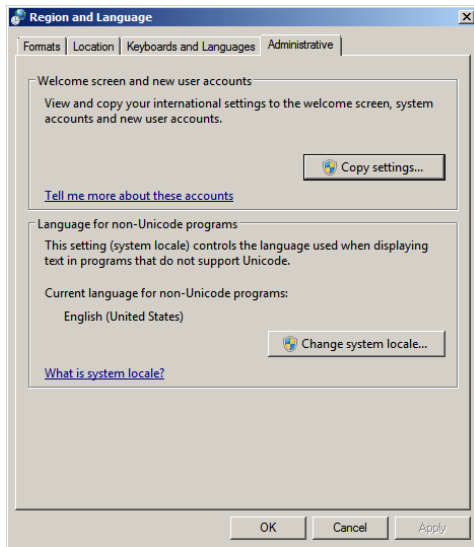
- In the **Turn off the display** dropdown list, select **Never**.



- Click **Save changes**.
- Perform the indicated changes for the remaining power plans.

6. Be sure that English is selected as the language for non-Unicode programs:

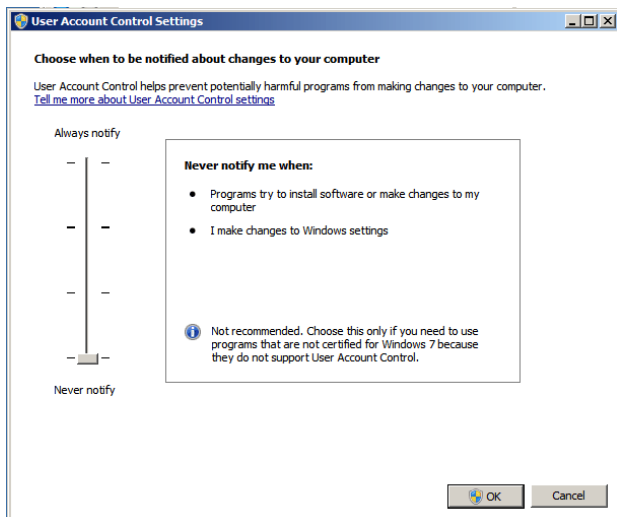
- Open **Control Panel > Region and Language**.
- In the **Region and Language** window, go to the **Administrative** tab.
- Be sure that the **Current language for non-Unicode programs** setting is "English (United States)".



- If needed, click the **Change system locale...** button and select English in the window that opens.

#### 7. Disable user account control (UAC):

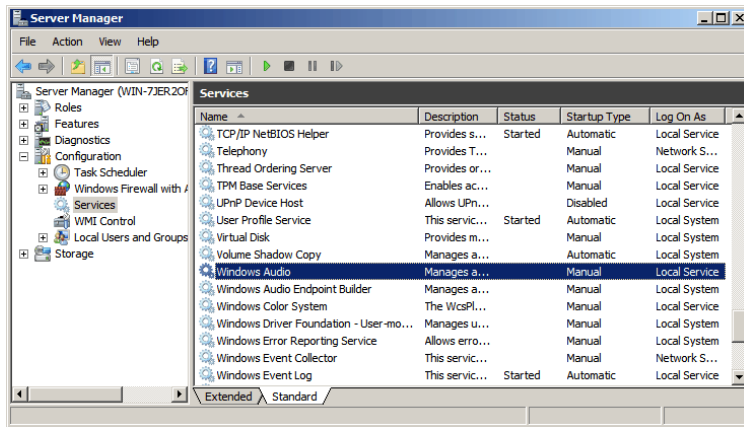
- Open **Control Panel > User accounts**.
- Click the **Change User Account Control settings** link.
- Move the slider to the "Never notify" position.



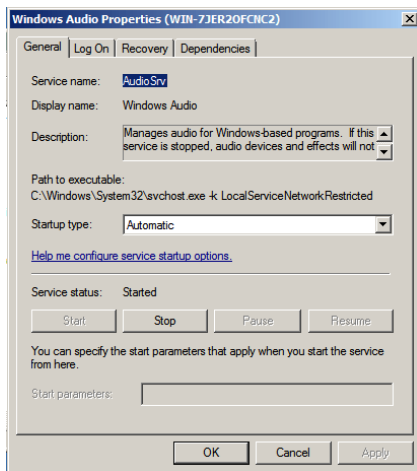
- Click **OK**.

#### 8. Enable the Windows Audio service. To do this:

- In the **Start** menu, right-click on **Computer**.
- In the context menu, select **Manage**.
- In the **Server Manager** window, open **Configuration > Services > Windows Audio**.



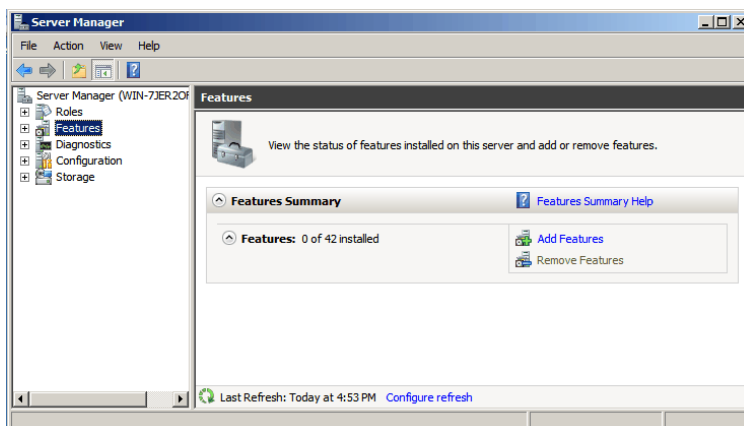
Start the service and change its startup type to "Automatic".



- Click **OK** in the service's properties window.

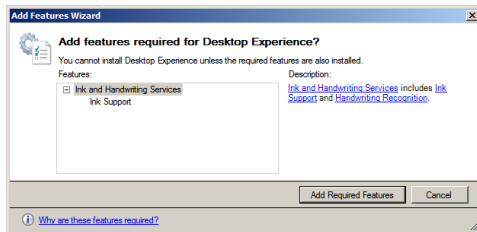
9. Enable the Desktop Experience. To do this:

- In the **Start** menu, right-click on **Computer**.
- In the context menu, select **Manage**.
- In the **Server Manager** window, select the **Features** tab.
- Click the **Add Features** link.

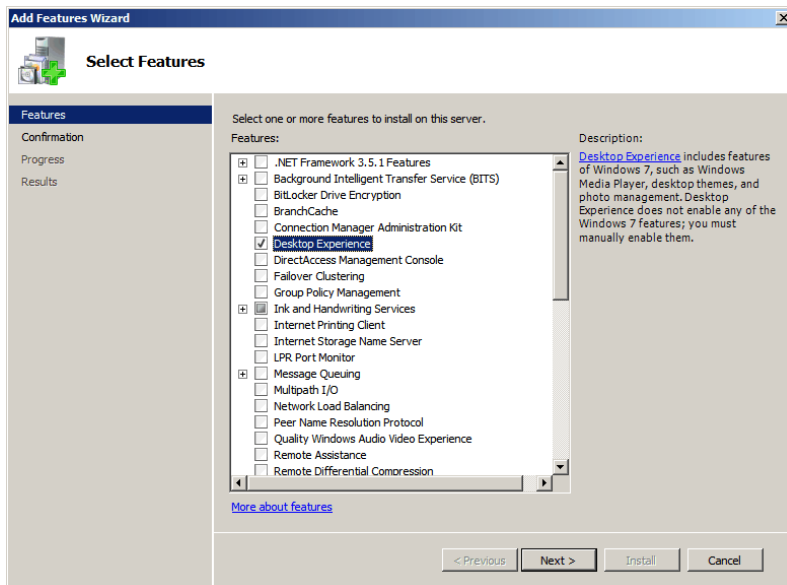


- In the **Add Features Wizard**, set the **Enable Desktop Experience** checkbox.
- Click **Add required features**.

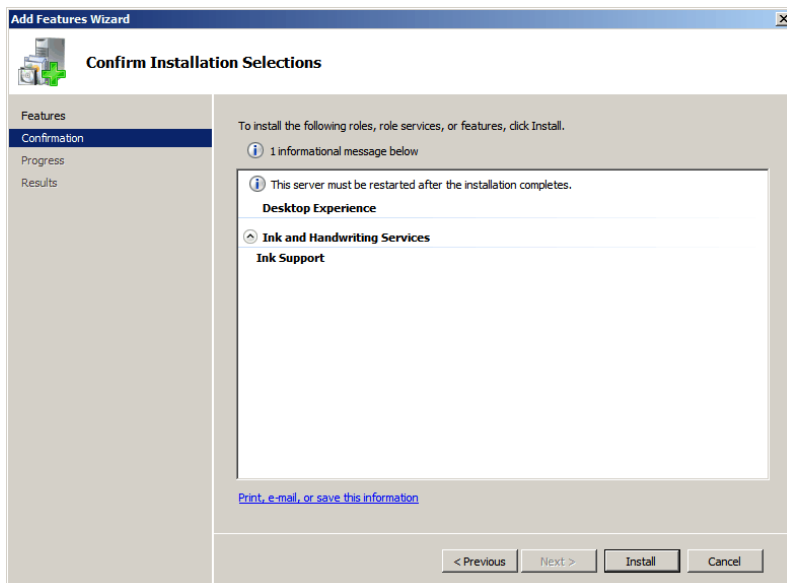




- Click **Next**.



- Click **Install**.

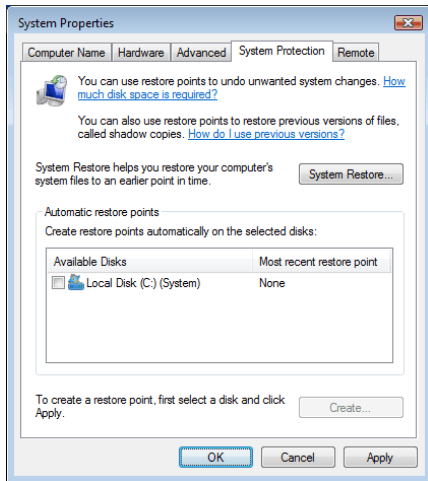


- After the installation completes, click **Close** and restart the computer.

## Windows Vista settings

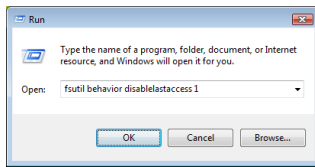
In order for TRASSIR to work properly on Windows Vista, perform the following configuration:

1. Disable system restore on all disks.



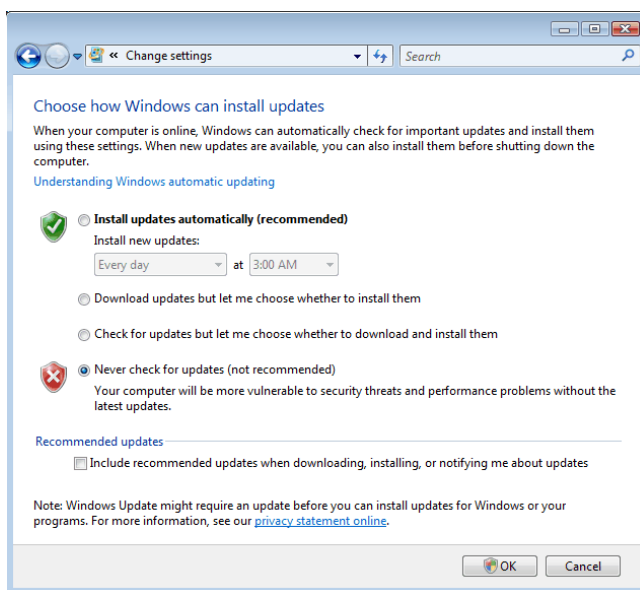
2. Enable `disablelastaccess` (disable the time of last access). This can help accelerate access to folders and files. To enable the setting:

- open **Start > Run**;
- In the input field, enter: `fsutil behavior set disablelastaccess 1` and click **OK**;
- restart the computer for the changes to take effect.



3. Disable automatic updating of Windows. To do this:

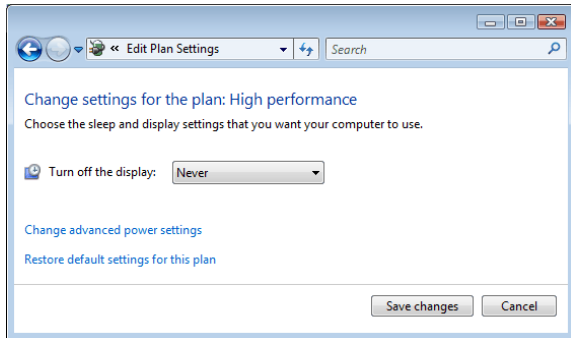
- Open **Control Panel > Windows Update**;
- In the left menu, select **Change settings**;
- In the settings window, select **Never check for updates (not recommended)** and click **OK**.



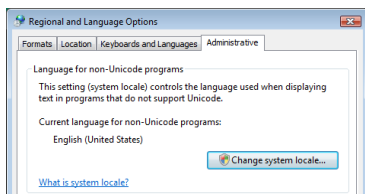
4. Disable the Windows screensaver and prevent the display from being turned off To do this:

- Right-click anywhere on the desktop to bring up the context menu and select **Personalization**;

- Click the **Screensaver** link;
- In the Screensaver dropdown list, select **None** and click **Apply**;
- click the **Change plan settings...** link;
- Specify the following settings for all power plans that are used:
  - **Turn off the display** - "Never";
  - **Put the computer to sleep** - "Never".

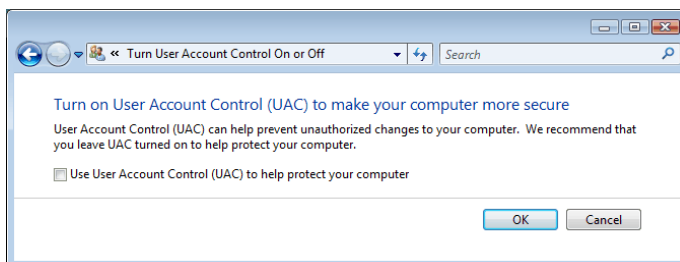


5. Be sure that English is selected on the **Administrative** tab of the **Region and Language** window.



6. Disable user account control (UAC). To do this:

- open the **Control Panel** and select **User accounts**;
- click the **Enable or disable User Account Control settings** link;
- in the settings window, clear the **Use User Account Control to protect my computer** checkbox and click **OK**.



Moreover, when configuring your network security settings, bear in mind that TRASSIR uses the following ports (the indicated values are used by default):

- PostgreSQL database cluster port - 5432;
- Server control port - 3080;
- Video broadcast port - 3081;
- Web server port - 8080;
- RTSP broadcast port - 554.
- HTTP broadcast port (flv, mjpeg) - 555.

- Cloud Connect activation port - 443/UDP.

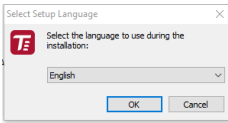
Be sure that your antivirus software does not monitor the ports used to connect and network devices. If needed, allow the use of the indicated ports and add TRASSIR 4 to the list of trusted applications after it is installed.



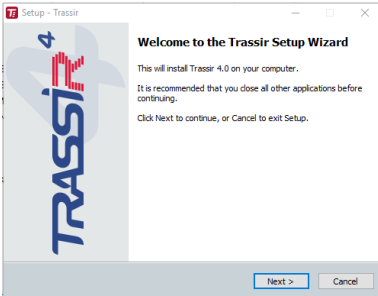
You can change the default port values.

## Installing TRASSIR server software

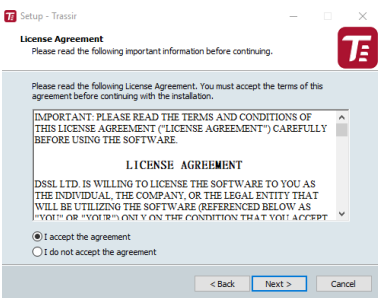
Start the executable TRASSIR Server installation file, select language and press **OK**.



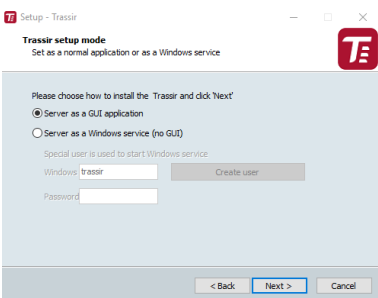
After a language is selected, the TRASSIR installer is started. Click **Next**.



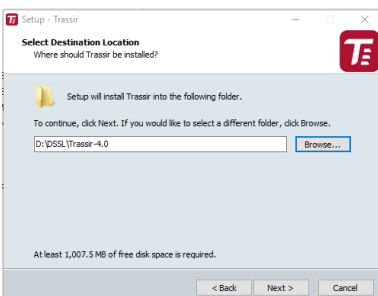
You can review the text of the license agreement on the **License agreement** screen. After reviewing the agreement, select **I accept the agreement** and click **Next**.



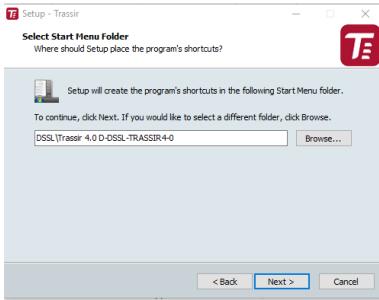
At the next step select the installation option **Server as GUI application** and press the button **Continue**.



Specify the TRASSIR installation folder by manually entering the path or by using the **Browse...** button. Click **Next**.

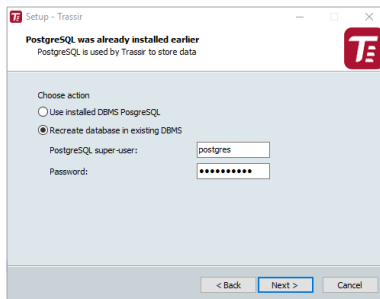


Specify the Start Menu folder where application shortcuts will be created. Click **Next**.



On the next screen, the installer will prompt you to install and configure the PostgreSQL DBMS. All events recorded in TRASSIR will be stored in the database. Although the software can work without connecting to a database, we strongly recommend using one. Moreover, certain modules require a database, i.e. *ActivePOS* and *AutoTRASSIR*. Depending on whether the DBMS is installed, the dialog window will look as follows:

- If a PostgreSQL database is already installed on the computer, the installer will prompt you to use the existing database; if you do not want to use the existing database, select **Recreate database in the existing DBMS** and enter the **PostgreSQL superuser password**. Otherwise, select **Use installed DMBS PostgreSQL**. Click **Next**.

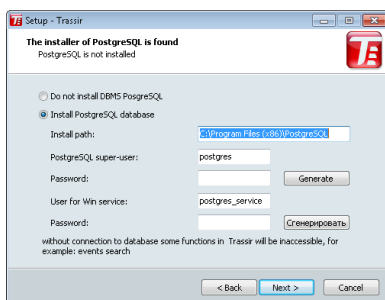


- In order to automatically install the database, download the archive of installation files from [our website](#) and unpack it in the same folder as the TRASSIR installer. You can also download PostgreSQL from its [official website](#) and perform the **database installation manually**.



Before beginning to install the database, you must configure the *operating system settings*.

If you have already the database installed or you want to do this later, select **Do not install DMBS PostgreSQL**. Otherwise select **Install PostgreSQL** and fill in all the fields. For your convenience, you can use the **Generate** buttons to generate passwords. After filling out all the fields, click **Next**. The installation of PostgreSQL will start automatically.

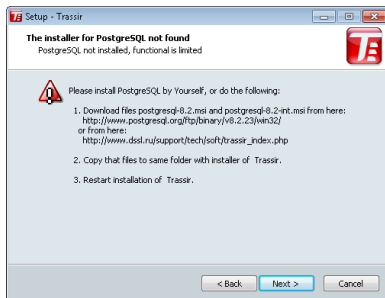




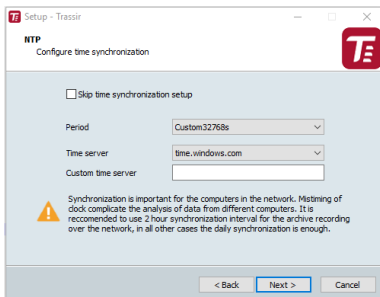
The **PostgreSQL superuser's password** can be selectable and you can subsequently create new database users.

The **Windows service user's password** must satisfy your operating system's security policy. To create a strong password, use the combination of uppercase and lowercase letters, as well as numbers and punctuation marks.

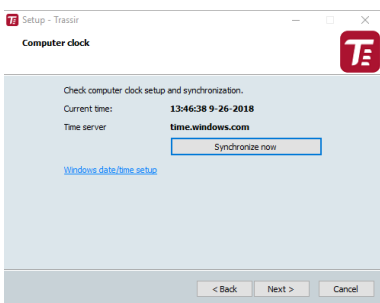
- If the installer cannot find the installation files for the DBMS next to the TRASSIR installer and PostgreSQL DBMS is not installed on the computer, the installer will issue a warning. Click **Next** to skip installation of the DBMS, or verify that the DBMS installation files are in the same folder as the TRASSIR installer and restart the installer.



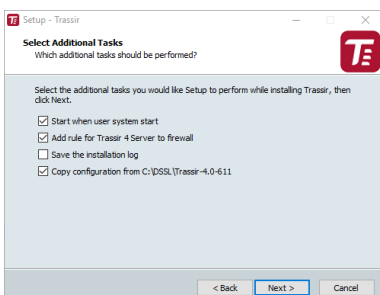
The TRASSIR installer will then prompt you to configure the time synchronization service (NTP). Select a synchronization **Period** and **Time server**. If needed, you can specify the address of an arbitrary NTP server or cancel the configuration of NTP by setting the **Skip time synchronization setup** checkbox. Click **Next**.



The TRASSIR installer will prompt you to verify the correctness of the server's current date and time. You can synchronize time using an NTP server by clicking the corresponding button or click the **Windows date/time setup** link to quickly navigate to the settings window. Click **Next**.

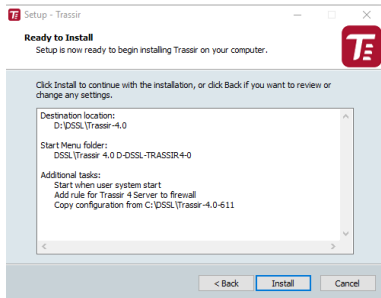


Select any additional installation settings. Click **Next**.

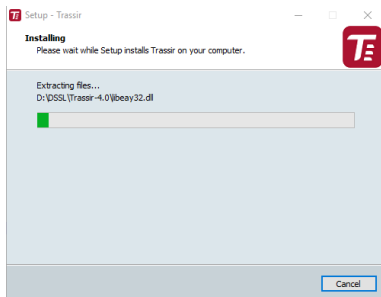


- **Start when user system starts** lets you restore a system to working order in the event of potential hardware failures, for example, if the electricity supplied to the site is unreliable.
- If you plan to use the standard Windows Firewall, then set the **Add rule for TRASSIR 4 Server to firewall** checkbox.
- If needed, you can **Save the installation log**.
- If you are installing to a different folder while updating TRASSIR, then setting the **Copy configuration from the previous installation** checkbox will copy all the settings from the previous version of TRASSIR. This will save time during the configuration process.

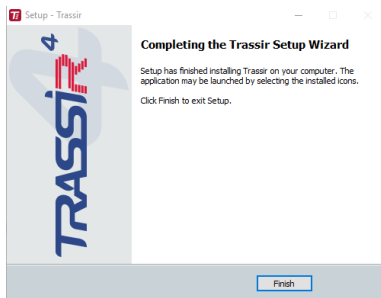
In its final screen, the TRASSIR installer will show the selected installation settings. Click **Install**.



The files will begin to be copied.



Complete the installation of TRASSIR by clicking **Finish**.

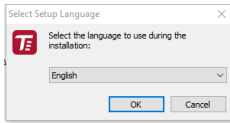


- *TRASSIR Server software installation as Windows service*
- *Installing Guardant USB keys*
- *Start the software and sign into the system*
- *Working with the basic interface*
- *Settings*
- *Installing TRASSIR client software*

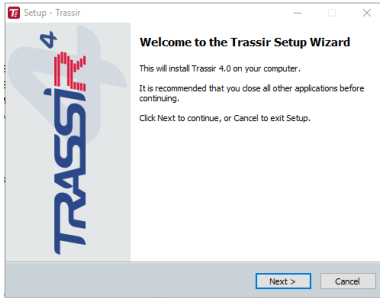


## TRASSIR Server software installation as Windows service

Run the executable file of TRASSIR Server installation, select language and press **OK**.



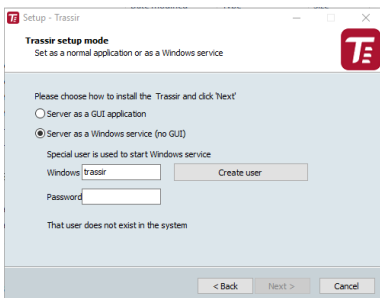
After a language is selected, the TRASSIR installer is started. Click **Next**.



You can look through the License Agreement text in the **License Agreement** window. To proceed with the installation check the **I accept the Agreement** box and press **Continue**.



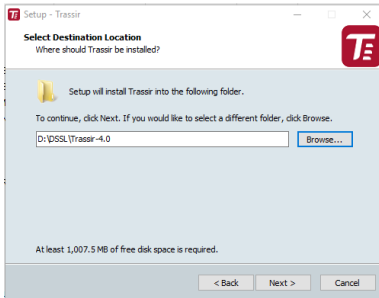
At the next stage select **Server as Windows service (without GUI)** installation option and enter the user data which will be used to run the service. In case such user is not available yet, you can create it, pressing **Create new user...**. Press **Next** to proceed.



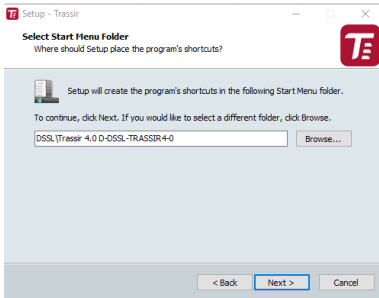
You can use a **TRASSIR client** to connect to a TRASSIR server that has been installed as a Windows service.

Learn more about connecting to a server in [Connecting to a new server](#).

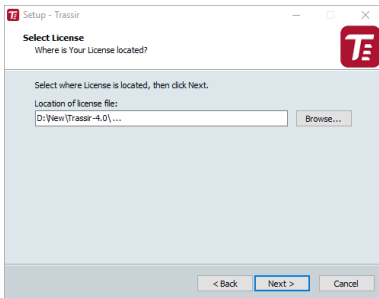
Select the installation folder by pressing **Browse** or enter the route manually. Press **Next**.




Select the folder in the Start menu to create program shortcuts. Press **Next**.



Locate license file and press **Next**.



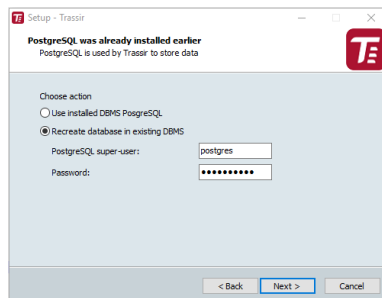
On the next screen, the installer will prompt you to install and configure the PostgreSQL DBMS.



All events recorded in TRASSIR will be stored in the database. Although the software can work without connecting to a database, we strongly recommend using one. Moreover, certain modules require a database, i.e. *ActivePOS* and *AutoTRASSIR*.

Depending on whether the DBMS is installed, the dialog window will look as follows:

- If a PostgreSQL database is already installed on the computer, the installer will prompt you to use the existing database; if you do not want to use the existing database, select **Recreate database in the existing DBMS** and enter the **PostgreSQL superuser password**. Otherwise, select **Use installed DBMS PostgreSQL**. Click **Next**.

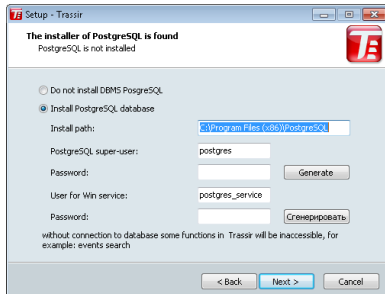


- In order to automatically install the database, download the archive of installation files from [our website](#) and unpack it in the same folder as the TRASSIR installer. You can also download PostgreSQL from its [official website](#) and perform the *database installation manually*.



Before beginning to install the database, you must configure the *operating system settings*.

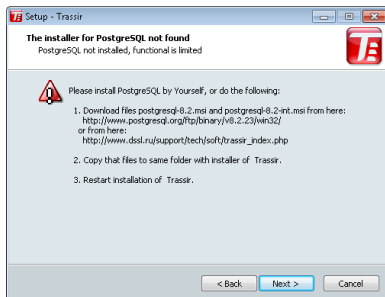
If you have already the database installed or you want to do this later, select **Do not install DBMS PostgreSQL**. Otherwise select **Install PostgreSQL** and fill in all the fields. For your convenience, you can use the **Generate** buttons to generate passwords. After filling out all the fields, click **Next**. The installation of PostgreSQL will start automatically.



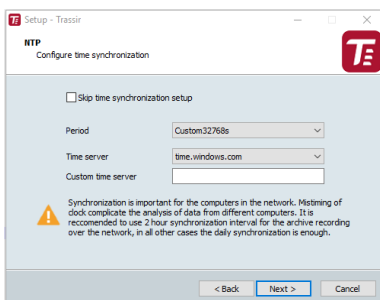
The **PostgreSQL superuser's password** can be selectable and you can subsequently create new database users.

The **Windows service user's password** must satisfy your operating system's security policy. To create a strong password, use the combination of uppercase and lowercase letters, as well as numbers and punctuation marks.

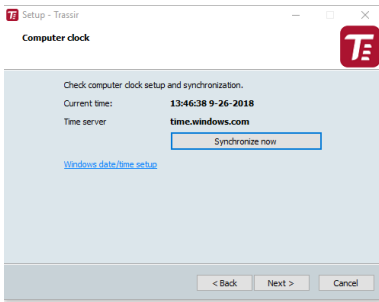
- If the installer cannot find the installation files for the DBMS next to the TRASSIR installer and PostgreSQL DBMS is not installed on the computer, the installer will issue a warning. Click **Next** to skip installation of the DBMS, or verify that the DBMS installation files are in the same folder as the TRASSIR installer and restart the installer.



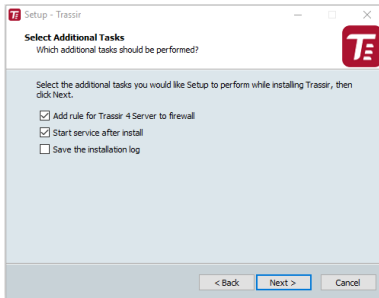
Next, set up time synchronization service (NTP). To do this, select **synchronization** period and **Time server**. You can insert the address of random NTP-server or cancel NTP setting by checking the box **Skip time synchronization setup**. Press **Next**.



The TRASSIR installer will prompt you to verify the correctness of the server's current date and time. You can synchronize time using an NTP server by clicking the corresponding button or click the **Windows date/time setup** link to quickly navigate to the settings window. Click **Next**.

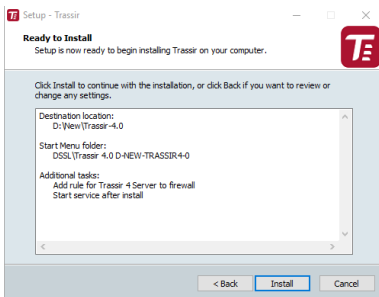


Select any additional installation settings. Click **Next**.

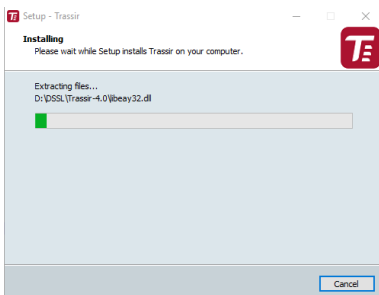


- **Add rules for TRASSIR 4 Server to firewall exception.** Check the box in case you use standard Windows firewall settings.
- **Reinstall the privileges for the user service account.** Check box to set the required rights of the user sufficient to provide correct operation of TRASSIR Server.
- **Run service on installation completion.** Check box to run TRASSIR Server service following its installation.
- If needed, you can **Save the installation log**.

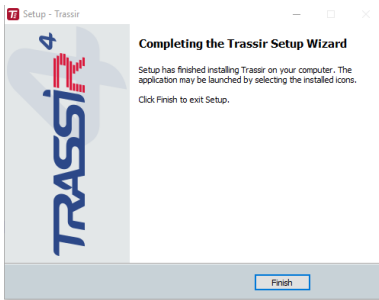
In its final screen, the TRASSIR installer will show the selected installation settings. Click **Install**.



The files will begin to be copied.



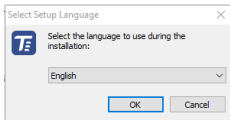
Complete the installation of TRASSIR by clicking **Finish**.



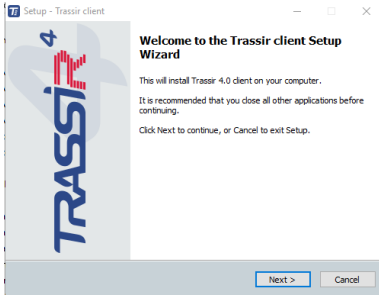
- *Installing TRASSIR server software*
- *Installing Guardant USB keys*
- *Start the software and sign into the system*
- *Working with the basic interface*
- *Settings*
- *Installing TRASSIR client software*

## Installing TRASSIR client software

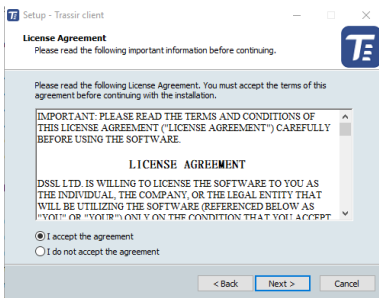
Run the executable file of TRASSIR-client installation, select language and press **OK**.



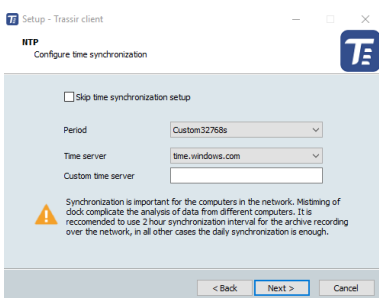
After a language is selected, the TRASSIR installer is started. Click **Next**.



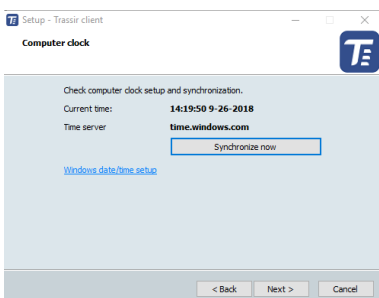
You can review the text of the license agreement on the **License agreement** screen. After reviewing the agreement, select **I accept the agreement** and click **Next**.



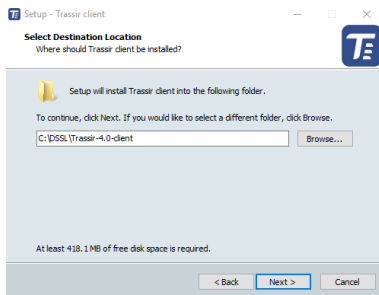
The TRASSIR installer will then prompt you to configure the time synchronization service (NTP). Select a synchronization **Period** and **Time server**. If needed, you can specify the address of an arbitrary NTP server or cancel the configuration of NTP by setting the **Skip time synchronization setup** checkbox. Click **Next**.



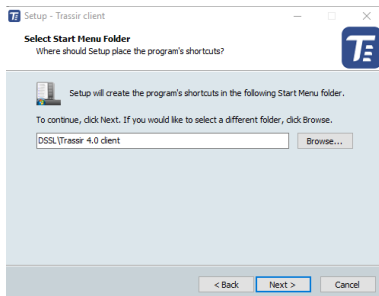
The TRASSIR installer will prompt you to verify the correctness of the server's current date and time. You can synchronize time using an NTP server by clicking the corresponding button or click the **Windows date/time setup** link to quickly navigate to the settings window. Click **Next**.



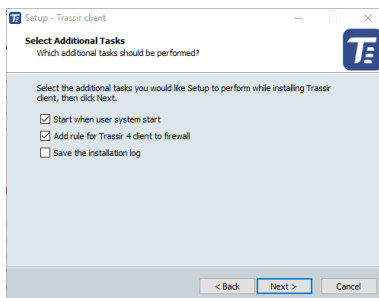
Specify the TRASSIR installation folder by manually entering the path or by using the **Browse...** button. Click **Next**.



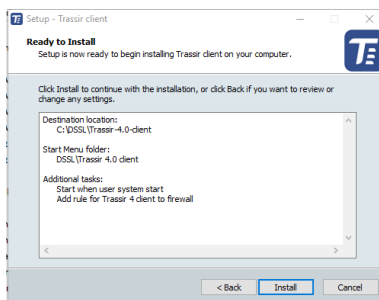
Specify the Start Menu folder where application shortcuts will be created. Click **Next**.



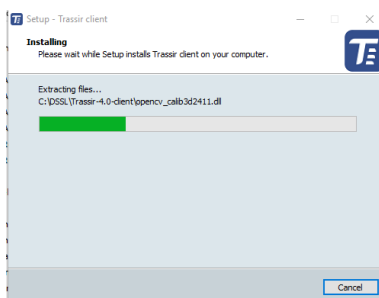
Select any additional installation settings. Automatically launching the application makes it possible to bring the system back in operation in the event of server hardware failures, for example, an unreliable supply of electricity to the site. If you plan to use the standard Windows Firewall, then set the **Add rule for TRASSIR 3 Client to firewall** checkbox. Click **Next**.



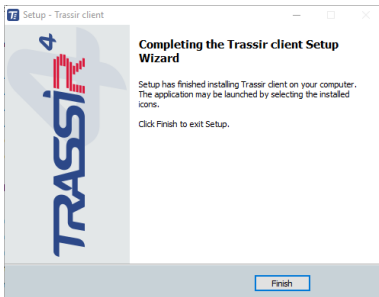
In its final screen, the TRASSIR installer will show the selected installation settings. Click **Install**.



The files will begin to be copied.



Complete the installation of TRASSIR by clicking **Finish**.



- *Working with the basic interface*
- *Connecting to a new server*
- *Installing TRASSIR server software*



## PostgreSQL DBMS installation

All events registered by TRASSIR are stored in the database. The database can be located on either a local or remote server. For example, a separate server, used only for recording events, may be chosen for the database.

A computer with the following minimum specifications is required to install PostgreSQL DBMS:

- Processor: Intel Pentium D 1.8 GHz or greater.
- RAM: 2 GB or greater.



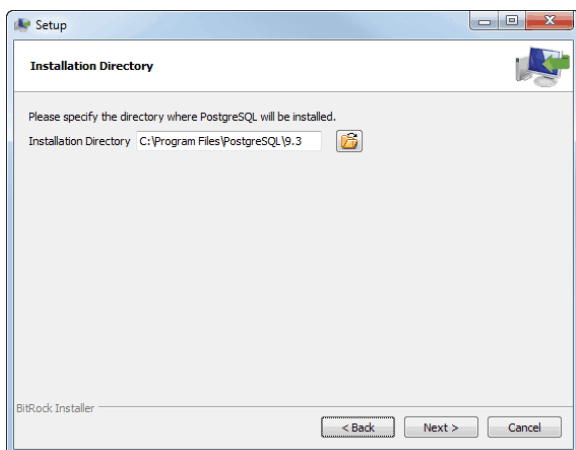
Before installing the PostgreSQL DBMS, review [Configuring the operating system to work with the PostgreSQL DBMS](#)

As an example, let us consider the installation of PostgreSQL DBMS 9.3.4 on Windows 7:

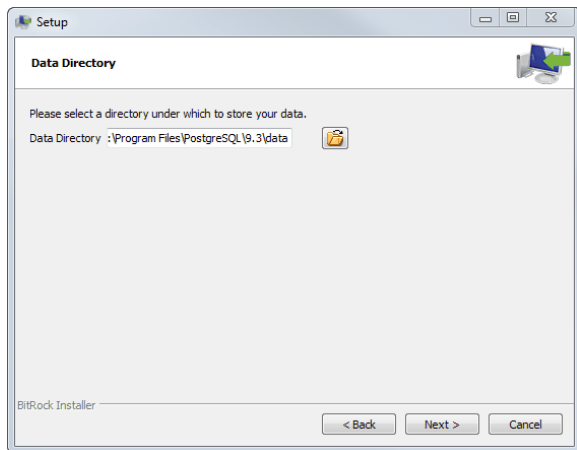
1. Download the PostgreSQL distribution from the [PostgreSQL website](#) (it's free).
2. Launch the installer and click **Next >** in the window that opens.



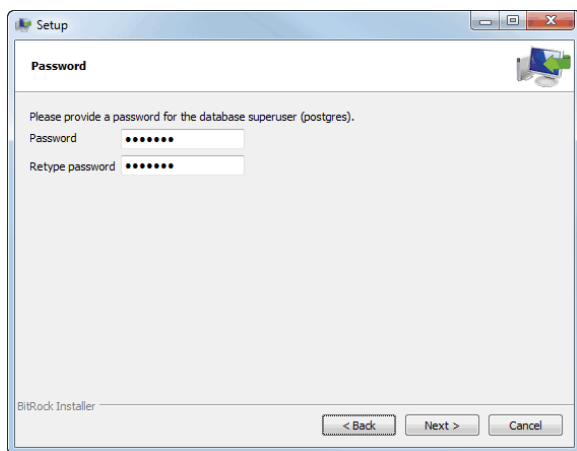
3. Select the database installation folder and click **Next >**.



4. After that select the folder that contains the DBMS files. Click **Next >** to continue.

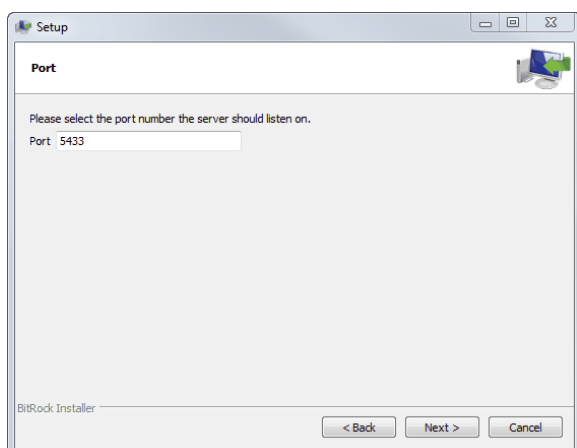


5. In the next step, enter the DBMS's superuser's password. Click **Next >** to continue.

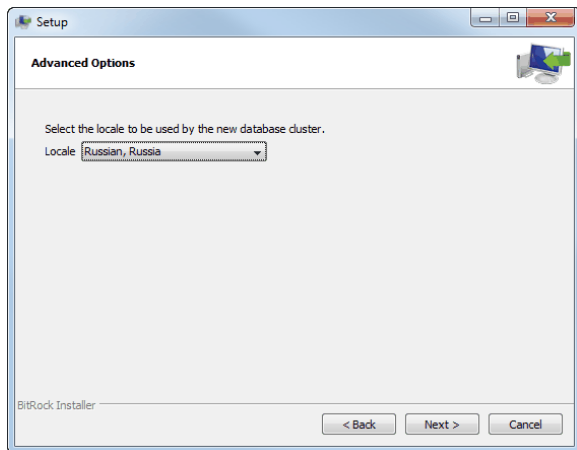


We strongly recommend that you memorize or write down the superuser's password. This password is required to *configure the database connection* and create a backup copy if the *DBMS is moved to a different server*.

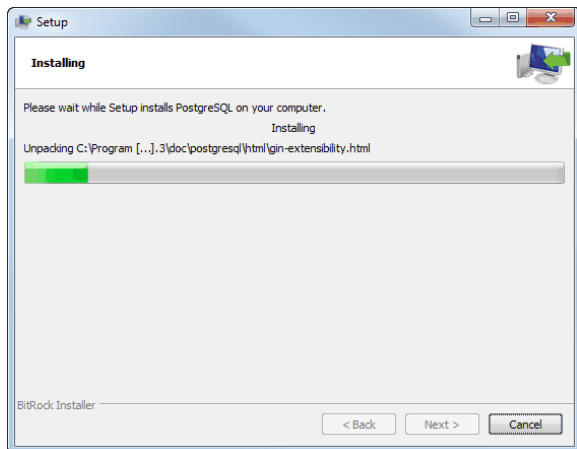
6. If needed, you can change the DBMS connection port. Click **Next >** to continue the installation.



7. In the next stage, select **Russian, Russia** in the Locale field. Click **Next >** to continue the installation.



8. Click **Next** on the next screen and wait for the installation to complete.



9. When the installation is complete, clear the **Launch Stack Builder at exit?** checkbox and click **Finish**.



- *Configuring the operating system to work with the PostgreSQL DBMS*
- *Starting the PostgreSQL Database Server service*
- *Moving a PostgreSQL database to a different server*
- *Allowing external connections to the PostgreSQL DBMS*
- *Database connection settings*

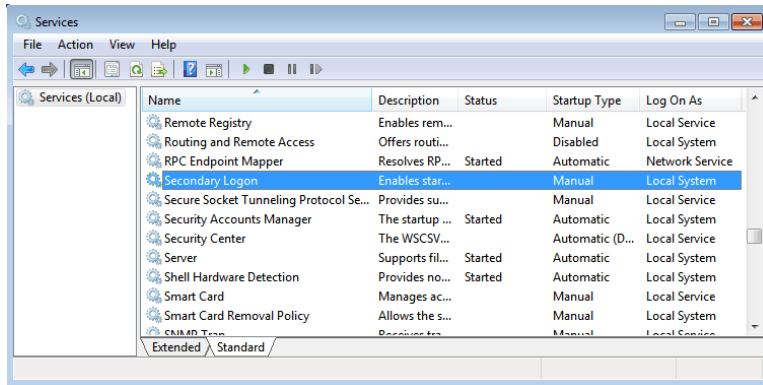
## Configuring the operating system to work with the PostgreSQL DBMS

Before installing PostgreSQL DBMS, be sure that the Secondary Logon service is running on Windows. This service is disabled by default in Windows 7.

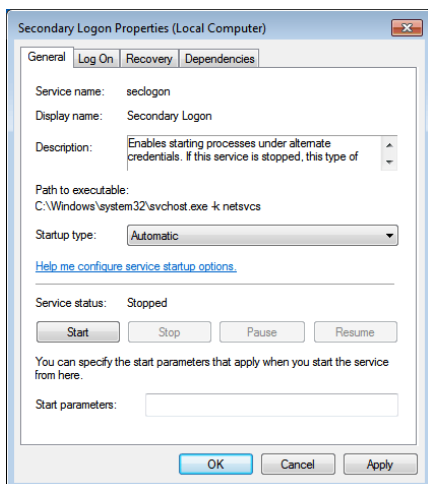
If the service is disabled, you will not be able to install the PostgreSQL DBMS.

To start the Secondary Logon service:

1. Bring up the Windows services management window by running `services.msc`.



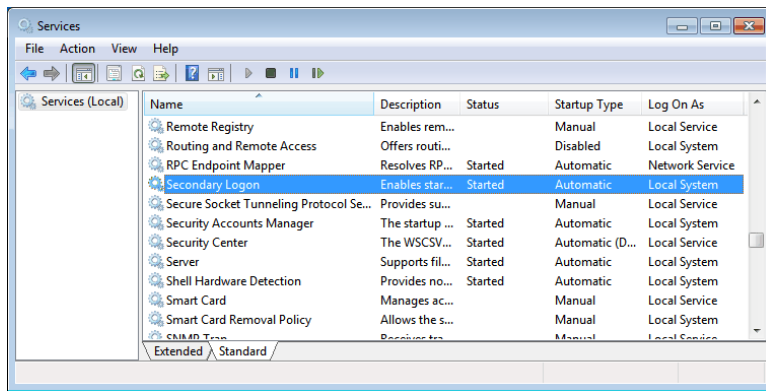
2. Find the **Secondary Logon** service in the list of services and double-click on it to open its settings window.



3. In the service's settings window:

- Select "Automatic" in the **Startup type** field;
- Click **Start**;
- Click **OK**.

4. Verify that the service started successfully in the window with the list of services (the **Status** field should say "Started").



- *PostgreSQL DBMS installation*
- *Starting the PostgreSQL Database Server service*
- *Allowing external connections to the PostgreSQL DBMS*
- *Database connection settings*

## Starting the PostgreSQL Database Server service

After installing PostgreSQL DBMS, the PostgreSQL Database Server service will be enabled by default. If the service is disabled, then TRASSIR will not be able to access the database and consequently it will not be possible to record events in the database. You can check if the service is enabled in two ways:

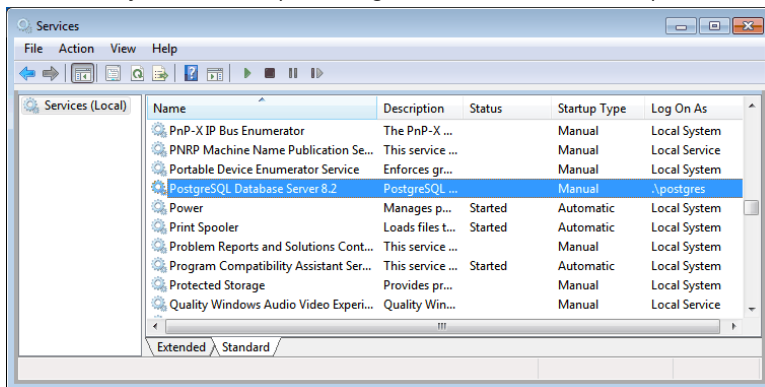
- using the standard tool for managing Windows services;
- using the pgAdmin III utility, which is installed together with PostgreSQL DBMS.



The service's name will be different if you changed it during installation (see step 7 of the [PostgreSQL DBMS installation](#) section).

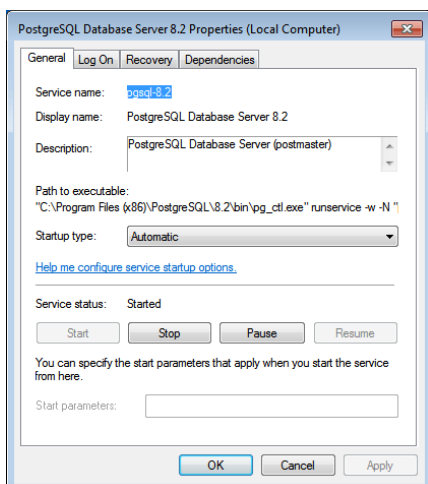
To verify that the service is enabled using the standard Windows tool:

1. Open the Windows services management window by running `services.msc`.
2. In the window with the list of Windows services, find the PostgreSQL Database Server and be sure the Status column says "Started" (meaning the service is enabled).

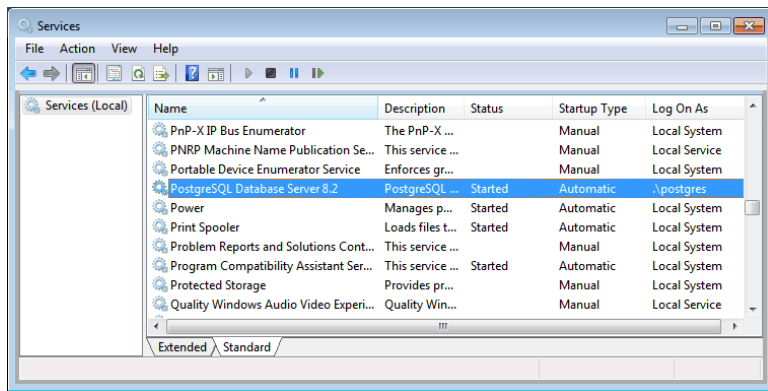


3. If the service is disabled, then open its settings window by double-clicking with the mouse. In the service's settings window:

- Select "Automatic" in the **Startup type** field;
- Click **Start**;
- Click **OK**.

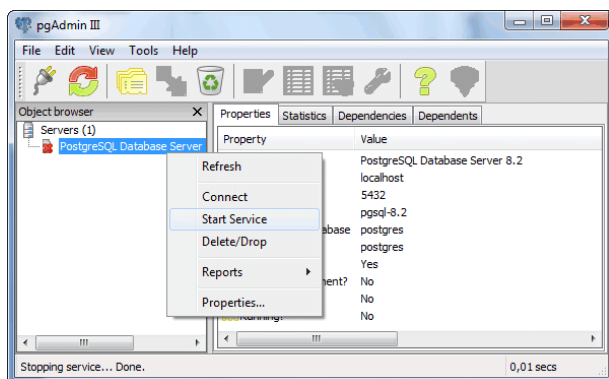


4. Verify that the service started successfully in the window with the list of services (the **Status** field should say "Started").

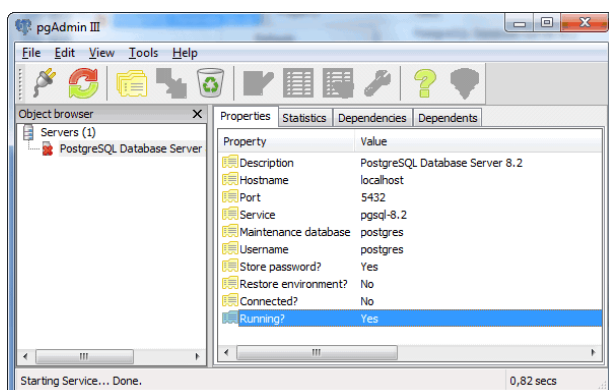


To verify that the service is enabled using the pgAdmin utility:

1. Launch the pgAdmin utility by running `C:\Program Files (x86)\PostgreSQL\8.2\bin\pgAdmin3.exe`.
2. In the window that opens:
  - Select the service in the list;
  - Bring up its context menu by right-clicking with the mouse;
  - Be sure the services enabled (the **Running** field should say "Yes");
  - If the service is disabled, enable it by selecting **Start Service** in the context menu.



3. Be sure that the service started successfully (the **Running** field should say "Yes").





- *PostgreSQL DBMS installation*
- *Configuring the operating system to work with the PostgreSQL DBMS*
- *Allowing external connections to the PostgreSQL DBMS*
- *Database connection settings*



## Moving a PostgreSQL database to a different server

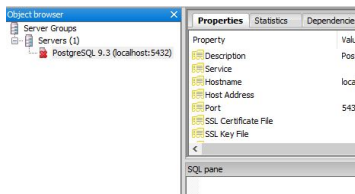
These instructions will help you move a PostgreSQL database from one server to another. We will consider the process of moving a database using PostgreSQL DBMS version 9.3.4 on Windows 7 as an example.

First, prepare the new PostgreSQL DBMS server to which the database is being migrated. To do this:

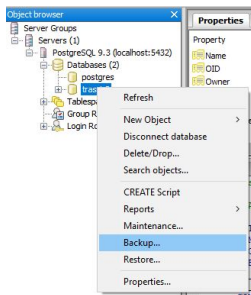
- *Configure the operating system to work with the DBMS;*
- *Install the DBMS;*
- *Launch the PostgreSQL Database Server service.*

Create a backup copy of the old database. To do this:

1. Launch the pgAdminIII utility (**Start -> PostgreSQL 9.3 -> pgAdmin III**).
2. Connect to the database by double-clicking on **PostgreSQL 9.3 (localhost:5433)**. If you are prompted for a password, enter the superuser's password that was specified during *installation of the DBMS*.

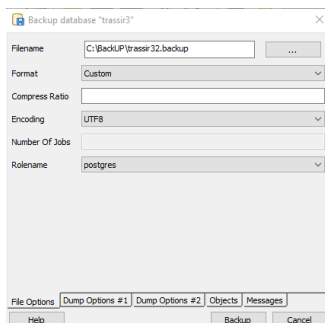


3. In the tree, select the database that you want to move to the new server and select **Backup...** in the context menu

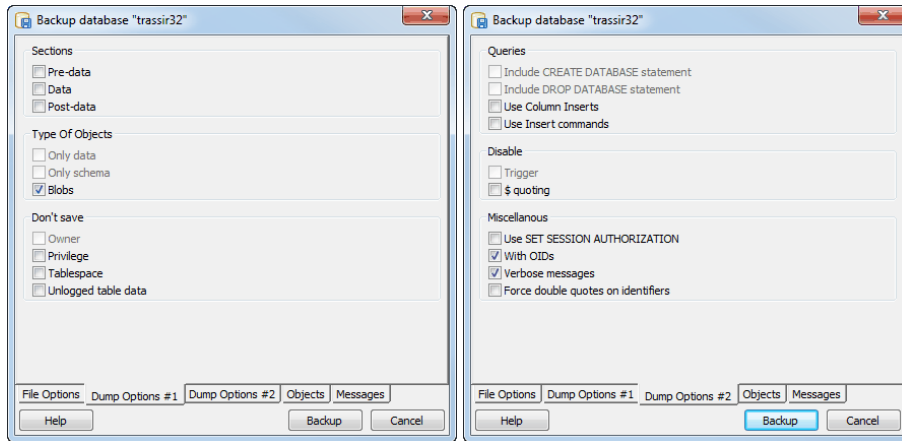


4. On the window that opens, in the **File Options** tab:

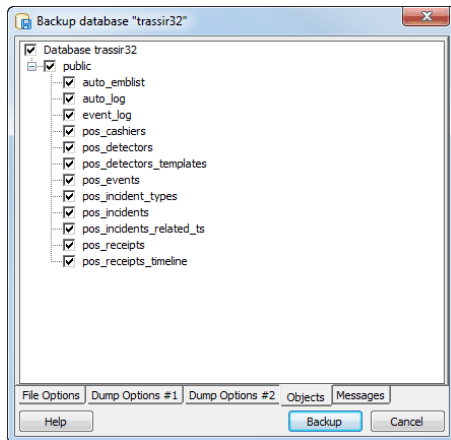
- Enter the **Filename** of the backup;
- In the **Format** field, select **Custom**;
- Leave the **Compress Ratio** field unchanged;
- In the **Encoding** field, select **UTF8**;
- In the **Rolename** field, select **postgres**;



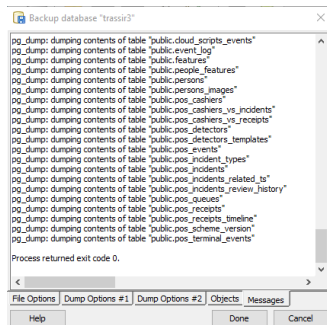
5. In the **Dump Options #1** and **Dump Options #2** tabs, set the checkboxes as shown in the images below:



6. Go to the **Objects** tab and set all of the checkboxes in the object tree:



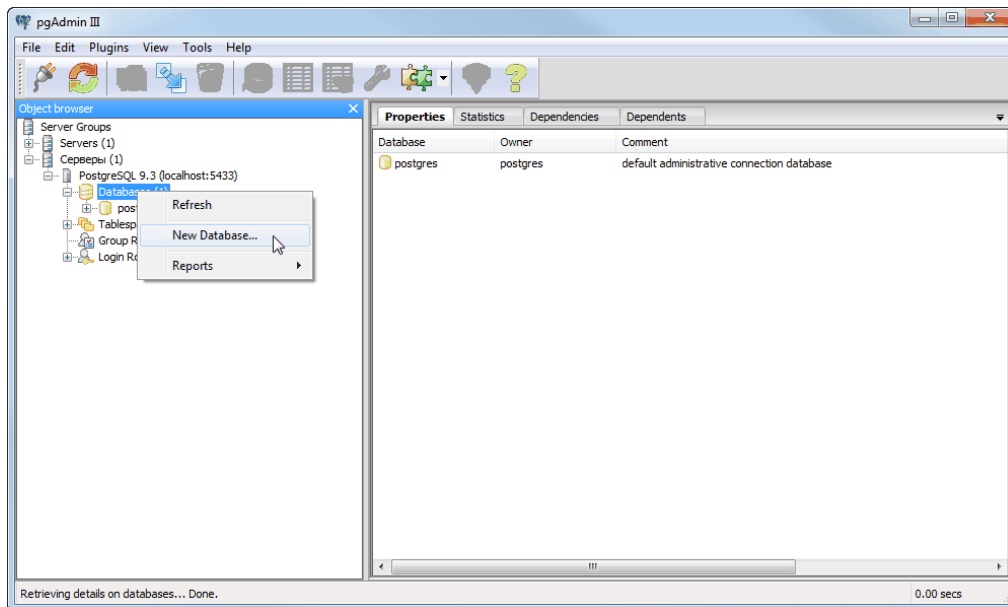
7. Go to the **Messages** tab and start backing up the database by clicking the **Backup** button.



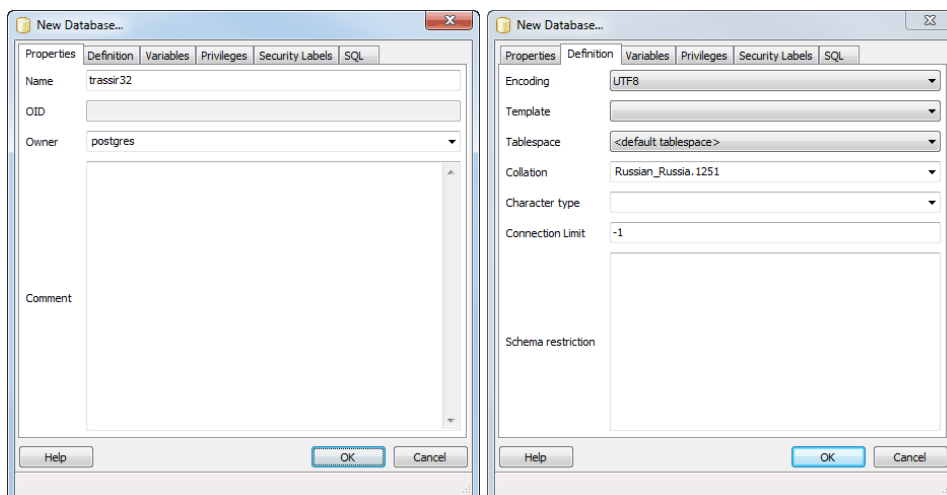
As the backup is created, messages will be displayed in the window. If the backup is created successfully, then **Process returned exit code 0** should appear last. Otherwise, verify the settings described above and repeat the process to create a backup.

After the backup has been created, move it to the new server and use it to restore the database. To do this:

1. Launch the pgAdminIII utility (**Start** -> **PostgreSQL 9.3** -> **pgAdmin III**).
2. Connect to the database by double-clicking on **PostgreSQL 9.3 (localhost:5433)**. If you are prompted for a password, enter the superuser's password that was specified during *installation of the DBMS*.
3. Select **Databases** in the tree and select **New Database...** in the context menu

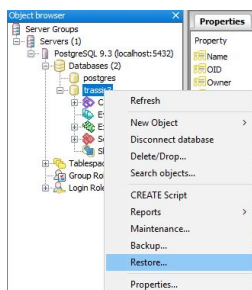


4. In the window that opens, in the **Properties** and **Definition** tabs, enter the parameters just as they appear in the images below:



In the **Name** field, enter the name of the database on the new server. Leave the parameters on the remaining tabs unchanged and click **OK** to create the new database.

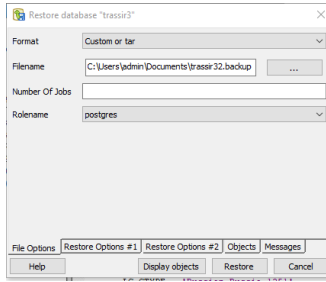
5. Select in the tree the newly created database and select **Restore...** in the context menu



6. On the window that opens, in the **File Options** tab:

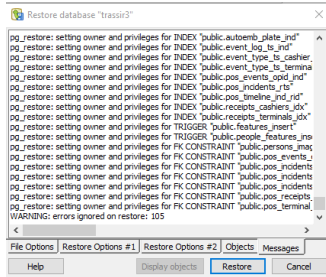
- In the **Format** field, select **Custom or tar**;
- In the **Filename** field, enter the path to the previously saved backup;
- Leave the **Number of Jobs** field unchanged;

- In the **Rolename** field, select **postgres**;



Leave the remaining tabs' parameters unchanged.

7. Go to the **Messages** tab and start restoring the database by clicking the **Restore** button.



As the database is restored, messages will be displayed in the window. If the database is successfully restored, then **Process returned exit code 0** should appear last. Otherwise, verify the settings described above and repeat the process to restore the database.

This completes the PostgreSQL database migration process. Now you can change the *database connection settings in TRASSIR*.



- *Database connection settings*

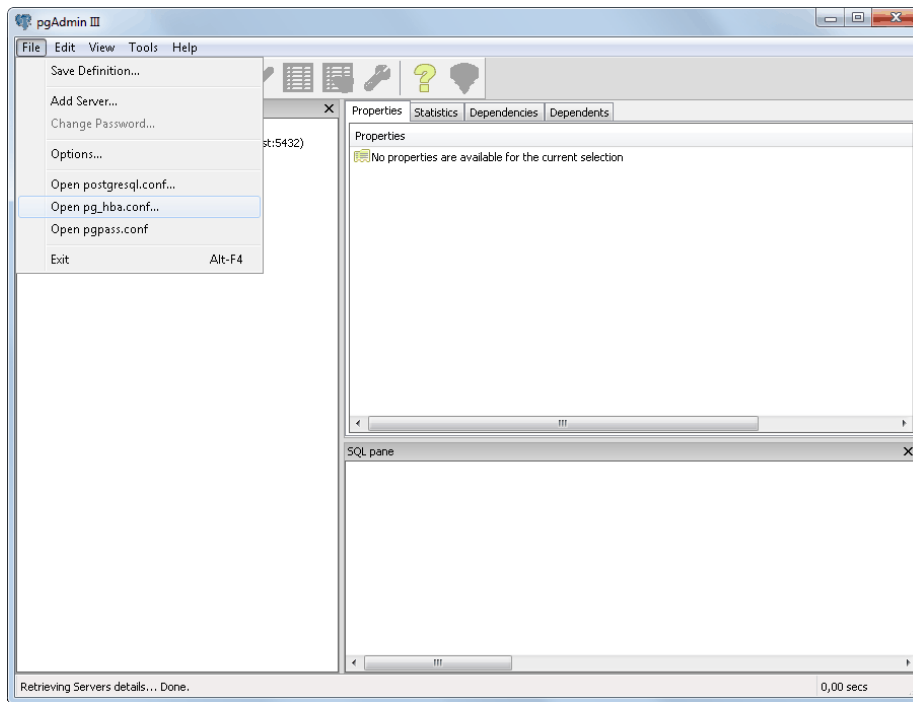
## Allowing external connections to the PostgreSQL DBMS

The file should be edited to allow external connections to the data base server `pg_hba.conf` and restart the PostgreSQL Database Server service.

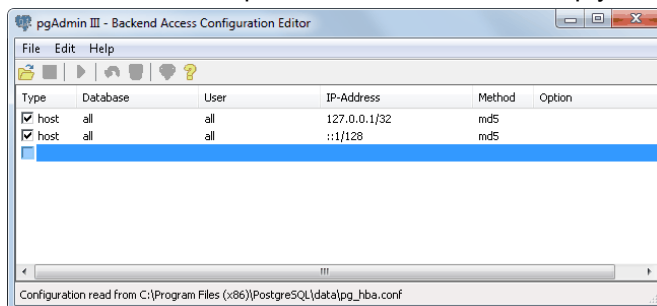
The file `pg_hba.conf` is located in `C:\Program Files (x86)\PostgreSQL\<version number>\data`. You can edit it in any text editor or with the pgAdmin utility.

To configure external connections using the pgAdmin utility:

1. Run the pgAdmin utility.
2. In the **File** menu, select **Open pg\_hba.conf...**

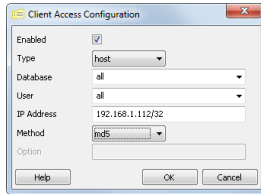


3. Select `pg_hba.conf` to configure the external connections.
4. In the window that opens, double-click in the empty checkbox for adding a new authorized connection.



5. Specify the connection parameters:
  - **Enabled** - Set the checkbox. If the checkbox is cleared, the connection will be preserved in `pg_hba.conf` as a comment, i.e. it will be inactive.
  - **Type** - Select "Host" from the dropdown list (authorization at the host level).
  - **Database** - Select "All" from the dropdown list (the connection is authorized to all databases).
  - **User** - Select "All" from the dropdown list (the connection is authorized for all users).
  - **IP Address** - Specify the range of IP addresses (given as [IP address/Mask]) from which the connection will be made. For example: "192.168.1.112/32".

- **Method** - Select "md5" (the type of encryption for data transmission).

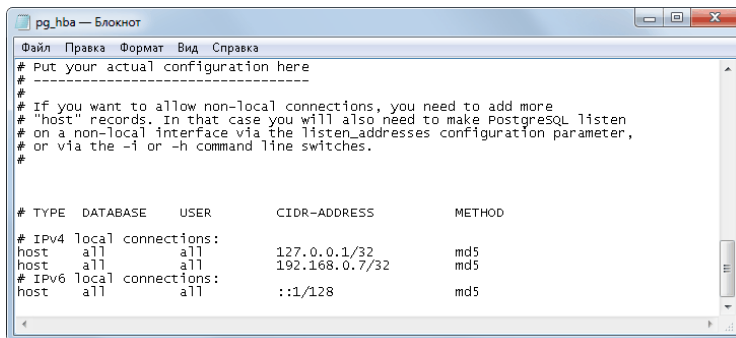


All addresses correspond to a "zero" subnet mask (signified by /0). A specific IPv4 address corresponds to a subnet mask with a 32-bit prefix (signified by /32).

6. If needed, add other connections in a similar manner (see step 5).
7. Press **CTRL+S** to save `pg_hba.conf`, and close the pgAdmin utility.

To configure external connections using a text editor:

1. Open `pg_hba.conf` using a text editor (for example, Notepad).
2. Find the following line in the file:  
# IPv4 local connections
3. In the list that follows, at a record that corresponds to the range of IP addresses of the computers from which the connection will be made.



For example:

```
host all all 192.168.0.7/32 md5
```

where:

- "host" means authorization at the host level.
- "all all" means access is available for all users to all databases.
- "192.168.0.7/32" is the range of IP addresses of the computers from which the connection will be made, given as [IP address/Mask]; in this case, it represents a single IP address.
- "md5" is the type of encryption for data transmission.



- [PostgreSQL DBMS installation](#)
- [Configuring the operating system to work with the PostgreSQL DBMS](#)
- [Starting the PostgreSQL Database Server service](#)
- [Database connection settings](#)

## Connecting analog PTZ cameras

Analog PTZ cameras are controlled through an RS-232 interface.

Ways to connect PTZ cameras:

1. **Connecting using an analog converter.** To connect through a serial port, a converter is required to transform signals from the camera (RS-485) to signals for the computer's serial port (RS-232).

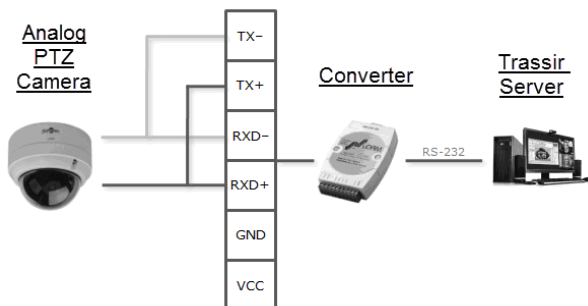
PTZ cameras have an RS-485 control interface. This interface can control video cameras at a distance of up to 1200 m in full-duplex mode when connected with a 4-wire cable, or in half-duplex mode - when connected with a 2-wire cable.

Thus, industrial converters with full-duplex or half duplex data transmission capabilities are required for the camera operate correctly. We strongly recommend using the following converters models:

- Moxa TCC-100.
- Adlink ND-6520.
- IronLogic Z-397.
- U-tek UT-208.

Connection procedure:

- Connect the camera to the converter.
- Connect the converter to the computer's COM port (RS-232) in accordance with the layout. If a full-duplex converter is being used in half duplex mode (with a two wire cable), then a couple of TX+/RXD+ and TX-/RXD- jacks must be connected in parallel.

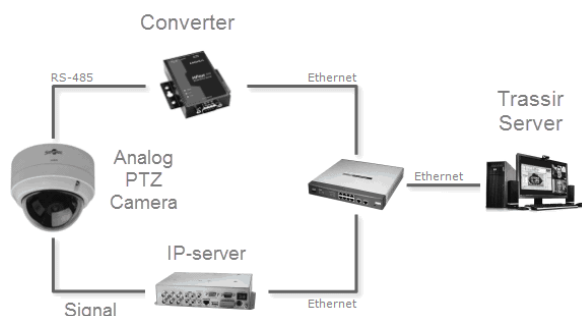


2. **Connecting using a network converter.** A network converter connects directly to the local network and has its own IP address, which must be bound to the server's serial port.

We strongly recommend using the NPort 5130 or NPort 5150 network converters. You can use the free [NPort Administrator](#) utility to bind the IP address.

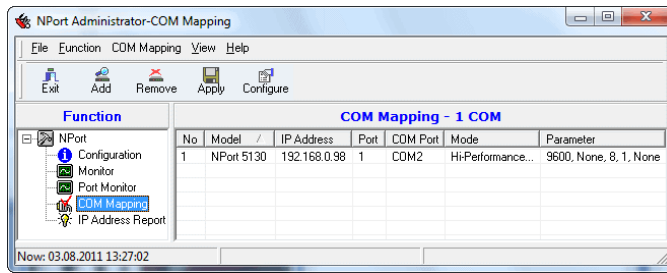
Connection procedure:

- Connect the camera to the converter, and connect the converter to the local network (see the figure).



- Use the **NPort Administrator** utility to find converters on the network. If necessary, you can use this utility to change the device's IP address.

- Bind the converter's IP address to the video server's COM port (the NPort 5130 converter is shown in the example).



3. **Connecting through IP video servers.** An IP video server's rear panel has the RS-485 socket necessary to connect PTZ cameras.



- *Serial port settings*



## Working with the basic interface

- *Start the software and sign into the system* - This section describes the first launch of TRASSIR and how to sign in to the main control panel.
- *Main control panel* - This section describes health metrics, monitor groups, background tasks, how to change users, and how to restart/shutdown the software.
- *Settings window* - A description of the server's main settings window and the basic ways to work with it.
- *Video monitor* - This section contains information about the purpose of the buttons in the video monitor menu.



- *Installation*
- *Settings*
- *Plugins*

## Start the software and sign into the system

The TRASSIR software consists of a server part and a client part: TRASSIR Server and TRASSIR Client. You can sign into the system locally using TRASSIR Server, or remotely using a different server, TRASSIR Client, or WebView.

- Guardant USB-key connected to server and license file are required to run the TRASSIR 4 Server application.
- Running the client application does not require a USB key or license.



Note: when signing in both locally and remotely, the account used must have the necessary access rights.

TRASSIR software can be run in two modes: normal mode and "no restart after fault" mode.

- **As usual** - starting of "Trassir 4 Server/Client" label created under installation in Start menu ( watchdog-vc120.exe file will be started from TRASSIR root folder). In this case dedicated module - *Watchdog* will trace server status.
- **In "no restart on failure" mode** - "Trassir 4 Server/Client shortcut starting (no restart under failure)", created under installation in Start menu (t1server-vc120.exe/t1client-vc120.exe will be started from TRASSIR root folder).

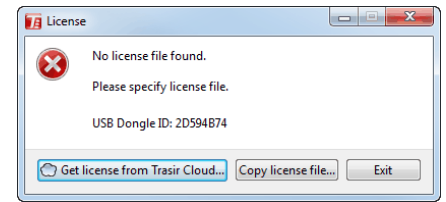


If the program launched successfully, the main control panel icon will be displayed in the top part of the screen and icon availability in the task panel.



- *First launch of the TRASSIR Server software*
- *System login*
- *Main control panel*

## First launch of the TRASSIR Server software

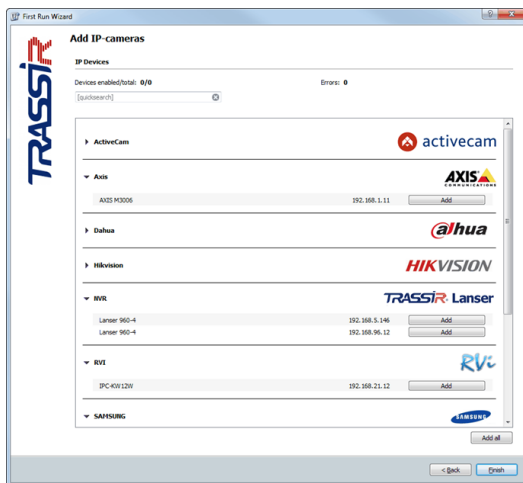


License file selection window will appear at the first run of TRASSIR Server.

- If you have license file, press **Copy license file...** button and specify it.
- To search for the license file in TRASSIR Cloud press **Find license in TRASSIR Cloud...** button and enter user name and ticket. In case earlier license has been stored in the cloud, it will be automatically found and loaded into TRASSIR.

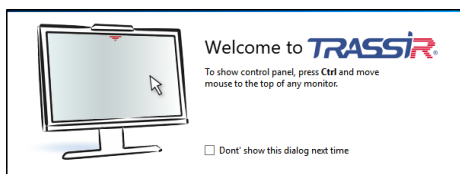
After that TRASSIR Server will run and **First run wizard** will appear:

- configure a connection with TRASSIR Cloud (see [Connecting server to TRASSIR Cloud](#));
- add IP devices, which have been automatically found on the local network, to the system (see [IP devices](#)).
- to add to the system servers which have been automatically found in the local network (see section [Connecting to a new server](#)).



When the wizard is done, click **Finish**.

The welcome window containing the prompt will appear on the screen. In order to skip this window upon further TRASSIR runs, check **Don't show this dialog next time** box.



- [Start the software and sign into the system](#)
- [Main control panel](#)
- [Settings window](#)
- [Video monitor](#)

## Watchdog

The Watchdog module is used to start TRASSIR 4, monitor its state, and restart TRASSIR in the event of critical failures. Watchdog settings are stored in `watchdog-t1server.config` (`watchdog-t1client.config`).

This file contains the following settings:

- `application` - the name of the application. Any value; must not be empty.
- `executable` - the executable file is specified here: for the server this is `t1server-vc120`; for the client it is `t1client-vc120`.
- `keepalive` - Watchdog's main setting. If the Watchdog module does not receive the state of the software for this period of time, then TRASSIR will be forcibly restarted. In order for TRASSIR software to work properly, this setting must be greater than 60 seconds.
- `executable-arguments` - additional settings for internal use.
- `log` - the value of this setting will be used to name a log file in the event that the Watchdog module terminates TRASSIR.

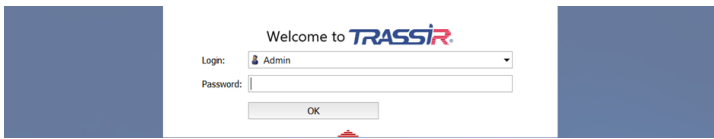



The default values in `watchdog-t1server.config` (`watchdog-t1client.config`) are optimal. Do not change them unless there is a real need.



- *Start the software and sign into the system*

## System login



To log in the system, enter **User name** and **Password**, and in case of successful authorization the *Main control panel window will open*. Otherwise, the sign will appear  which means the authorization failure.



Two users: **Admin** and **Operator** are available in the system by default.  
Administrator password in TRASSIR OS and in TRASSIR installed as Windows service is **12345**.  
Administrator of TRASSIR installed as Windows application does not have password.



Change user passwords for security reasons. You can read detailed information on the work with TRASSIR users in *Users* subsection.

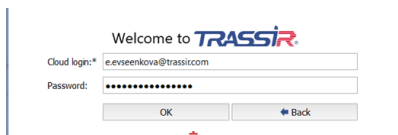
## Log in for TRASSIR Cloud system users

**TRASSIR Cloud** service users can also log in.

To do this:

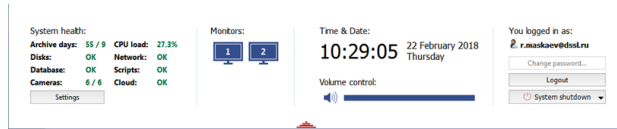
- server needs to be connected with the cloud user account (see section [Connecting server to TRASSIR Cloud](#));
- account user is allowed to access to this server (see [Guidance on TRASSIR Cloud](#)).

Provided all these requirements are satisfied, press **Other user** button to log in, type in the **Cloud user** name and **Password**.



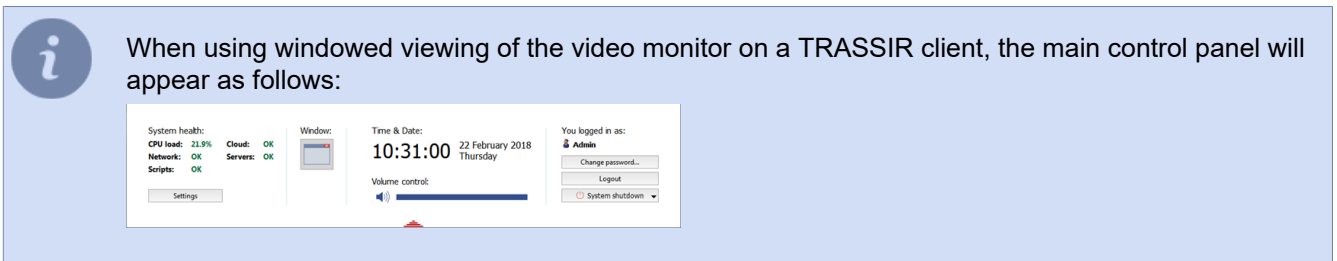
- *Start the software and sign into the system*
- *First launch of the TRASSIR Server software*
- *Main control panel*

## Main control panel

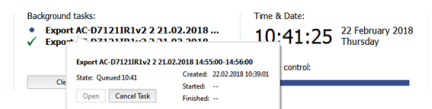


After signing in, the main control panel is grouped as follows:

1. **System Health** - are server operation parameters allowing to immediately identify the errors which are critical for its operation. See detailed information on system health in "Operator's Manual" (???)  
The **Settings** button opens the **TRASSIR settings window**.
2. The **Monitors** group is a button to show/hide the TRASSIR video monitor interface. If several monitors are connected to the computer, there will be several such buttons - each monitor has its own interface.  
By default, the video monitor interface is hidden when TRASSIR is installed. To display a monitor, you must click on its image. Clicking it a second time will hide the video monitor interface. You can read more about working with the monitor interface in the Operator's Guide (???)



3.



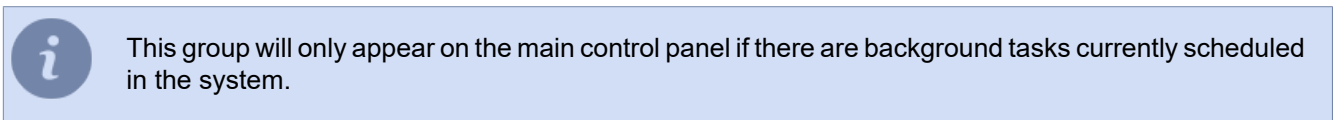
The **Background tasks** group shows a list of tasks whose execution has been postponed. The delayed export of an archive is an example of such a task.

Simply left-click on a task to view its status. A popup window with the information will appear. You can cancel the task in this window by clicking the appropriate button.

The icon next to the task changes depending on its current status:

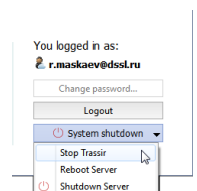
- - indicates a task waiting in the queue to be executed;
- ✓ - indicates a completed task.

The **Clear** button removes all completed tasks from the list.



4. The **Time & Date** - group displays the server's system date and time.  
Use the **Volume control** to adjust overall volume level in TRASSIR.

5.



The **You logged in as**: group displays the username for the person who is currently signed in.

The **Change password...** button allows users to change their own passwords.

The **Logout** button lets the system's current user sign out.

The **System shutdown** button brings up the following dropdown menu:

- **Stop TRASSIR** - shuts down the software.
- **Reboot Server** - restarts the server the operator is using.
- **Shutdown Server** - shuts down the server the operator is using.



If TRASSIR was started in "no restart after fault" mode, then when the **System shutdown** button is clicked, the dropdown menu will not be shown. Instead, TRASSIR will be shut down.



- *Start the software and sign into the system*
- *Settings window*
- *Video monitor*



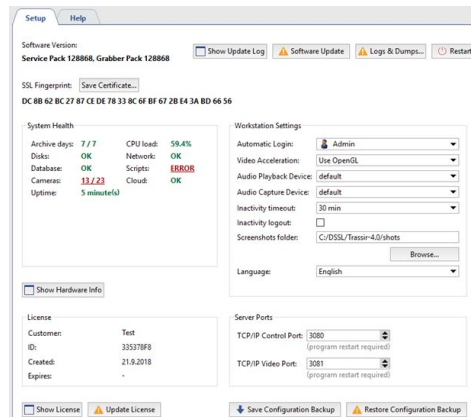
## Settings window

The administrator specifies all the TRASSIR server's settings in the **Settings** window.

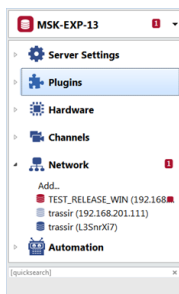
All of the TRASSIR server's settings are represented as an object tree. Moreover, the object tree may include objects from other TRASSIR servers – all you have to do is configure a network connection to them and you can configure them remotely.



Remote server configuration is only possible if the account being used to make the connection has the **necessary rights**. Remember that each TRASSIR server has its own list of users. Therefore, when remotely connecting to a server, use an account that was created on the remote server.



The local server is always located at the top of the list of servers. By default, the **main server settings** tab is displayed when the settings window is opened.

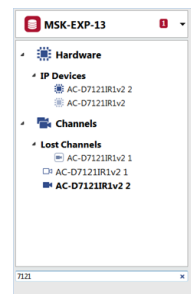


In case certain menu entries have errors in the settings, they will be automatically highlighted.

Total number of error messages is displayed in settings tree nodes.

A server can have a substantial number of objects parameters of which can be set (especially in case connections to the other servers are set from the given server).

Use fast context search field to proceed quickly to the requested objects.

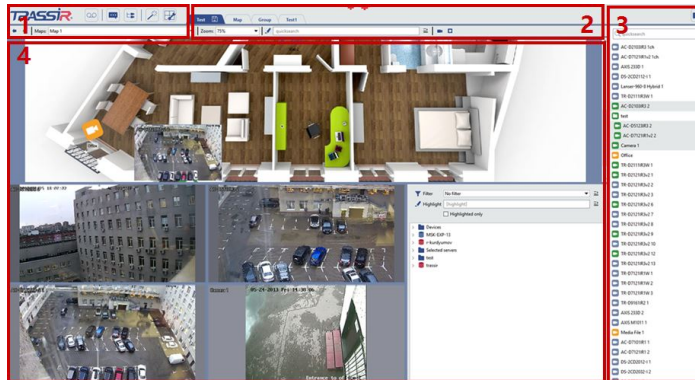


The following sections describe all of the TRASSIR server settings: **Settings** and **Plugins**









- **Start the software and sign into the system**
- **Main control panel**
- **Video monitor**

## Video monitor



The main interface elements are:

1. **Menu** - A set of buttons for controlling the video monitor interface:

-  switches the video monitor to archive viewing mode and back.
-  shows/hides the event log.
-  shows/hides the object tree.
-  additional functions. These functions include switching to a map, managing screenshots, or invoking an arbitrary user function (running a rule or script).
-  template editor.
-  shows/hides the list of channels.



Find detailed menu description in the corresponding section of the "Operator's Manual".

2. **Template menu** – The set of saved templates.

3. **Channel list** – The area used to monitor the state of cameras (and groups of cameras) and, if desired, to display the video from a particular camera on the entire screen.

4. **Main output area** – The area used directly for video surveillance. It is created using the template editor.

You can read more about working with and configuring the video monitor in the Operator's Guide (???)



- *Start the software and sign into the system*
- *Main control panel*
- *Settings window*

# Settings

Once a server has been installed, TRASSIR lets you get to work right away. In other words, the configuration made during [server installation](#) and [first launch](#) are sufficient for a TRASSIR server to operate.

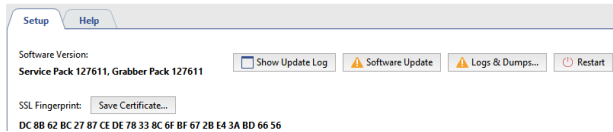
However, additional server settings must be adjusted to expand the TRASSIR server's basic functionality:

- [connect the server to a database](#) to save all server events;
- [change archive settings](#);
- [connect to TRASSIR Cloud](#);
- [create users and configure their rights](#);
- [connect IP devices to the server](#) and [change their channel settings](#);
- [connect to other TRASSIR servers](#);
- [create rules and scripts](#) to automate the server.

Moreover, with the [additional modules](#) you can significantly expand TRASSIR's basic functionality.

## Local server settings

The following information is displayed in the server's main settings window:



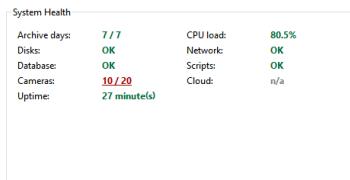
- **Software version** - the current version of TRASSIR. It consists of the Service Pack number (the version of the main modules) and the Grabber Pack number (the version of the IP cameras' drivers and compression cards).

Buttons:



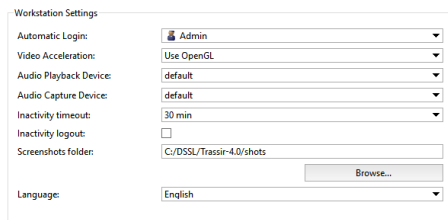
- **Update log** displays the log of installed Service Pack and Grabber Pack updates.
- **Software update** is intended to update TRASSIR modules and IP camera drivers without reinstalling software. On update's completion, TRASSIR will restart automatically. See detailed description of the function in the [Software Update](#).
- **Logs and dumps...** opens the window of TRASSIR system files selection which should be transmitted to the technical support. See the detailed description of the function in section [Logs and dumps](#).
- **Restart** is intended for TRASSIR software operational reloading (**Software**) or the whole server (**Hardware**) from the administrator's interface.

**SSL Fingerprint.** Each server has a unique identifier. This identifier serves to verify the server's authenticity when connecting to it over the network. You can use the **Save Certificate...** button to save the hash to a file, for example, a flash drive.



**System health** - Server performance measurements for rapid detection of critical server errors. The health metrics are duplicated, being shown in the [Main control panel](#) as well.

Workstation settings:



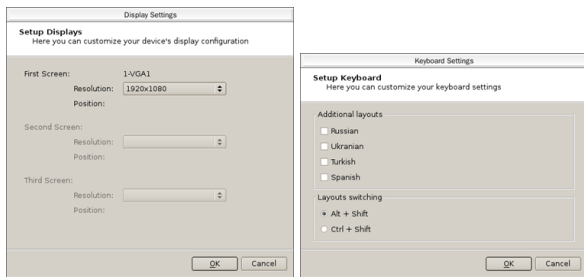
- **Automatic Login** - indicates the username for the account that will be used to sign in to the server when TRASSIR is launched. The default value is "None", e.g. a username and password are required to sign into the server.
- **Video Acceleration** - "OpenGL" or "DirectDraw". Specify the value that is best for the video card being used.
- **Audio Playback Device** - The device that plays back the audio recorded by the microphone connected to the camera.
- **Audio Capture Device** - The device that transmits audio from the video server to the speaker connected to the camera.

- **Inactivity timeout** - is the time period in the course of which an operator did not use TRASSIR interface. Check **Inactivity logout** box. Upon selected expiration period a notification of the current session completion in 60 second will occur on the screen and the countdown will start.



In case **Inactivity logout** box has not been checked, notification will not appear. Operator's inactivity can be traced through audit (see section [Audit](#)).

- **Screenshots folder** - the folder in which all screenshots made with "S" button will be saved. The folder can be located manually or you can locate it with the **Browse** button.
- **Language** is an interface language. When selecting the **default value**, the interface language will change to the one selected during installation.
- **Hardware acceleration** allows to use system resources to maximum extent in case that it is supported by the device.
- **Display settings...** and **Keyboard settings...** buttons open the corresponding settings windows.



**Workstation Settings**

Automatic Login:

Audio Playback Device:

Audio Capture Device:

Inactivity timeout:

Inactivity logout: ☐

Language:

Hardware acceleration: ☐

**Hardware acceleration** box and the **Screen settings...** and the **Keyboard settings...** buttons are displayed in case local or remote connection to the server from TRASSIR OS.

**Server Ports**

TCP/IP Control Port:  (program restart required)

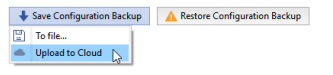
TCP/IP Video Port:  (program restart required)

Server ports:

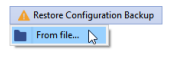
- **TCP/IP Control Port** - The server control port.
- **TCP/IP Video Port** - The video broadcast port.

Buttons:

- **Show Hardware Info** - Displays the OS version and the server's hardware configuration.
- **Save Configuration Backup** - You can make a backup copy of your system's configuration at any time and save it locally or in TRASSIR Cloud. If the backup is saved locally, a text file containing the settings is created named `_tlserver.settings`, which is located in the installation folder by default.



- **Restore Configuration Backup** - Restore a configuration from a previously created backup copy that was saved locally or in TRASSIR Cloud.



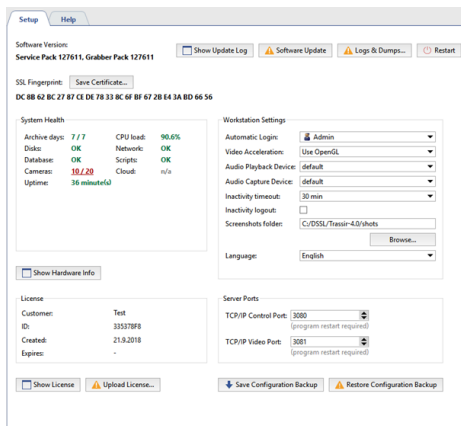
Learn more about saving backup copies to TRASSIR Cloud in [Connecting server to TRASSIR Cloud](#).

- **Show License** - Displays the license file. You can use this button to view the system's permissions and restrictions.
- **Upload License...** - You can specify a new license file for the server directly from the settings window. Updating license file may be necessary, for example, when expanding your system.



- [Archive setup on the server](#)
- [Database connection settings](#)
- [Configuring device settings](#)
- [Determining access rights](#)
- [Connecting to a new server](#)

## Remote server settings



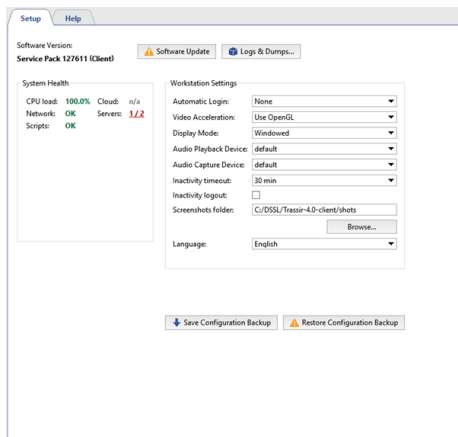
The main settings window for a remote server displays the same information as that for [local server settings](#).



Changing the language in connected server settings you change the interface language of it.

The **Connected through [server name]([server IP address])** string shows the server connected to the local server or client. Learn more about ways to connect remote servers in [Connecting to a new server](#).

## Client settings



The following information is displayed in the client's main settings window:

- **Software version** - is the current version of TRASSIR containing version number of the basic modules (Service Pack).

Buttons:

- **Software update** is intended to update TRASSIR modules and IP camera drivers without software reinstalling. TRASSIR will restart automatically after the update. See detailed description of the function in section [Software Update](#).
- **Logs and dumps...** opens the window of TRASSIR system files selection which should be transmitted to the technical support. See detailed description of the function in section [Logs and dumps](#).

**System health** - Server performance measurements for rapid detection of critical server errors. The health metrics are duplicated, being shown in the [Main control panel](#) as well.

Workstation settings:

- **Automatic Login** - indicates the username for the account that will be used to sign in to the server when TRASSIR is launched. The default value is "None", e.g. a username and password are required to sign into the server.
- **Video Acceleration** - "OpenGL" or "DirectDraw". Specify the value that is best for the video card being used.
- **Display Mode** - Select whether TRASSIR's main window will be displayed as a separate window or in fullscreen mode.
- **Audio Playback Device** - The device that plays back the audio recorded by the microphone connected to the camera.
- **Audio Capture Device** - The device that transmits audio from the video server to the speaker connected to the camera.
- **Inactivity timeout** is the time period in the course of which operator did not use TRASSIR interface. Check **Log off at inactivity** box. On the selected time period expiration a notification will appear on the screen of current session expiration in 60 seconds and the countdown will start.



In case **Inactivity logout** box is not checked, notification does not appear. Operator's inactivity can be traced with audit (see section [Audit](#)).

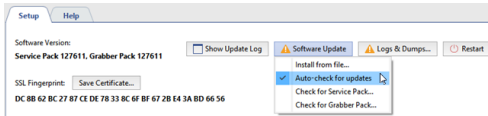
- **Screenshots folder** is the folder where screenshots made with "S" button will be saved. Folder location can be specified manually or located using the **Browse** button.
- **Language** is the interface language. While selecting value by default the interface language will change for the one selected during the installation.



## Software Update



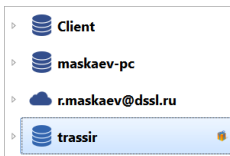
TRASSIR can be updated both locally and remotely, *by connecting* with client.



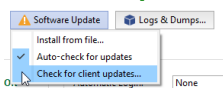
The **Software Update** feature allows you to update the server software and IP device drivers. Select one of the items to check for the updates:

- **Search for new ServicePack...**
- **Search for new GrabberPack...**

In case the required update is available in TRASSIR Cloud, you'll see the list of changes and the offer to download it.



Select **Auto-search for updates** to ensure automatic search for updates in TRASSIR Cloud. In case of update finding **Software update** button will start to flash and icon will appear in the settings tree.



Press **Software update** button, and you'll see the suggested update instead of **Search for new ServicePack...** and **Search for new GrabberPack...** menu items. Select the corresponding item to view list of changes and activate update function.

You can also download an update file from [our website](#) and update TRASSIR manually. In this case select **Install from file...** and locate the update file.



Depending on the operating system and the installation method, TRASSIR will restart automatically:

- **TRASSIR-server for Windows (installed as a standalone application)** or **TRASSIR-client** - only TRASSIR application will restart;
- **TRASSIR for Windows (installed as a service)** or **TRASSIR OS** - Windows or TRASSIR OS will restart.



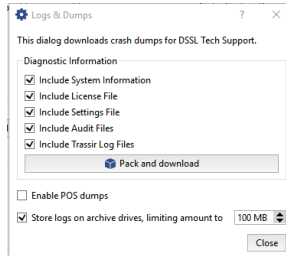
- [Local server settings](#)
- [Remote server settings](#)
- [Client settings](#)

## Logs and dumps

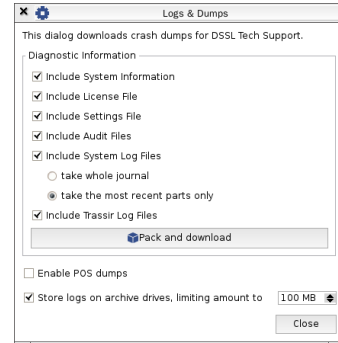
All TRASSIR activities are recorded into the log. In case of emergency software completion, dump files containing information on TRASSIR failure will be created on the drive. This function will collect and prepare all the required information based on which technical support stuff will find the cause of failure and give recommendations how to eliminate them.

The list of items to be selected depends on OS:

### TRASSIR for Windows



### TRASSIR OS



Select the relevant items by and press **Pack and download**. Send the output archive to technical support.



- [Local server settings](#)
- [Remote server settings](#)
- [Client settings](#)

## TRASSIR Cloud

**TRASSIR Cloud** is a professional cloud service to manage videosurveillance through the Internet. Its major functions and advantages are:

- **Simple settings** — connect you equipment to the cloud service without direct IP addresses and view without worrying about the settings.
- **Status monitoring** — get complete information of the status of connected device.
- **Situation monitoring** — get notifications from all the devices (by e-mail or SMS) to keep track of the events.
- **History** — view the history of notifications and equipment statuses in the personal account or through mobile app.
- **Storage and review** — the data from cameras is stored in the cloud and is available for review from any device.
- **Devices on the map** — indicate coordinates of the equipment layout and view them on the map.

In addition **TRASSIR Cloud** is the network-attached storage of the license files and TRASSIR 4 server settings which in case their loss can be recovered in the cloud. In its turn, it will allow to return server in operating status in few minutes.



In case you still have no account in TRASSIR Cloud, use the link [cloud.trassir.com](https://cloud.trassir.com) and create it. See functions and capabilities of the cloud service in details in [Manual on TRASSIR Cloud](#).

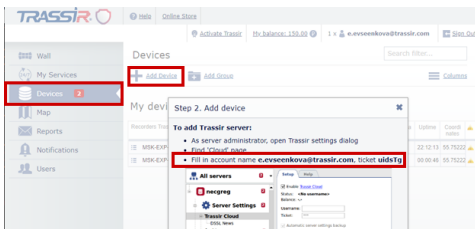


- [Connecting server to TRASSIR Cloud](#)
- [Client connection to TRASSIR Cloud](#)

## Connecting server to TRASSIR Cloud



If you have not account in TRASSIR Cloud, please go to [cloud.trassir.com](http://cloud.trassir.com) and create it. Read more about the features and capabilities of a cloud service, see the [Guideline for TRASSIR Cloud](#).



Before connecting to the TRASSIR Cloud service make sure that **Activate TRASSIR cloud** box is checked. Type in **User name** and **Ticket**. User name is an e-mail used for authorization in the cloud and the ticket can be received in the cloud's personal account.

If TRASSIR Cloud will work wrong, the errors will be displayed in the **Status**. In the **Balance** displays amount of funds, which is on the balance of the cloud user, logged on the server.

Each server which connected to the cloud, keeps a backup of your settings. Set the flag **Automatic server settings backup** and TRASSIR server will be saved configuration settings file (`_tlserver.settings`) and the license file (`Trassir License.txt`) in the cloud. When the number of backups in the cloud will reach 10, the new will replace the old ones.



At the first connecting server to the cloud, the first five backups will be saved every 2 hours, and the next - once per 30 days. If needed, you can update the latest backup manually (see section [Local server settings](#)).

Set the **Allow Cloud connection** flag to use **CloudConnect** to connect to this server.

In addition, TRASSIR Cloud is designed to store the archive. Set the flag **Allow archive synchronization to Cloud** to allow synchronization the cloud archive and archive devices, which connected to the server.



To synchronize must be enabled the corresponding service in the TRASSIR Cloud. For details, see [Guideline for TRASSIR Cloud](#).

You need bind TRASSIR cloud server with an account to access to the cloud channels and users. For this, set the flag **Import users and channels from Cloud**, and select the method to connect to the cloud:

- **Use Cloud Login** - in this case, you need to sign in to TRASSIR server with cloud user that the server is added to the list of available devices. In addition, you are getting access to all cloud devices of this user.
- **Use predefined cloud user** - enter the name and password of the cloud account and you are getting access to all cloud devices of this user.

Check **Show cloud channels** box to display cloud camera channels in the list of connected devices. Cloud cameras operation depends on the tariff of their connection to TRASSIR Cloud. See details on restrictions in the section [Cloud cameras in TRASSIR](#).



- *Start the software and sign into the system*
- *Client connection to TRASSIR Cloud*

## Client connection to TRASSIR Cloud



In case you still do not have personal account in TRASSIR Cloud, follow the link [cloud.trassir.com](http://cloud.trassir.com) and create it.

See details on cloud service functions and capabilities in the [Manual in TRASSIR Cloud](#).

Before connecting to TRASSIR Cloud service make sure that **Activate TRASSIR Cloud** box is checked. Select one of the options to access cloud devices:

- **Access to any cloud account devices**

The screenshot shows the 'Setup' window with the 'Enable TRASSIR Cloud' checkbox checked. The status is 'OK' and the balance is '150.00'. The 'Username' field is empty, and the 'Ticket' field is also empty. Below these fields, there are several checkboxes: 'Automatic server settings backup', 'Allow archive synchronization to Cloud', 'Allow Cloud Connect to this server', and 'Allow the transmission of anonymous usage statistics'. The 'Import users and channels from Cloud' checkbox is checked. Under this, the 'Use Cloud Login' radio button is selected. The 'Use predefined cloud user' radio button is unselected. The 'Username' and 'Password' fields are empty. The 'Show cloud channels' checkbox is checked. A note on the right states: 'Local users: Admin, Operator and all Cloud users explicitly given access to any resource of this server can login.'

Select **Cloud login** and leave the field **Bind to cloud user** blank.

Now any cloud user can authorize and get access to the cloud devices in the personal account, including the shared devices.



Please note that in case **Bind to cloud user** field is blank, user will receive the rights of TRASSIR client's administrator after the authorization.

- **Access to a single cloud account devices**

The screenshot shows the 'Setup' window with the 'Enable TRASSIR Cloud' checkbox checked. The status is 'OK' and the balance is '150.00'. The 'Username' field is filled with 'e.xosenkova@trassir.com', and the 'Ticket' field is empty. Below these fields, there are several checkboxes: 'Automatic server settings backup', 'Allow archive synchronization to Cloud', 'Allow Cloud Connect to this server', and 'Allow the transmission of anonymous usage statistics'. The 'Import users and channels from Cloud' checkbox is checked. Under this, the 'Use Cloud Login' radio button is selected. The 'Use predefined cloud user' radio button is unselected. The 'Username' and 'Password' fields are empty. The 'Show cloud channels' checkbox is checked. A note on the right states: 'Local users: Admin, Operator and all Cloud users explicitly given access to any resource of this server can login.'

Select **Use Cloud Login** and enter your cloud account name into **Bind to cloud user** field.

In this case local users and that cloud account users will be able to authorize the client.

After the authorization, cloud users will see only the devices added directly to the cloud personal account and access to which is allowed in user rights setting.



See cloud user rights settings in details in the TRASSIR Cloud Manual (section ???). Local user rights settings is described in [Determining access rights](#).

- **Access to cloud devices under local user**

The screenshot shows the 'Setup' window with the 'Enable TRASSIR Cloud' checkbox checked. The status is 'OK' and the balance is '150.00'. The 'Username' field is filled with 'e.xosenkova@trassir.com', and the 'Ticket' field is empty. Below these fields, there are several checkboxes: 'Automatic server settings backup', 'Allow archive synchronization to Cloud', 'Allow Cloud Connect to this server', and 'Allow the transmission of anonymous usage statistics'. The 'Import users and channels from Cloud' checkbox is checked. Under this, the 'Use predefined cloud user' radio button is selected. The 'Use Cloud Login' radio button is unselected. The 'Username' and 'Password' fields are empty. The 'Show cloud channels' checkbox is checked. A note on the right states: 'Local users only Admin, Operator can login.'

Select **Another user** and type in your cloud user name and password.

Now only local users can authorize on the client, therewith they get access to the cloud devices of the logged in user.

Check **Show cloud channels** box to display cloud camera channels in the list of connected devices. Cloud cameras operation depends on the tariff of their connection to TRASSIR Cloud. See details on restrictions in the section [Cloud cameras in TRASSIR](#).



- *Start the software and sign into the system*
- *Connecting server to TRASSIR Cloud*

## Cloud cameras in TRASSIR

Cloud cameras in TRASSIR operate with certain restrictions which depend on the tariff.

Feature	Basic	SD standard	HD standard	HD+ standard
Live video watch	5 minutes	10 minutes	20 minutes	40 minutes
Archive review	1 minute	10 minutes	20 minutes	40 minutes
Archive export Maximum fragment length	10 minutes	10 minutes	1 hour	2 hours

See detailed information on camera connection to the cloud and tariff selection in [TRASSIR Cloud Manual](#).



- [Connecting server to TRASSIR Cloud](#)
- [Start the software and sign into the system](#)



## Archive

An archive is a repository of recorded video data that can be constructed on one or more disks. The number and capacity of disks required to set up an archive depends on the archive depth that must be provided.

As an archive is recorded, the data is divided equally across all available disks. Once the disks are full, the data is overwritten automatically. The archive is deleted from the end, e.g. the oldest recordings are deleted first.

There are a number of particulars of working with a TRASSIR archive that must be taken into account when building a video surveillance system, namely:

- TRASSIR can work without an archive. In this case, video can only be viewed in real time; it is not saved to disk.
- TRASSIR cannot use a system partition for archive recording.
- Hard disks must have a capacity of at least 10 GB for archive recording. If the system has smaller-capacity disks, they cannot be used for archive recording. Such disks will be labeled as "Not suitable" in the **Statistics** field. Disks that already contain archive data are an exception. These disks will be available for reading only.

Writing always takes precedence when accessing an archive, i.e. TRASSIR will always try to use the available resources to write data. Moreover, the following rules apply:

- If there are simultaneous attempts to read and write to an archive and the system lacks the required resources, then the system will only write data (reading is stopped).
- If insufficient system resources are subsequently observed, the system will use 500 MB of memory as a video write buffer. If the buffer is consumed and there are still insufficient resources, then TRASSIR will issue an error message and part of the archive data will not be recorded.



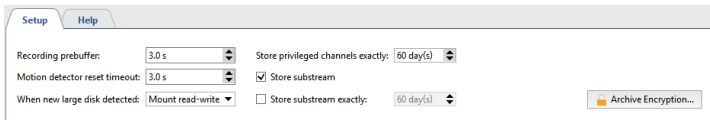
- [\*Archive setup on the server\*](#)
- [\*Archive setup on the client\*](#)
- [\*Selecting the number of disks for an archive\*](#)
- [\*Lost channels\*](#)

## Archive setup on the server



This section presents information about archive settings on TRASSIR server. We also recommend that you review the following sections: [Archive](#) and [Selecting the number of disks for an archive](#).

In the window **Settings** -> **Archive** tab, you can determine which disks and what mode will be used for the archive. At the top of the window is archive general settings. Below is the list of the drives used by the system (including networks drives, external hard drives, flash-drives, etc.), their statistics and settings.



- **Recording Prebuffer** - The size of the video buffer in seconds (from 0 to 10 seconds). TRASSIR will always store a buffer of the indicated size in memory. When an event occurs, the buffer is appended to the associated video. This lets the operator later view the archived video not from the moment the event was recorded, i.e. a door opens, but rather several seconds beforehand, making it possible to see who approached the door and how.
- **Motion detector timeout** - The amount of time for which motion will be considered to continue after a detector has indicated that motion within the frame has ceased. This parameter makes it possible to avoid cutting off a recording immediately after motion has ceased and continue to record several seconds at the end (from 0 to 10 seconds).
- **When New Large Disk Detected** - This parameter determines how TRASSIR will respond to a new disk being detected (for example, when a new network drive or a flash drive is connected). There are three possible values:
  1. **Ignore** - The disk will be shown in the list, but it will be otherwise ignored by the system; the disk can only be included manually.
  2. **Mount as read-only** - Nothing will be recorded to the disk, but if it contains TRASSIR archive files, they will be available in TRASSIR as *lost channels*.
  3. **Mount as read-write** - When a new disk appears in the system, TRASSIR will automatically use it for archive recording.

TRASSIR supports recording two video streams coming from devices: the main stream and the additional stream (substream). Because the auxiliary stream is generally several times smaller than the primary stream, recording it substantially increases the archive depth without changing the required disk space. Additionally, using the secondary stream significantly lowers network throughput requirements while viewing archived data from several channels simultaneously over a client-server connection.

If necessary, you can *mark* one or more channels as privileged and assign them an arbitrary archive depth in the main (primary) stream.

- **Store Privileged Channels Exactly** - Supports assigning a desired archive depth to specific channels.
- **Store Substream** - Enables recording of the auxiliary stream.
- **Save substream Exactly** - Supports assigning a desired archive depth to substreams. If no depth is assigned, then the substream will be erased together with the primary stream.



Be careful when setting up archive depth values. It is possible that, due to an attempt to maintain the desired archive depth of a substream and/or privileged channels, there will not be space under the usual archive. If during the overwriting process the archive depth of the primary stream is less than 24 hours, then the system will issue a warning about incorrect settings for archive recording.

If the flag **Store substream exactly** is not enabled, the sub-stream archive depth is equal to the greatest depth of the main or privileged stream. The sub-stream archive will contain video from the channels of the devices on which the sub-stream recording is enabled (see [Configuring device settings](#)).

To prevent unauthorized access to an archive, TRASSIR supports [encryption of video recordings](#). To configure encryption, click **Archive encryption...**

Disk	Enable	Read-only	Capacity	Current Stats
D:\	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Read-only		930.80 GB	1.83 MB/s, 0 errors

New mount point:

You can set specific settings for each drive:

- **Enable** - Enables or disables use of the disk in the system.
- **Read-only** - Enables or disables use of the disk for reading.
- The **Capacity** column displays the full capacity of the disk (partition).
- The **Current Stats** column displays the archive's current write speed and the number of errors. Sometimes there may be access errors when attempting to read from or write to a disk. For example, if the connection to a network drive is lost, if a disk cannot handle writing an excessively large stream, or if hardware problems are detected on a disk.



The "HDD Kicker" script is recommended for local disks. After several errors occur, the script can disable the problematic disk to avoid data loss.



If a disk's capacity is less than 10 GB, then it will be labeled as "Not suitable" in the list. You cannot use such a disk to record an archive. But if it contains TRASSIR archive files, then it will be displayed in the list and marked "Read-only".

**New mount point** - Adds any folder to the set of locations used for archive recording. Adding a new mount point may be appropriate if, for example, you need to view archive files written to another server that lacks a network connection. You can indicate the folder using the **Browse** button, or enter the path manually and press **Add**. No additional steps with the archive are required. Archive data added using a new mount point will be available in TRASSIR as [lost channels](#).

Archive statistics	Merge statistics
Main Stream: 848.17 GB / 8.0 Days = 106.38 GB/Day	Main Stream: 0.00 GB / 0.0 Days = ~ GB/Day
Privileged: 0.00 GB / 0.0 Days = ~ GB/Day	Substream: 0.00 GB / 0.0 Days = ~ GB/Day
Substream: 66.48 GB / 8.0 Days = 8.30 GB/Day	Hardware: 0.00 GB / 0.0 Days = ~ GB/Day

The archive's general statistics are displayed in the bottom part of the window. You can view the depth of days and the total volume of data separately for the primary and auxiliary streams. You can also view the statistics for privileged channels. A calculation of the disk space necessary to store one day of archive recordings is also presented here.

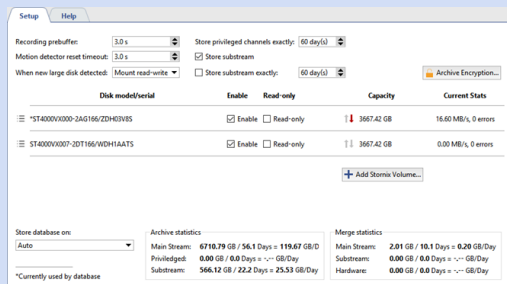


A version 4.0 archive supports a gradual upgrade of an archive from TRASSIR 3.1. The entire archive from old versions will be available as *lost channels* and will be erased as the new archive is written.



**TRASSIR OS** has some differences in the archive settings menu. That is:

- There is no **New mount point**, i.e. you cannot connect an arbitrary folder to the archive;
- you can run **Format** command from the context menu which will delete old records of archive or prepare a new drive for the archive record;
- There is a **Store database on** setting, which lets you select the disk to store the TRASSIR database on. The selected disk in the list of archive disks will be marked with an asterisk (\*).



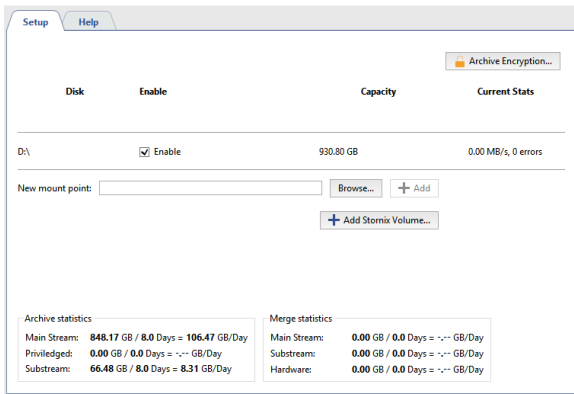
- [Archive](#)
- [Encrypting an archive](#)
- [Selecting the number of disks for an archive](#)
- [NAS Setup](#)
- [Recording network channels](#)
- [Lost channels](#)

## Archive setup on the client



This section contains information on archive setup on the TRASSIR client. We also advise you to get acquainted with the following sections: [Archive](#) and [Selecting the number of disks for an archive](#).

In the **Settings** -> **Archive** tab, you can determine which drives and what mode will be used for the archive.



You can set individual settings for each drive:

- **Enable** flag - authorization or prohibition to use the drive in the system.
- The capacity of the drive (partition) is given in **Capacity** column.
- **Current Stats** column displays current archive recording speed and the number of errors. In some cases an access error can occur while trying to access the drive for recording/reading. Such cases may include for example lost communication with network drive, in case the drive fails to cope with excessive data or it has hardware issues.



It is recommended to use "HDD Kicker" script for local drives. This script can disable problematic drive to prevent data loss.



In case the disk space is less than 10 Gb, it will be marked with "Not appropriate" line in the list. In case it contains TRASSIR archive files, check **Enable** to view them.

**New mount point** - Adds any folder to the set the location for the archive record. Adding a new mount point may be necessary if you need to view archive files written to another server that lacks a network connection. You can locate the folder using the **Browse** button, or enter the path manually and press **Add**. No additional steps with the archive are required. Archive data added using a new mount point will be available in TRASSIR in the list of [lost channels](#).

Archive statistics	Merge statistics
Main Stream: 848.17 GB / 8.0 Days = 106.38 GB/Day	Main Stream: 0.00 GB / 0.0 Days = ~ GB/Day
Privileged: 0.00 GB / 0.0 Days = ~ GB/Day	Substream: 0.00 GB / 0.0 Days = ~ GB/Day
Substream: 66.48 GB / 8.0 Days = 8.30 GB/Day	Hardware: 0.00 GB / 0.0 Days = ~ GB/Day

To prevent unauthorized access to archive TRASSIR allows to [encrypt stored video data](#). Press **Archive encryption...** to set up the encryption.

General archive stats is displayed at the bottom of the window. You can see the depth in days and total scope of data for mainstream and substream individually as well as privileged channels stats. Here you can also see how much space is required to store one day of the archive records.



Archive of 4.0 supports gradual archive upgrade from TRASSIR 3.1. The archive of the older versions will be available as *lost channels*, and will be deleted as and when new one record will take place.

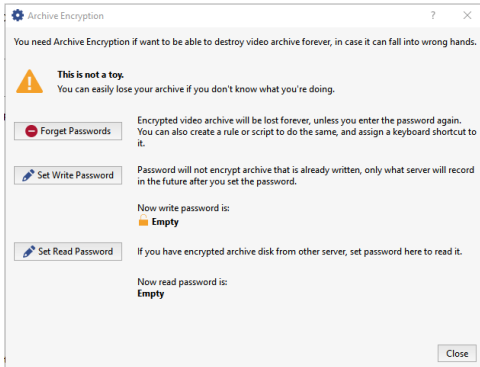


- *Archive setup on the server*
- *Selecting the number of disks for an archive*
- *Lost channels*

## Encrypting an archive

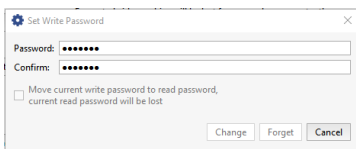


Improper use of the archive encryption feature may result in the permanent loss of an archive. We recommend that you contact our technical support before using this TRASSIR feature.



By default, TRASSIR does not use archive encryption. In other words, an archive stored on one server may be freely transferred and viewed on a different server.

To enable archive encryption, click **Set Write Password**.

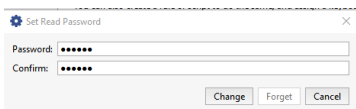


The portion of the archive saved before encryption was enabled will be stored in unencrypted form. The entire portion of the archive recorded after the password is set will be encrypted. Moreover, archive encryption in no way affects the current operation of the server, i.e. all archive operations will be available just as before encryption was enabled. If an encrypted archive is transferred to a different server, all archive operations for that archive, including viewing, exporting, etc., will be unavailable. For example, if a hard disk with an archive is stolen, the thief will not be able to view it without the archive's encryption password.



You will also have access to all archive operations when connecting over a network to a server with archive encryption enabled.

To access a previously encrypted archive, click **Set Read Password**.



In other words, this password will be used only to decrypt the archive that was used to encrypt it.



If you previously enabled archive encryption and want to change the password, you can set the **Move current write password to read password** checkbox. In this case, the archive encrypted with the old password will become unavailable. To access it, you must enter the prior read password.

Use the **Forget** button if you need to disable archive encryption. If you do this, the entire encrypted archive will become unavailable and the new archive will be saved in unencrypted form. To access a previously saved encrypted archive, enter the read password or re-enable archive encryption using the same password.



- *Archive setup on the server*
- *Archive*
- *Recording network channels*
- *Lost channels*
- *NAS Setup*



## Creating and setting up RAID for archive record



The following settings description is aimed for use on **Ultrastation** servers.



To create and set up RAID on **UltraStation** servers a **MegaRAID** utility is used, which is embedded into TRASSIR OS.

You can download the utility from [www.broadcom.com](http://www.broadcom.com) and run on any PC, if necessary.

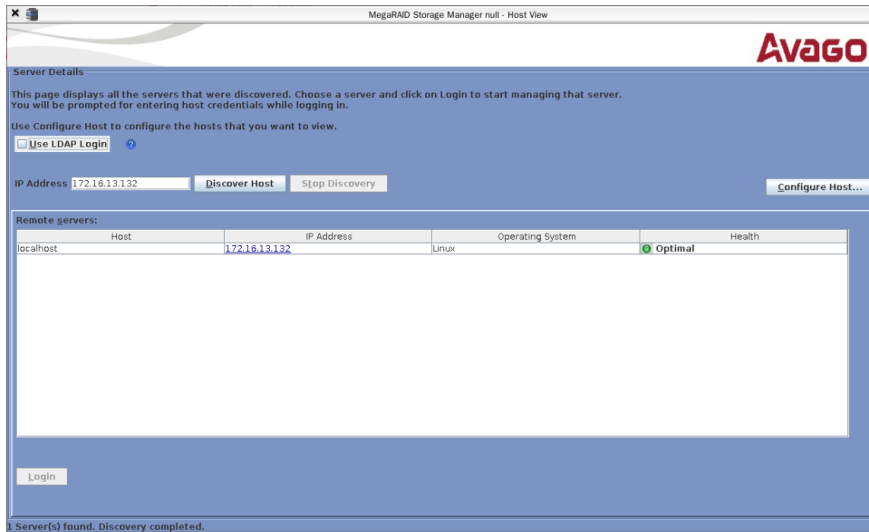
To start the utility:

- **On Windows:** run the previously installed **MegaRAID Storage Manager** app.
- **On TRASSIR OS:** press the **LSI MegaRAID Manager** button on **Server settings** -> **Archive**.

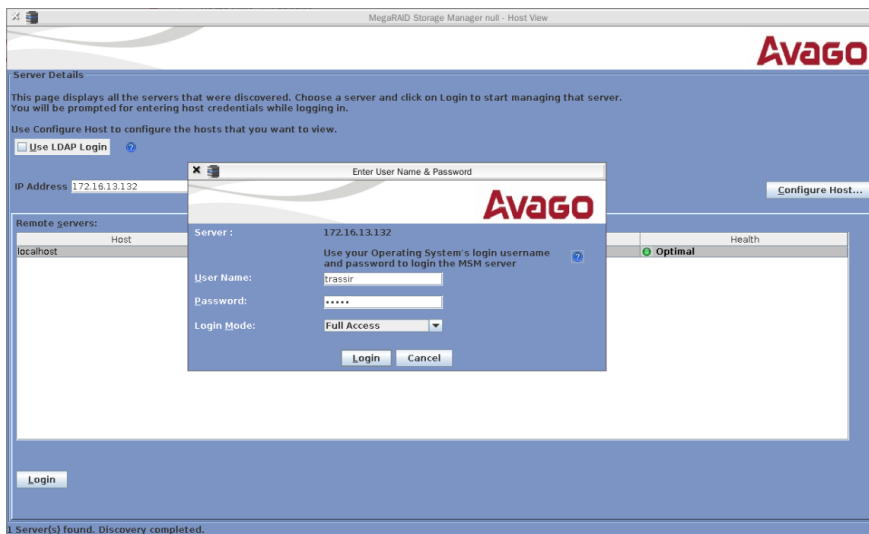


## RAID Creation

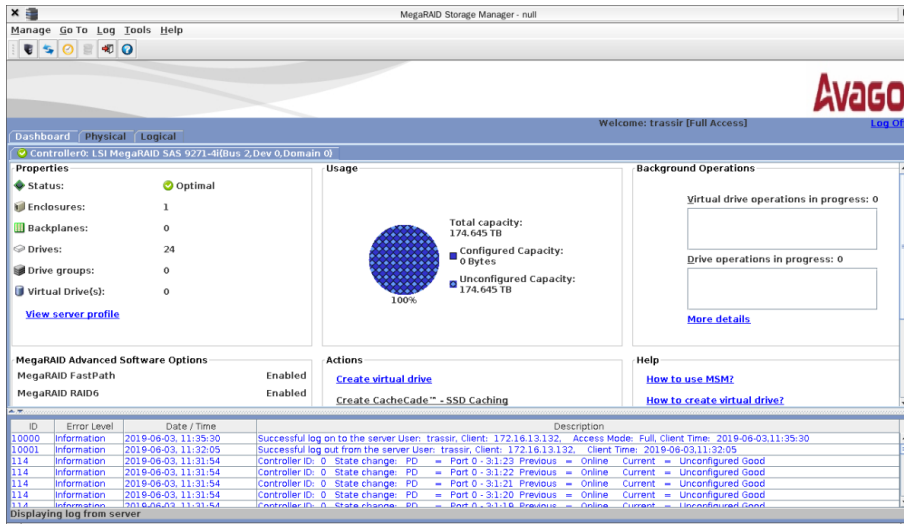
1. Enter server IP address into **IP Address** field and press **Discover Host** button.  
The found server will be displayed in the **Remote servers** list.



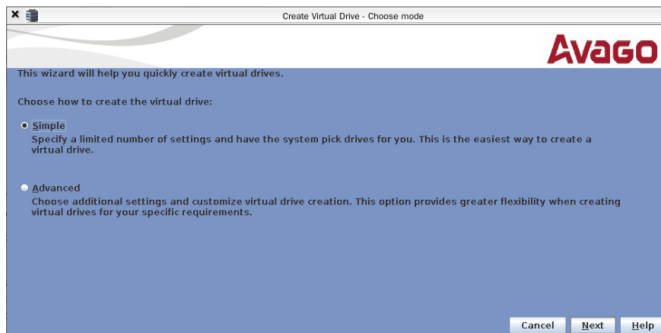
2. Select the server from the list to connect and press **Login**. In the opened window:
  - in the **User Name** field enter **trassir**;
  - in the **Password** field enter the **Administrator** user password (12345 by default);
  - in the **Login Method** field select the **Full Access** connection mode.



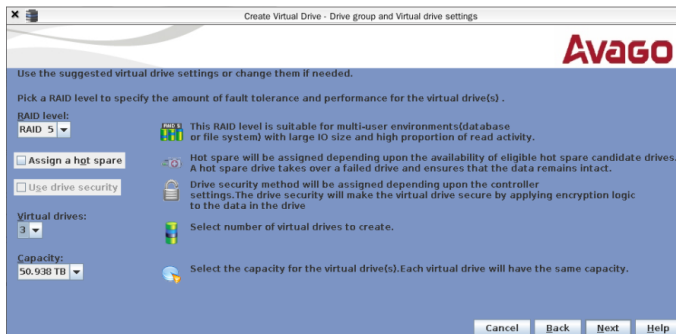
3. After the connection establishment click the **Create virtual drive** link on the **Dashboard** tab.



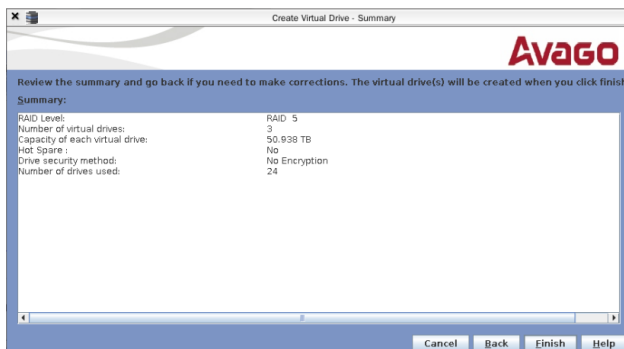
4. Select **Simple** and press **Next** to continue.



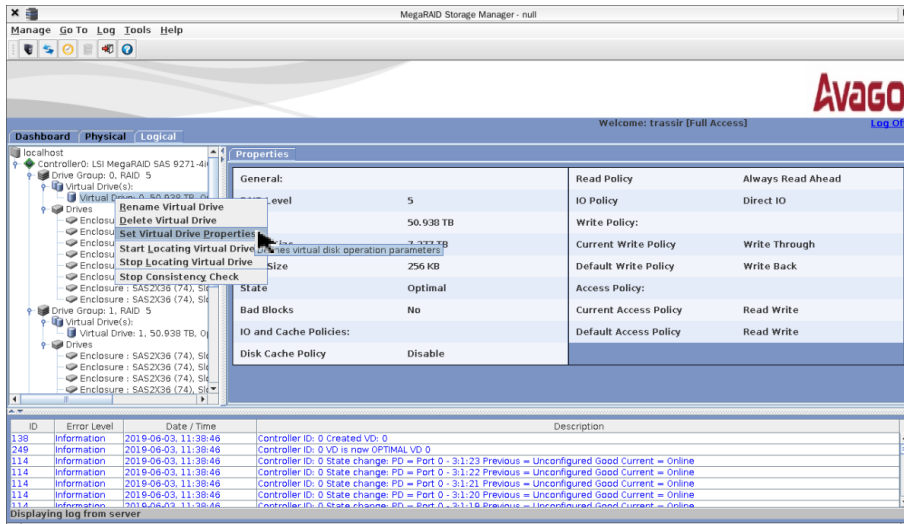
5. After that in the **RAID level** field select the RAID level (RAID 5 by default). In the **Virtual drivers** field select the amount of the virtual drives. Press **Next** to continue.



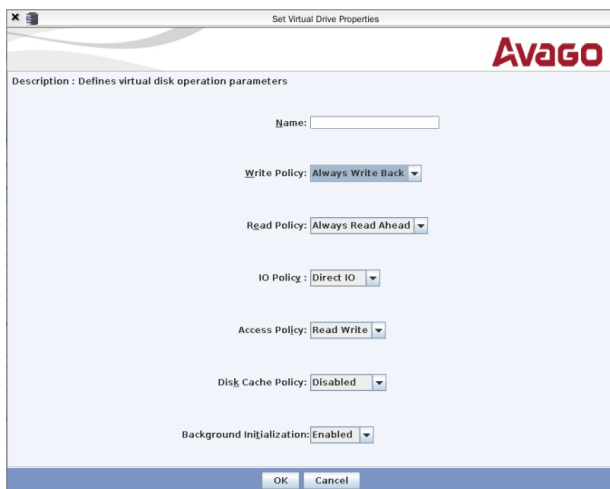
6. Press **Finish** to complete.



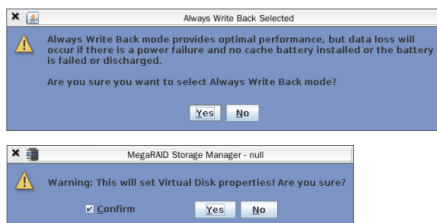
7. Open the **Logical** tab and then with the right click on the virtual drive select the **Set Virtual Drive Properties**



8. In the opened window in the **Write Policy** field select **Always Write Back**. Leave the other settings unchanged. Press **OK** to save the settings.

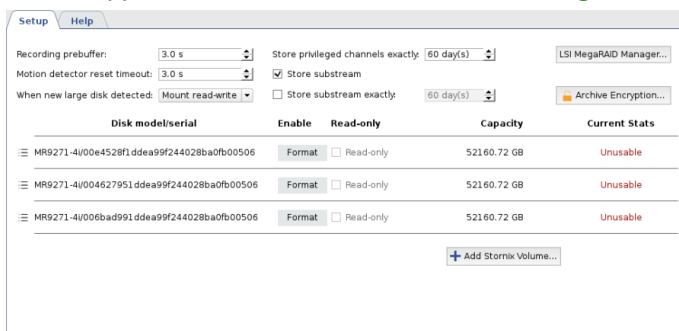


After that, in the notifications displayed, press **Yes**, then check the **Confirm** mark and press **Yes** once more.



Repeat the above described procedure for all array virtual drives.

9. To complete the RAID creation, close the utility. Meanwhile, the exact amount of virtual drives, created in RAID, should appear in TRASSIR on the **Server settings** -> **Archive** tab.



The drives will become available for use in TRASSIR after the formatting.

Setup Help

Recording prebuffer:  Store privileged channels exactly:  LSI MegaRAID Manager...

Motion detector reset timeout:  ☒ Store substream

When new large disk detected:  ☐ Store substream exactly:  Archive Encryption...

Disk model/serial	Enable	Read-only	Capacity	Current Stats
MR9271-4U00e4528f1ddea99f244028ba0fb00506	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Read-only		51952.97 GB	0.00 MB/s, 0 errors
MR9271-4U004627951ddea99f244028ba0fb00506	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Read-only		51952.97 GB	0.00 MB/s, 0 errors
MR9271-4U006bad991ddea99f244028ba0fb00506	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Read-only		51952.97 GB	0.00 MB/s, 0 errors

+ Add Storix Volume...



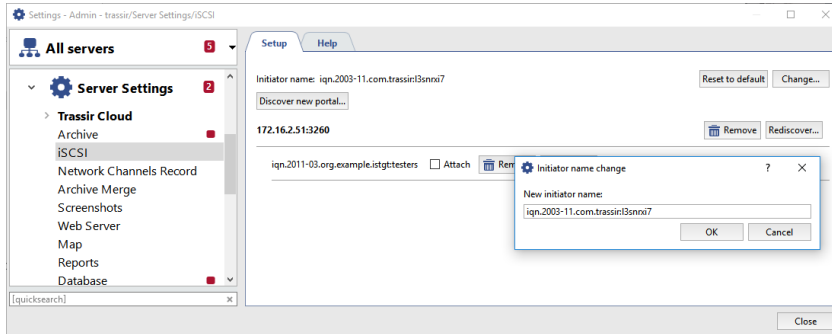
- [Archive](#)
- [Archive setup on the server](#)
- [Encrypting an archive](#)

## Configuring a network storage connection in Linux-based TRASSIR OS

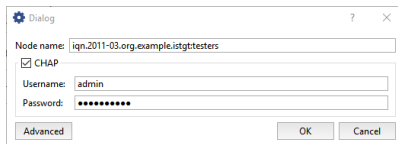


The description of this feature is intended to be used in the Linux-based TRASSIR OS

To configure a TRASSIR server's connection to network storage using iSCSI, go to the iSCSI tab and, if needed, click on the **Change** button and enter an **Initiator name**. This name will be displayed in the network storage's log when the TRASSIR server connects to it.

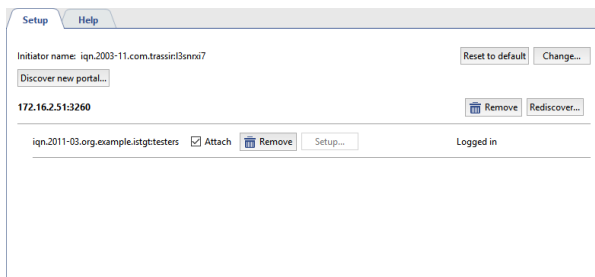


Then click the **Discover new portal...** button and enter the settings for the portal being connected to:



- **Portal** - The IP address or DNS name of the portal being connected to.
- **Port** - The iSCSI port, *configured in the network storage*.
- If you entered CHAP authentication parameters when configuring the network storage, set the **CHAP** checkbox and enter your username and password.
- Click the **Advanced** button to expand the advanced connection settings. You can change them, if needed.

Click **OK** and TRASSIR will attempt to discover the iSCSI portal using the specified settings. The window will either show the new portal or display a message about a connection error.



If you need to change a portal's connection settings, click the **Setup...** button and make the necessary changes in the window that opens.

Dialog

Node name: iqn.2011-03.org.example:istgttesters

☒ CHAP

Username: admin

Password: .....

Advanced OK Cancel

Commands to queue (power of 2): 128

Abort timeout: 15 sec

Host reset timeout: 60 sec

Logical unit reset timeout: 30 sec

Target reset timeout: 30 sec

Session initial login retry max: 8 times

DefaultTime2Retain: 0 sec

DefaultTime2Wait: 2 sec

Error Recovery Level: 0

FastAbort: Yes

FirstBurstLength: 262144 bytes

ImmediateData: Yes

InitialR2T: No

MaxBurstLength: 16776192 bytes

MaxConnections: 1

MaxOutstandingR2T: 1

Device's queue depth: 32

Replacement timeout: 120 sec

Xmit thread priority: -20

Target Portal Group Tag: 2

To connect a TRASSIR server to a network storage via iSCSI, set the **Attach** checkbox. The state will change to **Connected** and the logical disks configured on the network storage will appear in the **Archive** tab.



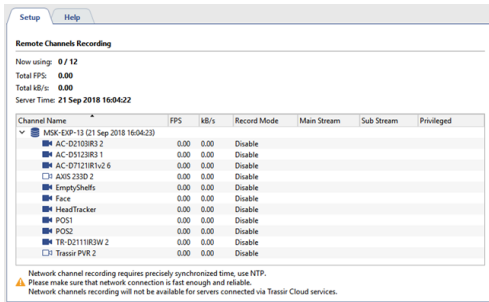
- [NAS Setup](#)
- [Configuring a QNAP Turbo NAS](#)
- [Connecting a network storage in a Windows OS](#)
- [Archive setup on the server](#)

## Recording network channels

TRASSIR Server supports recording an archive from devices connected to a different TRASSIR server as if these devices were connected directly to it instead.



Note that your software license determines your ability to record network channels and the limit on the number of network channels.



Channel Name	FPS	MB/s	Record Mode	Main Stream	Sub Stream	Privileged
MSK-EXP-13 (21 Sep 2018 16:04:23)						
AC-02103R3 2	0.00	0.00	Disable			
AC-05123R3 1	0.00	0.00	Disable			
AC-071218N2 6	0.00	0.00	Disable			
AXIS 233D 2	0.00	0.00	Disable			
EmptyShells	0.00	0.00	Disable			
Face	0.00	0.00	Disable			
HeadTracker	0.00	0.00	Disable			
POST	0.00	0.00	Disable			
POST2	0.00	0.00	Disable			
TR-Q211183W 2	0.00	0.00	Disable			
Trassir PVR 2	0.00	0.00	Disable			

Statistics are shown in the top part of the **Recording network channels** tab: License usage and restrictions, cumulative statistics for the stream of recorded network channels, and the current time. Below is a table with a list of network-connected servers and their channels. It visually depicts the current recording mode.

There are several modes for recording a network channel:

- **Permanent** - Recording will take place continuously;
- **On Detector** - Recording will take place when there is motion in the frame;
- **Like On Server** - Recording will take place using the same settings configured for this channel on the network server;
- **Disable** - Disables recording of this channel.



Note that an operator enabling manual recording of a network server in no way affects the recording of network channels on your server.

You can choose which streams will be recorded and mark one or more channels as privileged. The recording depth of the main stream for these channels will be determined by special [archive settings](#).



To properly record network channels, time must be synchronized on the servers. The local time of each network server is shown next to its name in the table. If it differs from your server's time, you must configure time synchronization across the network. The recommended synchronization period is two hours.



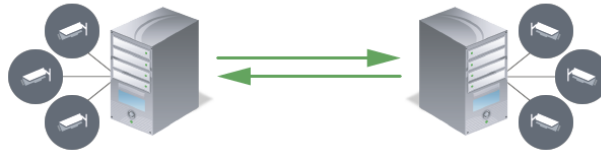
- [Archive setup on the server](#)
- [Archive](#)
- [Lost channels](#)



## Archive merge

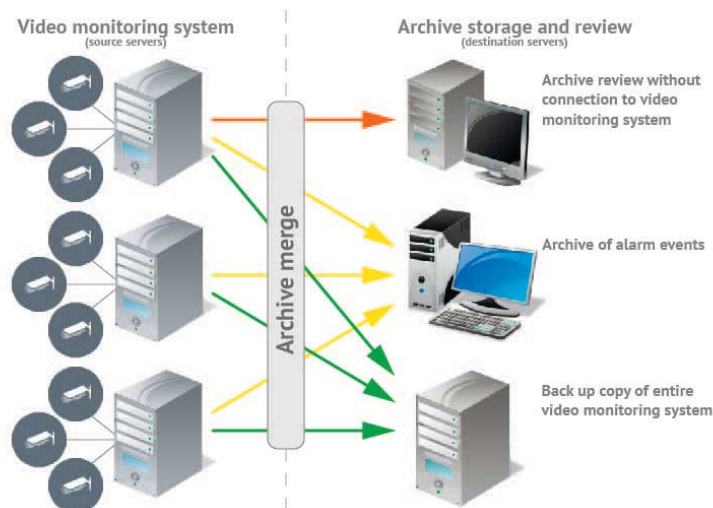
**Archive merge** - is a unique technology, allowing to share an archive from a server to which the video surveillance devices are connected, and which has the archive record set up, to one or several other servers.

Merging archives of two servers



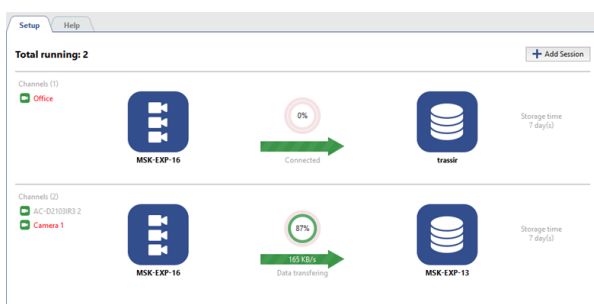
The purpose of the archive merge:

- **Backup copy.** - Create the identical (mirror) copies of all video surveillance servers archives. You set the time to start copying by yourself and the archive depth of the destination server can be much greater than the source one.
- **Archive review without connection to the video surveillance system.** You don't need to connect to the video surveillance servers to review the archive. Configure archive stream from several servers to a single one. Connect to this server to review the entire video monitoring system archive.
- **Creation of the alarm events archive.** You don't need to search for an archive fragment with a particular event captured. You can configure TRASSIR to mark a fragment as an armed one. Archive merge will allow to copy all these fragments to ant server, where you can review and analyze them.



### Settings highlights:

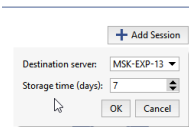
- Archive merge is activated and configured on the source server.
- The amount of the channels that can be uploaded to the destination server is defined by the quantity of licenses on it.



During the archive merge configuration, you can set up the following **session** parameters:

- **Where to copy?** - Set up the destination server to which *your server is connected*.
- **What to copy?** - Select what should be merged: all data or *armed events only*; set the archive depth, as well.
- **When to copy?** Right after the archive recording started or *at the scheduled time*.

## Adding a session



Press **Add Session** button and set the **Destination server** and **Storage time**.



If the source server is a server that stores archive from *personal video recorders* than press **Setup PVR Merge** and select **Destination server** and **Storage time** to transfer the archive to another server.



The maximal storage time on the destination server is **600 days**. Thus you can set up the archive of smaller size on your videosever. Connect to the source server the quantity of hard drives required to store the archive for several days and make regular copies to the destination server.

Further session configuration is described in *Configuration of the archive merge session on the source server*



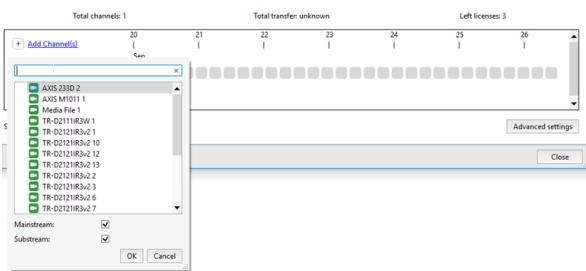
- *Connecting to a new server*

## Configuration of the archive merge session on the source server

After [adding a session](#) add channels and set the streams, the archive of which will be transferred to the destination server. To do this, press **Add Channel(s)** and select one or several channels. If you need to transfer **Mainstream** or **Substream** only, uncheck the corresponding box.



If the source server is a server that stores archive from [personal video recorders](#), there is no need to select channels to transfer archive to another server. The source server automatically adds channels to the session which all correspond to the PVR user archive. In case during [PVR turn in](#) you select the "Anonymous" user, the PVR identifier will be displayed instead of the channel name.

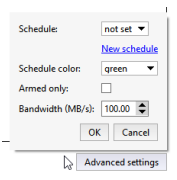


The number of channels added to the session is defined by the number of licenses on the destination server. The number of remaining licenses is displayed in the **Left licenses** field.



The archive merge will start after the channel selection immediately. The previously recorded archive won't be merged.

You can find more settings by pressing **Advanced settings** button.

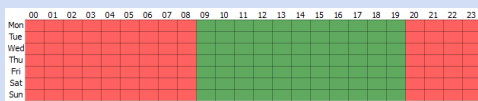


It will let you:

- **Set up the merge schedule.** Select the schedule in the **Schedule** field. In case there is no schedule created, press **New schedule** to create one. To change the selected schedule, click the **settings** link. After that, in the **Schedule color** field select the color of the area of schedule whereby the archive transfer to the destination server will take place.

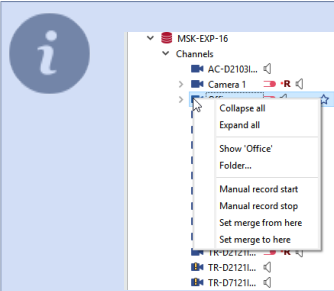


Usually the archive merge is set up at the least loaded time of the day, i.e. at night (red area).



You can learn how to set up a schedule in the [Schedules](#).

- **Activate the armed mode.** Check **Armed only** to do this.



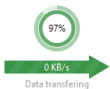
You can mark the recorded archive as armed:

- **Manually**, by selecting the corresponding item in the object tree.
- **Automatically** using [the script](#). For example, to activate the start of the event upon the motion start in the frame and the event end - upon the motion end.

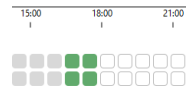
- **Set the merge speed.** In the **Bandwidth (MB/s)** field set the maximum value.



Advanced merge settings are the same for all channels in the session. If any channel requires other settings, add a new session for it.



The **round chart** displays the merge session progress. The outer circle represents the substream merge and the inner one represents the mainstream. The number in the middle stands for the size of the archive, transferred to the destination server.



On the bottom the info on each channel merge is shown. Point to the block to see the info on the data transferred to the destination server. The block size represents the stream type and the merge current state:

- **gray** there was no merging;
- **deep green** both streams or mainstream transferred;
- **light green** only substream transferred;
- **white** - merging is expected.



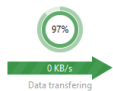
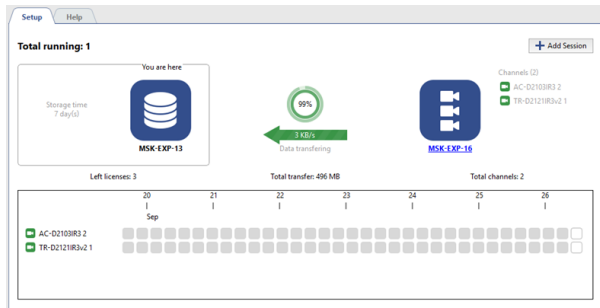
- [Archive merge](#)
- [Connecting to a new server](#)

## Reviewing the archive merge session on the destination server

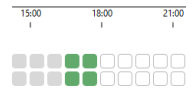
The archive merge session settings page on the destination server looks exactly the same as [on the source server](#). This page does not allow any configuration, it shows the info on the **Archive merge** operation.



If the destination server is synchronizing with the server that stores archive from the [personal video recorders \(PVR\)](#), the names of users that have been selected during [PVR turn in](#) are displayed instead of the channel names. In case you select the "Anonymous" user during PVR turn in, the PVR identifier will be displayed instead of the channel name.



The **round chart** displays the merge session progress. The outer circle represents the substream merge and the inner one represents the mainstream. The number in the middle stands for the size of the archive, transferred to the destination server.



On the bottom the info on each channel merge is shown. Point to the block to see the info on the data transferred to the destination server. The block size represents the stream type and the merge current state:

- **gray** there was no merging;
- **deep green** both streams or mainstream transferred;
- **light green** only substream transferred;
- **white** - merging is expected.



- [Archive merge](#)
- [Configuration of the archive merge session on the source server](#)

## Screenshot management

TRASSIR supports saving frames (screenshots) while viewing live video as well as when working with archived recordings. There are many ways to take a screenshot: the operator can do so manually or frames can be saved as an automatic response to specific system events (motion detected, ACS sensor passed, alarm zone crossed, etc.). The software has a feature to take screenshots based on a schedule. You can also take a screenshot independently of the SDK.

A special module has been designed for working with screenshots in TRASSIR. It lets you both view captured frames, copy them to removable drives (including exported video archives), and delete them. When connecting to a different TRASSIR server, you'll also have access to that server's screenshots and exported archive segments. You will be able to interact with the remote server's files just as if they were on your own server's disks.



You can work with screenshots directly from the settings window or from the *software's own interface*.

You can read more about working with the screenshot management module in the Operator's Guide (???).



- *Video monitor*

## Web server (SDK)

The web server is protected by the HTTPS protocol. You can use a browser to connect to the web server. When connecting, the browser should issue a warning that the server's identity could not be established. In order to avoid the warning, the server's certificate must be downloaded on the settings page and installed on the client computer. After the certificate is installed, if the warning occurs again it implies a third-party attempt to *insert its own program* between the client and server. [More about HTTPS](#).

The [web client](#) is a fully functional interface to access TRASSIR in the browser.

TRASSIR SDK is a set of tools for interaction with TRASSIR. It makes it easy to integrate third-party applications with TRASSIR functionality. You can read more about TRASSIR features in "TRASSIR SDK"

Stream broadcasting is available in JPEG, MJPEG, FLV/H264, and RTSP/MPEG4 formats. Select the broadcasting format, channels, and compression. Then use the context menu to copy the stream's address. The address can be pasted into any media player (we recommend [VLC](#) for testing), and you can integrate a FLV stream in your website using a Flash player.



Video transmission is not encrypted and may be intercepted by a hacker. Use a VPN to protect the connection.



When assigning ports, be sure they are not blocked and are not used by other software programs.



- [Configuring a server to work with the TRASSIR SDK](#)
- [Access to TRASSIR WEB-interface](#)



## Configuring a server to work with the TRASSIR SDK

Check **Trassir SDK** flag to enable access to TRASSIR server via SDK.

Depending on the functionality you are going to use, you should set the corresponding flags: **Object Tree**, **Call Methods**, **Events**, **POS Events**, **AutoTRASSIR Events**, **Read Settings**, **Screenshots**, **PTZ**, etc. You can use the item links for quick performance check of one or another feature, as well as a hint to the command syntax. If you wish to get video from the server or play the archive, check the following flags: **FLV**, **JPEG**, **MJPEG**.



See detailed description of TRASSIR features in ???.

You can change the **Port** which will be used to connect to server, if necessary. The default value is 8080.

Enter the password that will be used to get session or send commands when working through the SDK password in the **SDK password** field.



Access to SDK features is possible only in case **SDK Password** is entered.

The user under which the SDK will be accessed must have the **rights** necessary to use the functionality you need. When working through the SDK password, you must configure the required rights for the **Script** user.

In order to connect to the server via the Onvif protocol, set the **Enable** flag in the **Onvif** settings group, select the connection port and enter a phrase that can be used to find the server in the local network in the **Server location** field. In order to activate **RTSP Video Streaming** check the corresponding box and select the connection port.

TRASSIR has its own WEB-interface where you can configure the server and watch video from cameras. You can access the WEB-interface from any browser. Set the flag **Allow Trassir access from browser** to enable. Click the link next to the flag and the TRASSIR WEB-interface will open. Read more about connecting to TRASSIR server from the browser in [Access to TRASSIR WEB-interface](#).



Check **Redirect from port 80** box and you can use IP address of server only to open TRASSIR WEB-interface.

## Access to TRASSIR WEB-interface



The default ports to connect to TRASSIR WEB-interface are:

- **8080** and **80** - major and additional ports of access to TRASSIR WEB-interface. You can modify major port value and activate additional port use in [Web-server settings](#).
- **555** is video streaming port.

Add the connection to these ports to the firewall exception.

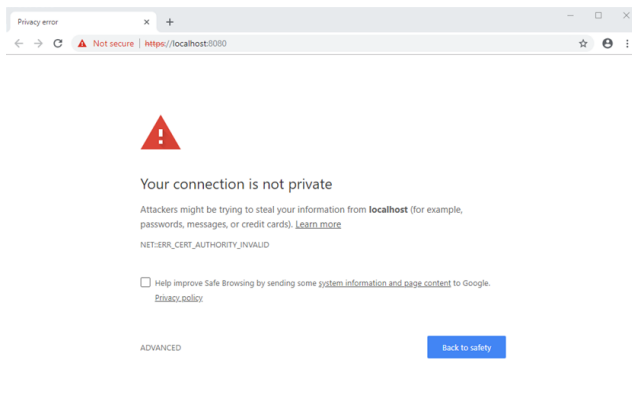
Connect to TRASSIR WEB-interface with the following steps:

1. Enter IP-address of server and access port (for example, <https://192.168.1.201:8080>) in browser address line.



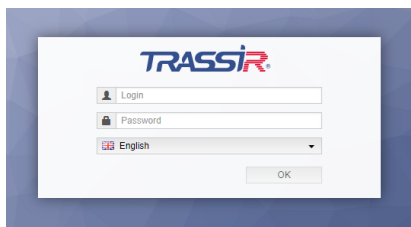
In case the **Redirect from port 80** box is checked in the settings, you can use only server IP-address to log in, for example, <https://192.168.1.201>.

2. Upon connection, a browser security system notification will appear. Click the corresponding link to confirm proceeding to server WEB-interface.

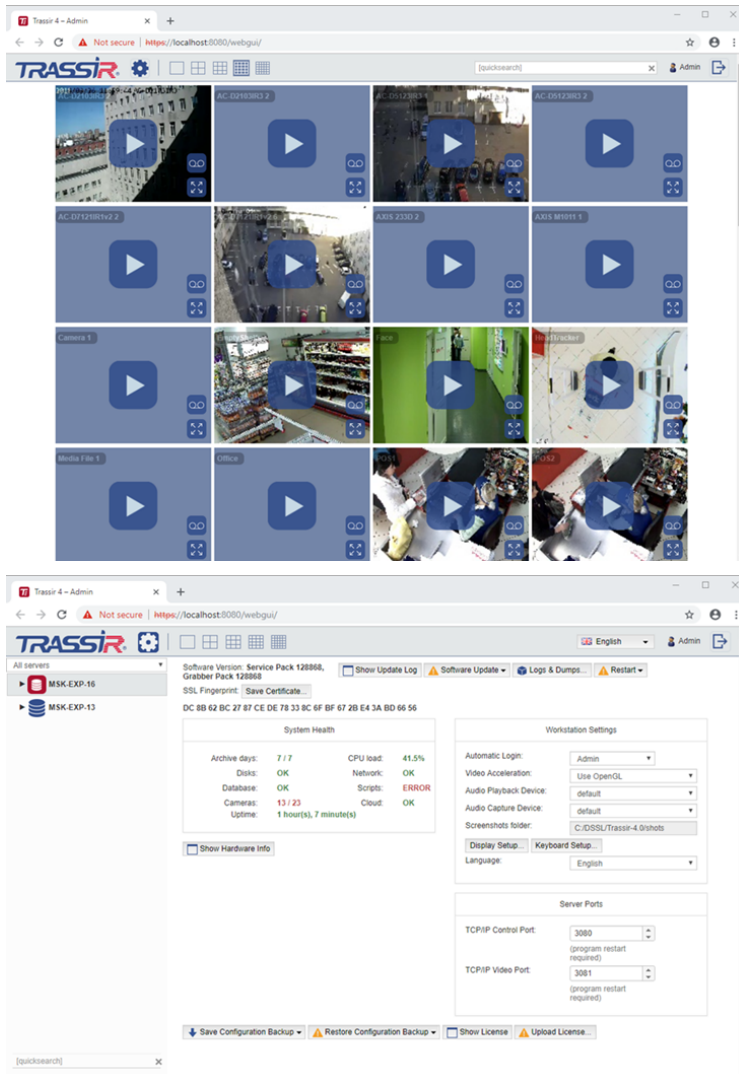


Add TRASSIR server IP-address to the browser secure address list. Therefore, upon the next connection the browser won't show the notification.

3. Enter **User name** and **Password** into authorization window. You can set TRASSIR WEB-interface language, if necessary.



4. You can start the work after that!



- *Configuring a server to work with the TRASSIR SDK*

## Map

TRASSIR lets you organize video surveillance using a two-dimensional graphical map on which you can arrange video cameras and other objects (for example, access control devices). You can create several maps in TRASSIR. Each map could represent a floor of a building or a group of rooms.

Adding a map in TRASSIR includes the following stages:

1. *Creating a map*. In the first stage, you give a name to the map and load its underlying structure (an image file with a floor plan).
2. *Adding cameras*. After creating a map, the range cameras on it (and, if necessary, other objects such as access control devices). Arranging the objects upon the floor plan facilitates easier comprehension, and when an event occurs (for example, motion), it makes it possible to know precisely where in the building it happened.
3. *Adding teleports*. A teleport is a named object on a map that can be used to switch to a different map. If you have several maps, then you can put teleports on each of them to switch between the maps.
4. *Adding floor to the map*. Floor is an object on the map required for the module operation *Neuro detector* which will display people on the map.

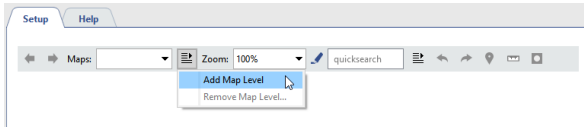


- *Creating a map*
- *Adding cameras*
- *Adding teleports*
- *Adding floor to the map*

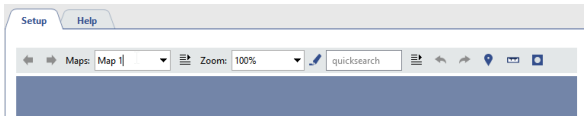
## Creating a map


To create a map:

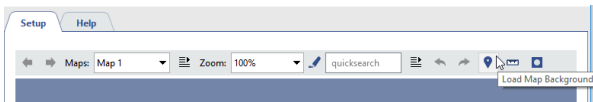
1. Open the **Settings** window.
2. Select **Map** in the list of settings.
3. Expand the **Maps** dropdown list and select **Add Map Level**.



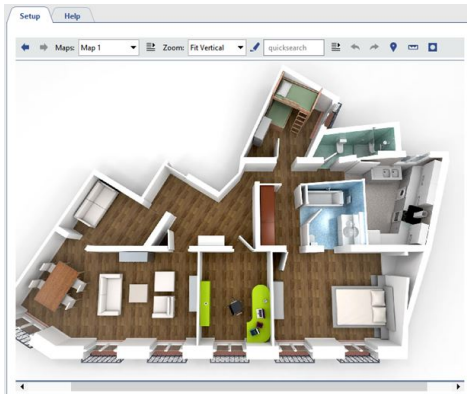
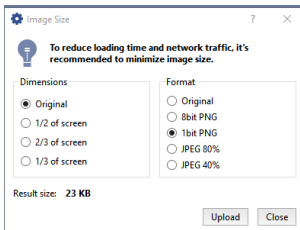
4. Enter a name for the new map.




5. To upload image press the button .



6. Select an image file and specify the image compression settings:



7. To washout the background press the button . Blurring the background makes objects and teleports more crisp and clear, helping to keep them from blending into the map's background image.

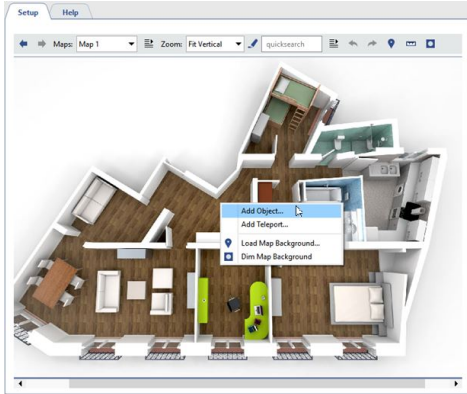


- [Adding cameras](#)
- [Adding floor to the map](#)
- [Adding teleports](#)

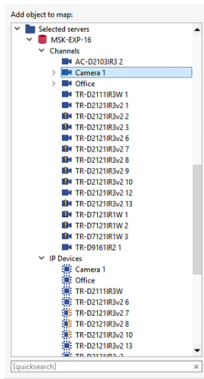
## Adding cameras

To add a TRASSIR object to the map:

1. Right-click anywhere on the map.
2. In the context menu that appears, select **Add object**.



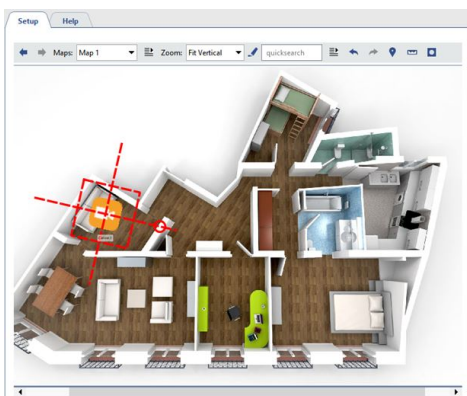
3. In the list of objects, double-click on the object to be added to the map (for example, a camera).



You can add other objects to the map in a similar way, such as servers, boards, IP-devices, Orion devices, floor areas.

An example of adding a floor area is described in section [Adding floor to the map](#).

4. Close the list of objects by clicking anywhere on the map.
5. Put the camera you just added in the desired location on the map. To do this:  
Left-click with the mouse to select the camera and drag it to the desired location on the map.



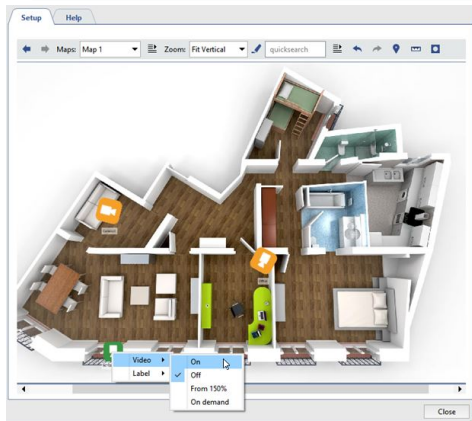
Left-click near the red circle and drag to set the required rotation and scale on the map.

6. Specify the camera's video display settings. To do this:

- Point the cursor at the camera icon and right-click.
- In the opened context menu set up the **Video** parameters:  
 "Disable" - if the camera's video does not need to be displayed on the map.  
 "Enable" - if the camera's video needs to be displayed on the map.  
 "Enable at 150% zoom" - if the video should be displayed only when the map's zoom level is 150% or more.  
 "On demand"—if videos are only need to be opened on demand by double clicking the channel icon.

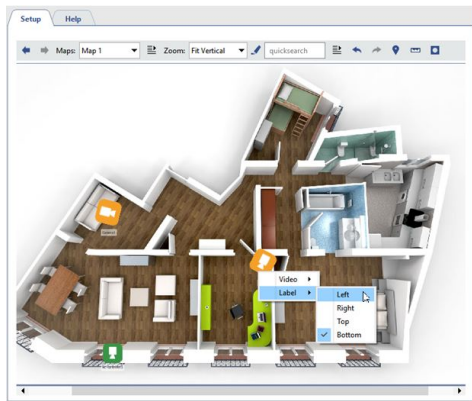


After making your selection, the video display area will be shown. If desired, you can change the area's size and location on the map.



7. Specify how the caption will be displayed relative to the camera icon (it is displayed below by default). To do this:

- Point the cursor at the camera icon and right-click.
- In the context menu that opens, use the **Caption** submenu to select a caption display option. The currently selection option is marked with a checkmark. To disable the caption for an icon, select the currently selected option (this will clear the checkmark; see the figure).



- [Creating a map](#)
- [Adding teleports](#)



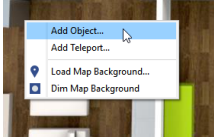
## Adding floor to the map



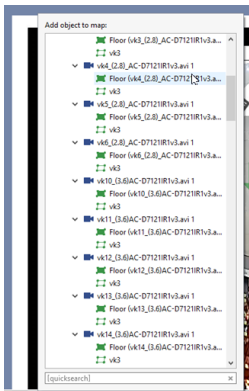
Adding floor to the map is possible only after its creation and calibration. See details in [Floor mapping settings](#).

To add floor to the map:

1. Right click on any place on the map and select **Add object** in the context menu.

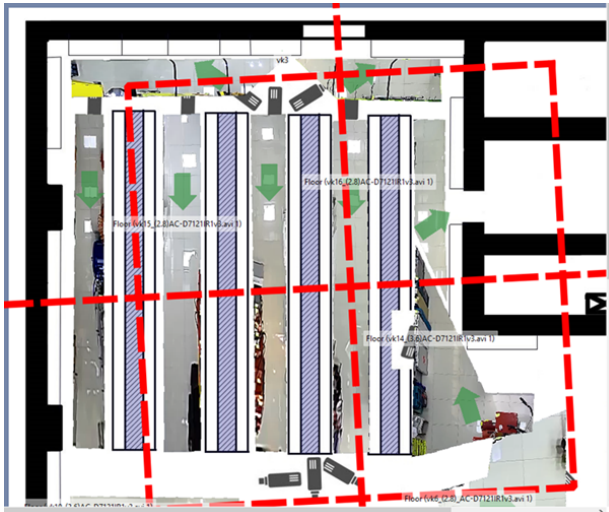



2. Find **Floor** object in the opened list and double click on it.

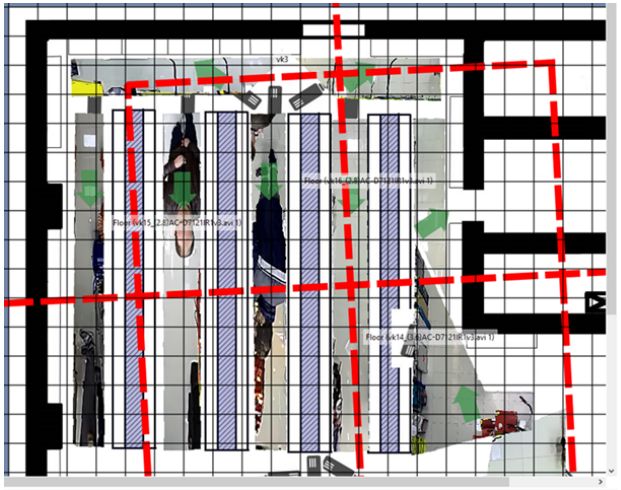


Click any place on the map to close the object list.

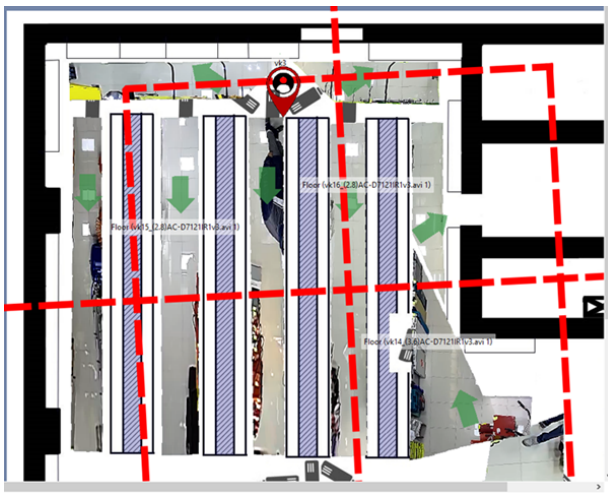
3. Change the angle and the size of an object to match the floor area with the plan on the map.



4. Click the  and using the grid and **Pixels per meter** adjust the image scale. Grid lines are placed on the image with 1 meter increment.



5. Click the  using the corresponding settings adjust the **Human marker size**, which will appear on the map while human detecting.

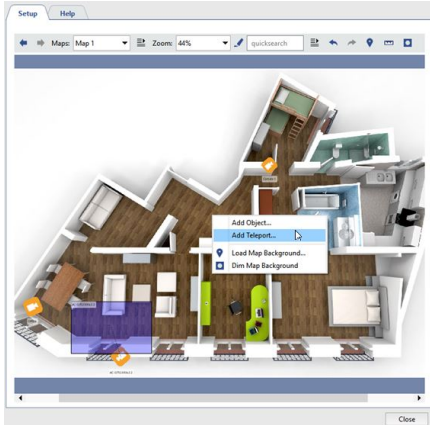


- *Creating a map*
- *Adding teleports*

## Adding teleports

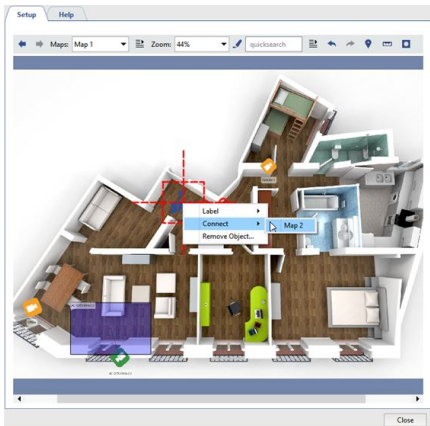
To add a teleport:

1. Right-click anywhere on the map.
2. In the context menu that opens, select **Add teleport...**



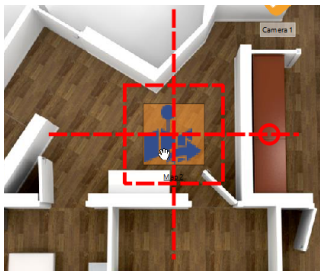
3. Link a teleport to the map that will be displayed when the teleport is selected. To do this:

- Point the cursor at the new teleport icon and right-click.
- In the context menu that opens, use the **Connect** submenu to select a from the list. The specified map will open when the teleport is double-clicked.



4. Specify the teleport's location on the map. To do this:

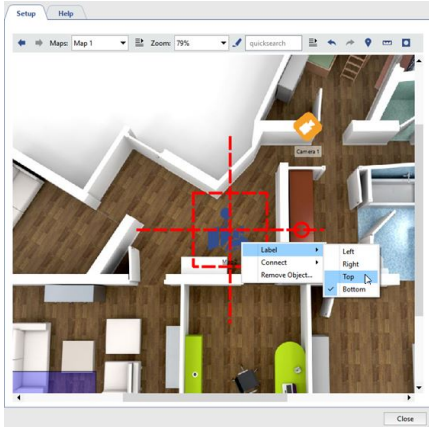
- Left-click with the mouse to select the teleport.
- Without releasing the mouse, drag the teleport to the desired location on the map.



5. Specify how the caption will be displayed relative to the teleport icon (it is displayed below by default). To do this:

- Point the cursor at the teleport icon and right-click.

- In the context menu that opens, use the **Label** submenu to select a caption display option.



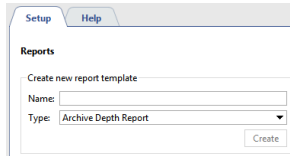
The currently selected option will be marked with a checkmark. To disable the caption for an icon, select the currently selected option (this will clear the checkmark).



- [Creating a map](#)
- [Adding cameras](#)

## Reports

The reports module is designed automatically or manually generate reports on the operation of a TRASSIR server in accordance with the specified templates.



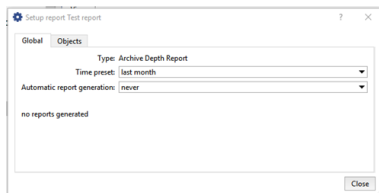
To start, you must create a report template. Enter template name, select a report type, and click **Create**. The *report template settings window* will open automatically.



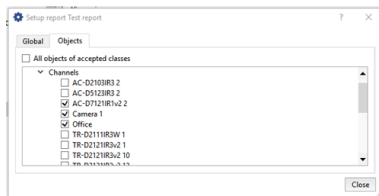
- *Report template settings*

## Report template settings

1. Open the **Settings** window.
2. Select **Reports** in the menu.
3. Give the new report a name.
4. In the report type drop-down list, select "Archive Depth Reports".
5. Click **Create**.
6. In the settings window, click **Properties...** and enter the settings for generating the report:
  - Global properties:
    - **Time preset** - The period of time for which the report should be prepared (for example, an hour, today, last month, etc.).
    - **Automatic report generation** - This parameter determines if and how often reports should be automatically generated. The default value is "never", i.e. reports are only created manually.

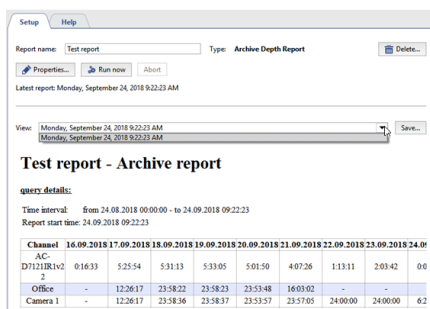


- Objects - The list of channels whose data should be used to generate the report. By default, all channels are used to create the report, but you can build a report using only the channels that interest you. To do this, clear the **All objects of accepted classes** checkbox on the **Objects** tab and check the desired channels.



7. Close the **Setup report** window.
8. Click **Run now**. When the reports been generated, a table will be displayed with the data gathered from the channels. For each of the selected channels, the days and corresponding archive depth will be indicated.

All newly created reports are saved in the database. Use the **View** dropdown list to access the reports; the list includes all reports created of the specified type. If a report is no longer needed, it can be deleted. To do this, select it in the **View** list and click **Delete**.



• **Reports**

## Database connection settings

All events registered by TRASSIR are stored in the database. The database can be located on either a local or remote server. For example, a separate server, used only for recording events, may be chosen for the database.



If you have a system with a heavy stream of events, we recommend using a database installed on a separate computer, i.e. a server used exclusively for the database's needs.

TRASSIR uses a PostgreSQL database, automatically creating all of the required tables and objects. In order for TRASSIR to work with a database, you must configure the database connection.

Note that in order to connect to the database, the PostgreSQL Database Server service must be running (the name will be different if you changed it during [installation](#)). If it is disabled, [enable it](#) using the pgAdmin utility or the standard tools for managing Windows services.

To configure the database connection:

1. Open the **Settings** window.
2. Select **Database** in the list of settings.
3. Specify the connection settings:
  - **Server type** - Leave this as "PostgreSQL".
  - **Host** and **Port** - The IP address or DNS name of the server where the databases installed. If the databases installed locally, then leave the value as **localhost**.  
If the database is installed on different server, then be sure your IP address is in the [list of authorized address](#) for external connections.
  - **Database Name**, **Username**, **Password** - The parameters that were specified for the database [when it was installed](#).
  - **Keep records for** - The period of time for which old events will be stored before being overwritten by new events.
4. Verify that the connection was established successfully ("Connected" will appear in the **Current state**: field).

The screenshot shows the 'Setup' window with the 'Database' tab selected. The 'Server type' is set to 'PostgreSQL'. The 'Current state' is 'Connected'. Under 'Connection Options', the 'Host' is 'localhost', 'Port' is '5432', 'Database Name' is 'trassir3', 'User' is 'postgres', and 'Password' is empty. The 'Keep records for' is set to '180 days'.

If the connection cannot be established, then the **Current state**: field will contain an error message containing the reason why the connection failed. For example, the connection failed in this case, because the database name was not entered correctly:

The screenshot shows the 'Setup' window with the 'Database' tab selected. The 'Server type' is 'PostgreSQL'. The 'Current state' is 'ERROR' with the message 'Error code: fe\_sendauth: no password supplied'. Under 'Connection Options', the 'Host' is 'localhost', 'Port' is '5433', 'Database Name' is 'trassir3', 'User' is 'postgres', and 'Password' is empty. The 'Keep records for' is set to '180 days'.



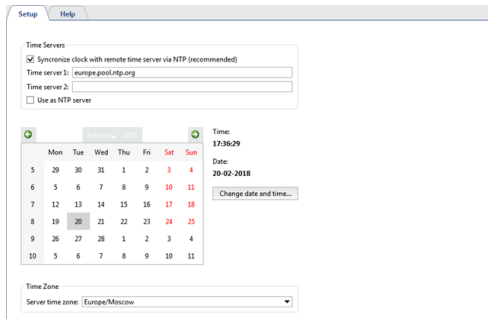
- *PostgreSQL DBMS installation*
- *Configuring the operating system to work with the PostgreSQL DBMS*
- *Starting the PostgreSQL Database Server service*
- *Allowing external connections to the PostgreSQL DBMS*



## Date and time



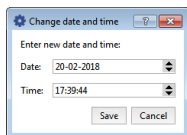
The description of this feature is intended to be used in the Linux-based TRASSIR OS



In the **Time Servers** settings group, you can enter the addresses of up to two NTP servers, which will be used to synchronize the date and time on the video server.

A server with TRASSIR OS can act for any IP device as an NTP server. To do this, set the **Use as NTP server** flag, and in the IP device settings, set the IP address of this server as the NTP server.

To manually change the date and time, click the **Change date and time...** button and enter the current date and time in the window that opens.

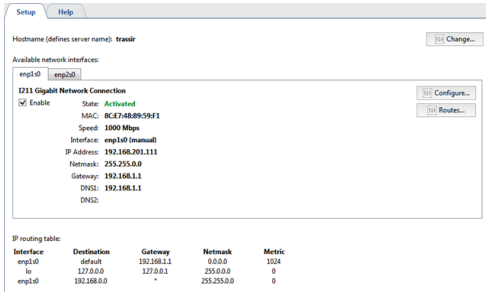


In the **Time Zone** settings group, select the time zone the video server is in.

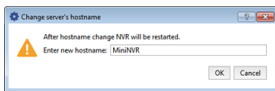
## Network interfaces



This tab is only displayed in TRASSIR OS. It is absent in the Windows version.



You can change the name of the server on the tab. To do this, click the **Change ...** button and enter a new name in the opened dialog box.



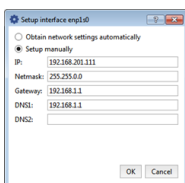
If the server name changes, TRASSIR OS asks to restart the video server in order to apply the change.

Below, **Available network interfaces** is displayed. Configuration of network interfaces, switching them on and off are made in the tabs.



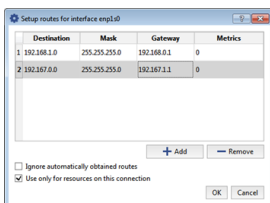
When connected to 3G / 4G modem server, connection settings tab will appear.

You can change the interface settings by clicking the **Configure...** button.



To configure the settings automatically, select option **Obtain network settings automatically** or **Set automatically**. Otherwise, select **Setup manually** and specify required connection settings.

For any network interface, you can define an IP routing table. Click **Routes..** button to create it.



Click **Add** button and edit the route.



To make the network interface use only the entered routing settings, set the **Ignore automatically obtained routes** flag.

Set **Use only for the resources on this connection** flag to restrict the connection to the limits of local network.

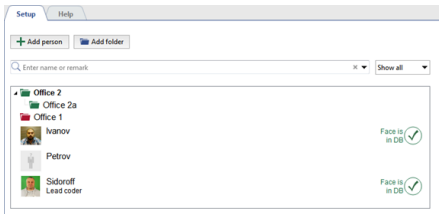
Created IP routing table will be displayed at the bottom of the tab.

IP routing table

Interface	Destination	Gateway	Network	Metric
enp1s0	default	192.168.1.1	0.0.0.0	1024
lo	127.0.0.0	127.0.0.1	255.0.0.0	0
enp1s0	192.168.0.0	*	255.255.0.0	0

## Persons

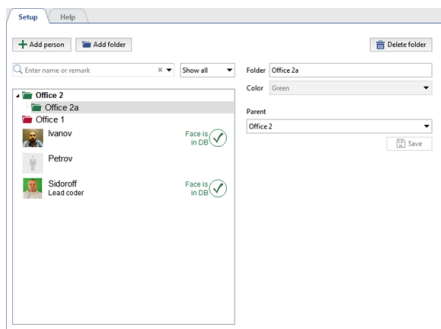
**Persons** is a database that contains information about people. TRASSIR allows you to create any structure of Persons database, consisting of folders and persons.



Persons database is used in operation of the following TRASSIR devices and modules:

- When **personal videorecorders** are used, the Persons database is needed to identify the person who received or returned the personal videorecorder and the video he filmed.
- For the **face recognition module**, anthropometric data is stored in the database to compare faces, recognized from the video, and the persons from the database. Select **Show faces DB** in the filter and only persons with entered anthropometric data will remain in the database.

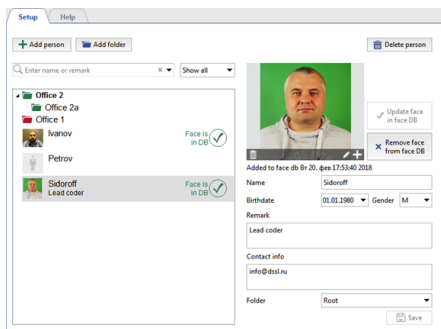
## Folders creation



To create a folder click **Add folder** button and fill in:

- **Folder** - folder name
- **Color** - folder color. When creating a folder of the 2nd level and above, the color will be the same as the 1st level folder.
- **Parent** - parent folder.

## Persons creation



To create person, click **Add person** button and do following:

- Click **Add photo** and choose photo of the person.  
If the person will be used for comparison in the *Face Tracker/Recognizer* module, click **Add face to face DB** button. In this case, the person will be added to the *Face Database* and marked with the corresponding icon.



Be careful, the size of the Faces database is determined by the license. Photos used for recognition should comply with the recommendations described in the *Recommendations for photos used for recognition* section.

- Enter person's name in **Name** field.
- Select **Birthdate**.
- Select **Gender**.
- Enter **Remark** and **Contact info**.
- Select **Folder** where person will be located.

## Users

TRASSIR implements a multi-tiered rights allocation system built on user accounts. Each TRASSIR server has its own list of user accounts with associated rights that are only applicable on that server. This must be considered when designing and initially configuring a video surveillance system based on several TRASSIR servers.

After installing TRASSIR, the following users are created in the system: Admin, Operator and [WebView](#). In addition to these users, a "Script" account is also created in the system, which is designed to limit the rights of [scripts](#) and the [TRASSIR SDK](#). The passwords for these users are not set by default.

TRASSIR is distributed video surveillance system. Its architecture supports combining an arbitrary number of video servers in a single network. You can control any TRASSIR server through client software or a web browser. You can administer and control servers you are directly connected to as well as servers you are indirectly connected to through a chain of other servers. You can read more detailed information about network connections between servers in the section entitled [Network](#).

User accounts are used to both start a TRASSIR server and to connect a TRASSIR client to a server. Regardless of what user started the server, the client software can connect under any user on the server who is allowed to sign in over the network.



TRASSIR 4 implements a full-fledged remote administration and control system. You can change any server setting from the client software; to do this, connect to the server using an administrator account or any other account that has rights to administer and control server settings. This feature makes it possible to administer and configure a server from any remote workstation, without requiring physical access to the server.

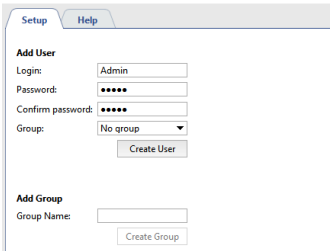


- [Adding users and user groups](#)
- [Determining access rights](#)
- [Per object rights](#)
- [Examples of user rights settings](#)
- [Audit](#)

## Adding users and user groups

TRASSIR lets you create accounts for individual users as well as groups of users. And you can configure detailed access rights for each account.

To create an account for a group or a single user, in the **Settings** window on the **Server settings -> Users** tab, select **Add**. Then enter the name of the user or group, create a password, and click the **Create** button.



The screenshot shows a web interface with two tabs: 'Setup' and 'Help'. Under the 'Setup' tab, there are two sections. The 'Add User' section has fields for 'Login' (containing 'Admin'), 'Password' (masked with dots), 'Confirm password' (masked with dots), and a 'Group' dropdown menu (showing 'No group'). Below these is a 'Create User' button. The 'Add Group' section has a 'Group Name' field and a 'Create Group' button.

An account for the user or group will then be created in the system. The new account will only be given basic rights: "View" and "View archive" for all devices, and the ability to view settings. To change rights, select the group or user in the list and define the access rights of the *user* or *group*.



When creating a user account you can select a group to add it to. To do this, select the group's name in the **Group** field. In doing so, all the rights of the selected group will be applied to the new user.



- [Determining access rights](#)
- [Determining access rights for a group](#)
- [Per object rights](#)
- [Examples of user rights settings](#)



## Determining access rights

You can access TRASSIR video surveillance system on server locally, as well as through network connection via another server, TRASSIR Client, [Web-client](#), or through mobile application. Local and/or network login can be allowed as well as forbidden for each user.

Check the corresponding boxes to enable:

- **Enable local login** - local user login.
- **Enable login from Trassir Server/Client** - network connection via remote server or TRASSIR client.
- **Enable login from mobile/web** - connection through mobile app or Web browser, or connection with TRASSIR [Web server](#).
- **Enable remote analytics** - consumption of the server computing resources in the operation of such plugins as [Neuro detector](#), [ArUco Detector](#), etc.



If local and other connections are forbidden, the user account will be blocked. All account settings will be saved in the system, but it cannot be used.

The **Enable remote analytics** checkbox is only available on **NeuroStation** type videorecorders.

The **Password** field is designed to forcibly change a password. Note that each user can change his or her own password through the [Control panel](#).

In the **Group** settings, select the user group that the user will belong to. In doing so, all the rights will remain the same as those in the selected user group.

The **User Interface Limitations** set of options also makes it possible to change the following settings:

- **Allow manage template** - If this checkbox is cleared, the user will not be able to save and create new templates. In other words, the user will only be able to use previously created templates.
- **Allow share templates**—if you uncheck this box, the user won't be able to upload a template to the cloud to share it with other cloud users.
- **Allow Settings button**—if you uncheck this box, you will prevent the user from logging in to TRASSIR settings window.
- **Allow Shutdown and Reboot**—if you uncheck this box, the user won't be able to turn TRASSIR off or turn off and reboot the server (won't be able to use these features in TRASSIR).
- **Allow "View" dialog** - If this checkbox is cleared, the user will not be able to change the camera window's appearance settings.
- **Allow password change** uncheck this box to prevent user from changing the password.
- **PTZ Priority** - This setting makes it possible to create a priority level for each user for PTZ device control. Thus, the higher the value of this setting, the higher the priority given to this user's PTZ commands relative to users with a lower priority.

- **Max archive playing speed**—this option determines the maximum speed value the operator can *review archive* with.

A user's base rights determine his or her abilities with respect to all of the objects on the server. Base rights include the following abilities:

- **View** - Determines the ability to see settings and objects. If this setting is disabled, the user will not be able to view a single object.
- **View archive** - Determines the ability to view the archive for all available channels, as well as the ability to create bookmarks in an archive. If this setting is disabled, the user will not be able to view the archive for live- or *lost channels*.
- **Hear Sound** - Determines the user's ability to listen to audio in real-time mode and in an archive.
- **Export archive, Screenshots** - This setting determines the user's ability to export an archive and save screenshots.
- **Edit Archive Bookmarks** - This setting determines the user's ability to create and edit bookmarks in an archive.
- **Use PTZ** - Determines the ability to control all available PTZ cameras.
- **Modify** - Determines the ability to manually control recording, generate reports, and control available objects (for example, the ability to change the state of Orion ACS objects).
- **Setup** - Determines the ability to change all server settings. If this setting is disabled, the user will not be able to add/delete devices, configure modules, etc.
- **Manage Users and Scripts** - This setting determines the user's ability to edit rights for all accounts.

In addition to base rights, you can assign *Per object rights*, in particular, rights to view, control, listen to audio, view archives, and control PTZ devices.

If the user account is no longer needed, it can be removed. To do this, open **Users** in the server settings, select the required user account and press **Delete**.



If that account was used for *server connection*, you won't be able to connect to the server with it. If you want to make an account inactive while preserving it on the system, then clear the **Enable Local Login** and **Enable Login from Remote** checkboxes.

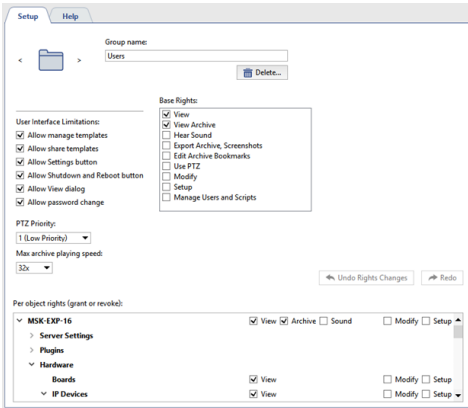


- *Adding users and user groups*
- *Per object rights*
- *Examples of user rights settings*

## Determining access rights for a group



When a group's rights change, the rights of all users in the group automatically change.



Configuring a group's access rights is no different than [configuring access rights for a single user](#).

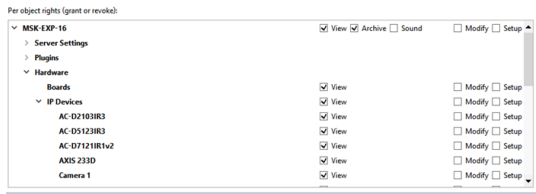
If a group account is no longer needed, then it can be deleted. To do this, open the **Users** item in the server settings, select the group, and click **Delete**. This will not delete the accounts of the users in the group.



- [Adding users and user groups](#)
- [Determining access rights](#)
- [Per object rights](#)
- [Examples of user rights settings](#)

## Per object rights

In addition to the base rights, the user may be assigned access rights to individual objects in the system – everything from the connected servers to an archive of loss channels.

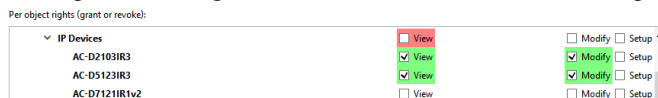


The following access rights can be assigned for each object in the system:

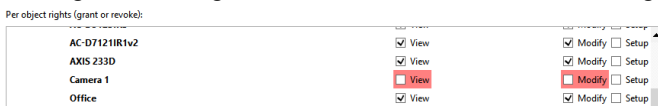
- **View** - Determines if the user can see an object in the system (if it is a device, channel, or server) and/or see specific system settings (server state, server settings, modules, and network).
- **Archive** - Determines if the user can view the archive for the selected channel. This settings is only applicable to channels.
- **Sound** - Determines the user's ability to listen to audio in real-time mode and in an archive.
- **PTZ** - Determines if the user can control PTZ cameras. This settings is only applicable to channels.
- **Modify** - Determines if the user can control the selected object.
- **Setup** - Determines the user's ability to listen to audio in real-time mode and in an archive.

The access rights system has its own hierarchy that includes basic (global) settings, settings for groups of objects (several levels), and access settings for individual objects. In the hierarchy, lower-level settings may match or differ from higher-level settings. If lower-level settings have not been assigned manually, they will automatically be changed to match higher-level settings. If lower-level settings are assigned manually and their state conflicts with higher-level settings, the corresponding item will be highlighted with a specific color:

- If a higher-level right is denied while the lower-level right is allowed, the latter will be highlighted in green.



- If a higher-level right is allowed while the lower-level right is denied, the latter will be highlighted in red.



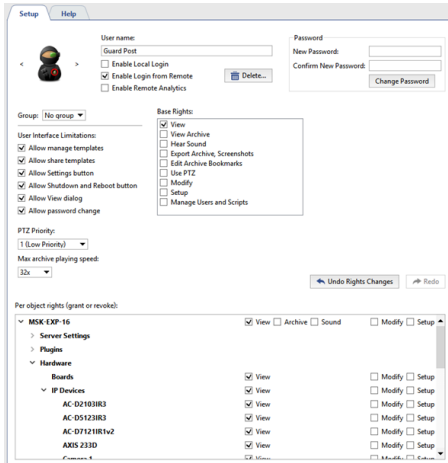
- [Adding users and user groups](#)
- [Determining access rights](#)
- [Examples of user rights settings](#)

## Examples of user rights settings

This section presents two examples of rights settings for typical user accounts:

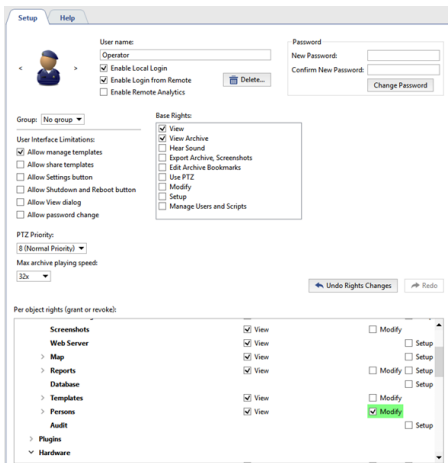
### 1. Account for a guard post.

- Only signing into the system over the network is allowed in the basic settings.
- The **Base rights** allow for **View**. Thus, this user can view live video from cameras and switch between previously created templates.



### 2. Server operator.

- The basic settings allow for signing into the system locally as well as over the network. Template management is also allowed.
- The **Base rights** allow **View** and **View archive**. Thus, this user can view a live video and work with an archive (only in view mode). Note that given these settings the operator will be able to see the picture but not hear audio.
- In the **Per object rights (grant or revoke)**, you must also allow template management, because the **Control** setting is disabled in the **Base rights**.

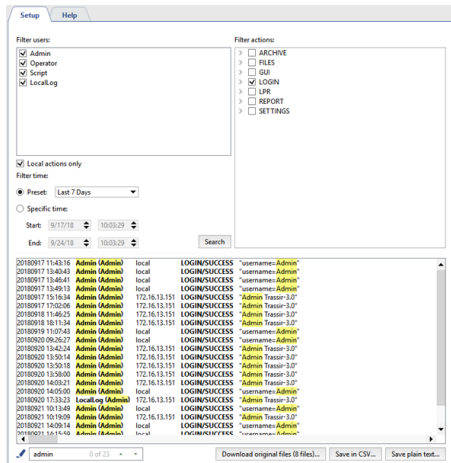


- *Adding users and user groups*
- *Determining access rights*
- *Per object rights*

## Audit


Audit is a module that tracks all user actions in TRASSIR. For example, a manual change to an archive's recording mode, a change to IP devices' settings, an operator's viewing of an archive, etc.

In the **Settings** window on the **Server settings** -> **Audit** tab, you can view the log.



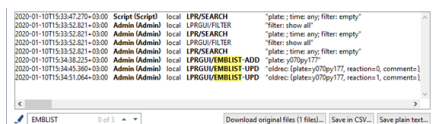
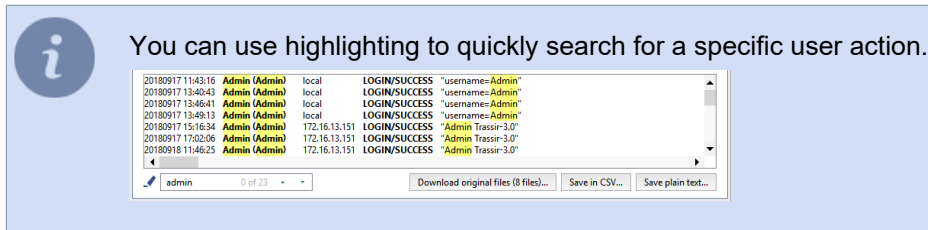
In the top part of the **Audit** tab there is a set of filters you can use to display only desired events in the log. You can use the following filters when viewing the log:

- In the **Filter users** field, select one or more users whose actions should be displayed in the log.

 TRASSIR actions that were not the result of users' direct actions are stored in the log under the **LocalLog** user.

- In the **Filter actions**, select the actions that should be displayed in the log.
- In the **Filter time** settings group, select the time period for which you want to view the log.

When the **Search** button is clicked, user actions that match the selected filters, along with the date and time when they were performed, will show in the bottom part of the tab.



If you need to find users who made changes in the **AutoTRASSIR embedded list**, select **LPR** in the **Filter actions** and start searching. The changes made in the lists are displayed through the following actions:

- EMBLIST-ADD** - adding a license plate number;
- EMBLIST-UPD** - editing the license plate number;
- EMBLIST-DEL** - removing the license plate number.

You can save the resulting action log to a file, if needed. To do this, click the **Save in CSV...** button or **Save plain text...**

As TRASSIR runs, all user actions are saved in the file `*.log`, which is located in the `audit` folder in the installation software folder. A log file is created every day when TRASSIR is first launched. At the same time, the old (yesterday's)

file is archived and saved in the same folder and, if needed, can be downloaded and viewed. To download a file, click the **Download original files...** button.



- [\*Users\*](#)
- [\*Adding users and user groups\*](#)
- [\*Determining access rights\*](#)
- [\*Per object rights\*](#)
- [\*Examples of user rights settings\*](#)

## Devices

TRASSIR ensures fully-featured operation with video capture boards manufactured by TRASSIR and with IP-devices manufactured by TRASSIR as well as by other companies. You can see the list of third party manufacturers of IP-devices supported by TRASSIR *at any time at our web-site*.

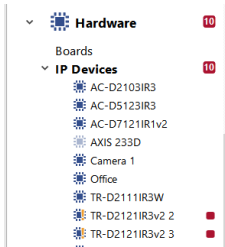


- *[Boards](#)*
- *[IP devices](#)*
- *[Configuring device settings](#)*






## IP devices


The list of the current IP-devices is always available in **Settings** window on **IP-devices** tab. IP-devices list is empty right after the installation of the system and it will expand if and when added.



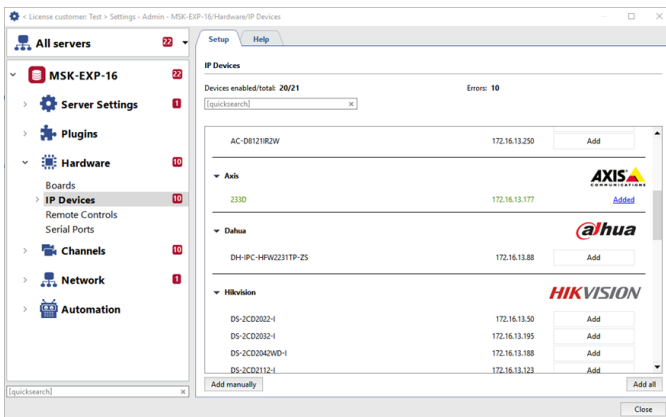
Each device in the list is identified by one of the following icons:

-  Connection OK. No error pending.
-  An error occurred when connecting to IP-device (it is necessary to open the tab of appropriate device to get detailed information concerning the mistake), or reload IP-device.
-  IP-device is disconnected. To activate the device select it in the list and press **Setup connection** button on the settings page.

On the right part of the window displays statistics of added/activated IP-devices and IP-devices operating with errors. Following is the list of IP-devices sorted out by manufacturer. Press **Add** button in appropriate line to add the device to the system.



Note that the list of available manufacturers is determined by the software license.



The devices will be highlighted with various colors depending on IP-address status:

- black - a newly-discovered network device;
- green - the device has been added and is working properly;
- red - the devices been added, but it is functioning improperly (for example, the credentials have been entered incorrectly).

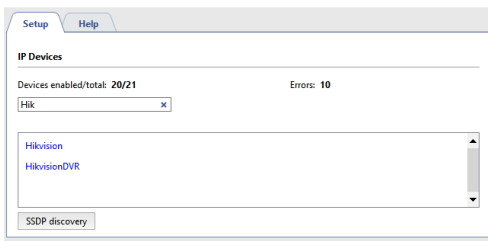
Use **Add all** button to quickly add all found devices to the system.

The **Add manually** button is used to **Add IP devices manually**.

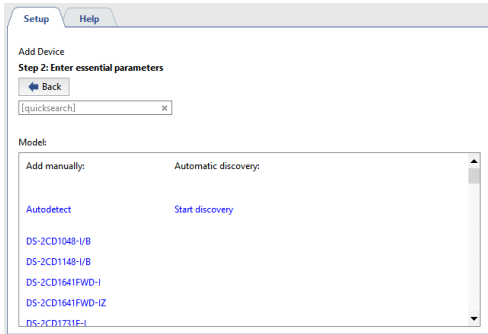


- *Adding IP devices manually*
- *Configuring device settings*
- *Channel settings*
- *Boards*

## Adding IP devices manually



Select a model from the **Add manually** list. If needed, you can use quick search to shorten the list of camera manufacturers and models, or click **Search** and select the desired device from the search results.

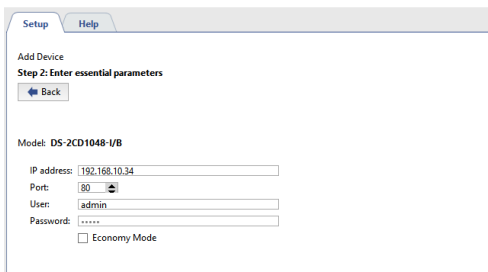


If the device you'd like to add is not on the list, you can use **SSDP discovery** option. In this case you'll need to set up the connection parameters and TRASSIR will recognize the model of the device and connect it.



**SSDP discovery** and **Autodetect** are supported only by certain manufacturers. **SADP** utility should be installed to provide for NVR and HikVision equipment autodetect.

Enter the connection information in the window that opens.



- **IP address** - The address doesn't need to be specified if the device was found automatically.
- **Port** - The number of the network port for connecting to the device (may be different from the web interface's port).
- **Username and password** - Note that the username and password entered must be for a user whose credentials are stored on the device itself.
- **Economy mode** - Set this checkbox if the transmission channel is unstable, costly, or if you do not intend for video from this device to be continually transmitted (e.g. the video will only be provided on-demand).

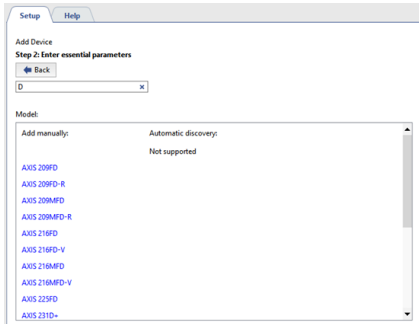
Click **Create**. The **device settings** window will open.



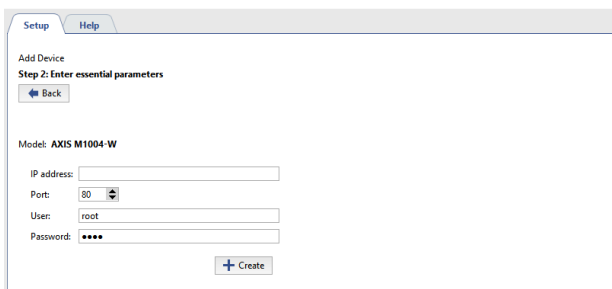
- *IP devices*
- *Adding IP devices that use the ONVIF protocol*
- *Adding IP devices using RTSP*
- *Configuring device settings*
- *Channel settings*
- *Boards*

## Adding IP devices that use the ONVIF protocol

TRASSIR supports working with IP devices using the ONVIF protocol. To add a new device, in the *IP devices* tab of the **Settings window**, click **ONVIF**.



Select the device model from the **Add manually** list. As needed, you can use quick search to shorten the list of camera models. Enter the connection information in the window that opens.

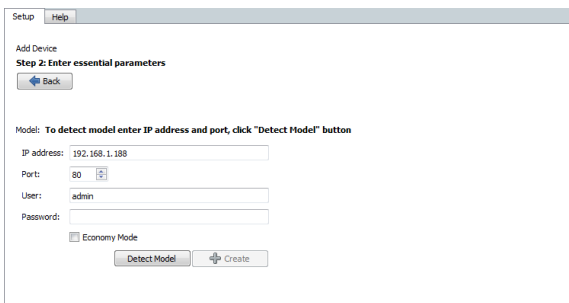



- **IP address** - The address doesn't need to be specified if the device was found automatically.
- **Port** - The number of the network port for connecting to the device (may be different from the web interface's port).
- **Username and password** - Note that the username and password entered must be for a user whose credentials are stored on the device itself.



Be sure to enter a valid username and password, because some devices use authentication at the model identification stage.

Click **Create**. The *device settings* window will open. If your device's model is not in the list, click **Identify model**. In the window that opens, enter the connection information just as described above and click **Identify model**.



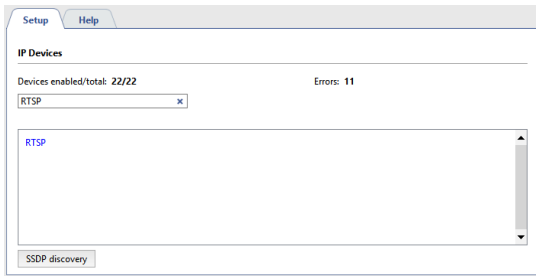
The **Model:** field will look as follows . After some time, the device model will be identified. Click the now-active **Create** button. The *device settings* window will open.



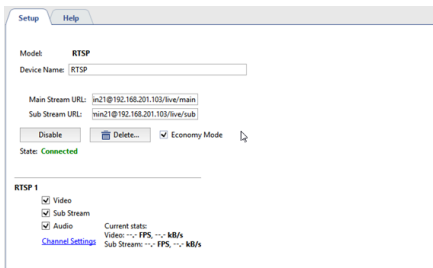
- *Adding IP devices manually*
- *Adding IP devices using RTSP*
- *Configuring device settings*
- *Channel settings*

## Adding IP devices using RTSP

TRASSIR can receive RTSP stream directly from various devices and use it in your video surveillance system by writing it to an archive, processing using video analysis, or transmitting it over the network. To add a new RTSP stream, in the *IP devices* tab of the *Settings window*, click *RTSP*.



Select RTSP from the *Add manually* list. Enter the connection information in the window that opens.



Fill in RTSP query strings *Main stream URL* and *Substream URL* using the following format:

```
rtsp://[user]:[password]@[ip_address]:[port]/[query]
```

- *Login* and *Password* are stored on the device.
- *IP-address* - device address you're connecting to.
- *Port* - The network device's RTSP port number (this is different from the web interface's port, usually 554).
- *Query* - camera-specific location of the required RTSP stream.



You can find possible RTSP query variants in camera user manual or technical documentation.

For example, for Axis 233D camera with IP-address 192.168.10.10 username "admin" and password "12345" URL will look like this:

```
rtsp://admin:12345@192.168.10.10:554/mpeg4/media.amp
```

*Add virtual channel* button is used to *isolate image area into a separate video channel*.

Click *Create*. The *device settings* window will open.

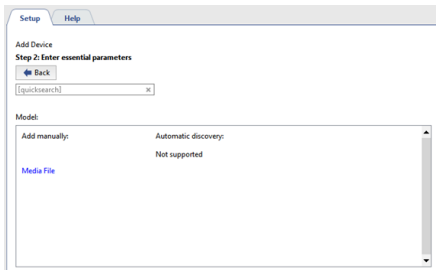


- *Adding IP devices manually*
- *Adding IP devices that use the ONVIF protocol*
- *Configuring device settings*
- *Channel settings*

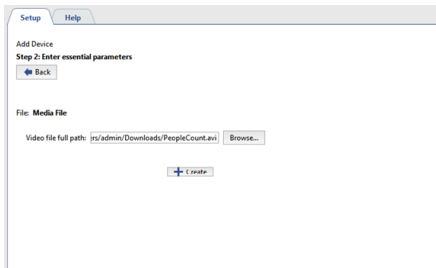
## Adding video files

TRASSIR lets using video files as video channels.

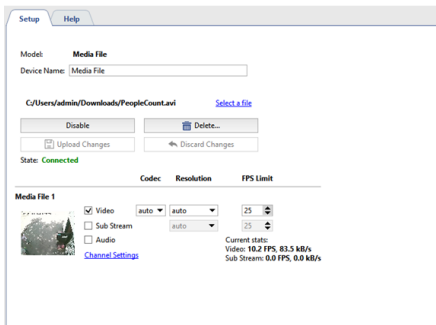
To add a video file, open **IP devices** tab. Select manual adding mode pressing **Add manually** button, and then go to **File -> Media File**.



Locate video file in the opened window and press **Create** button.



Video stream parameters settings window will open.



See more about settings in [Configuring device settings](#).

To substitute a video file, click **Select file** link and locate another file.

**Add virtual channel** button is used to *isolate image area into a separate video channel*.



- [Configuring device settings](#)
- [Channel settings](#)



## Image dewarp into several channels

Video transmitted by Fisheye-camera has a number of features: wide viewing angle and intense image deformation on the periphery. TRASSIR allows to dewarp the image into several independent channels and each of them will be recorded into the archive with its own settings.

Channel	Codec	Resolution	GOP	FPS Limit	Compression	Bitrate	Type
TR-D9161IR2 1	h264	6MP	20	25	Minimum	6000	Variable
TR-D9161IR2 2	SW MPEG4	640x480	20			1024	
TR-D9161IR2 3	SW MPEG4	640x480	20			1024	

To create a new virtual channel press **Add virtual channel** button.



The number of devices for which virtual channels can be created is determined by the software license. TRASSIR allows to create 4 virtual channels as maximum on each device.

New channel will appear under the main one. You can activate **Sound** if it is activated on the major channel and set the following parameters:

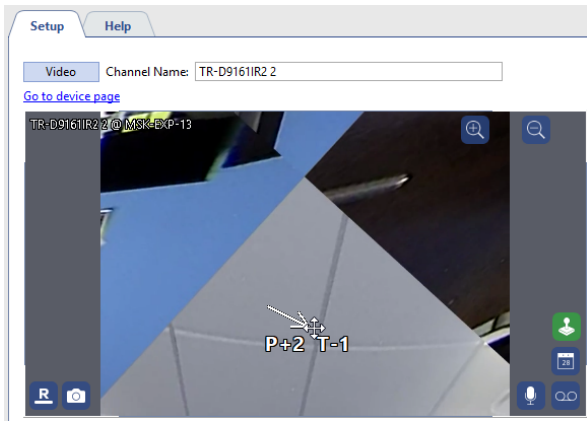
- **Codec** is compression codec used. **mpeg4** codec is used to compress virtual channel.
- **Resolution** is size of image.
- **GOP (Group of pictures)** group of pictures containing one key picture.
- **Bitrate** - video compression level.



Please note that at local view of the virtual channel non-compressed stream is displayed, and the compressed stream is recorded to archive. You will also see compressed stream while virtual channel viewing from TRASSIR client.

**Current stats** field displays video FPS and the speed of the channel record to the TRASSIR archive.

Go to **Channel settings** to specify image area to be isolated in to the virtual channel and saved into archive. To do this use PTZ-functions of the image control:



Other channel settings feature are also applicable to set up a virtual channel.





- *Configuring device settings*
- *Channel settings*

## Boards

TRASSIR can work with two kinds of compression cards issued by DSSL:

- DVS and DVS2 hardware-based compression cards (Silen, DV-M, DV-H, and DV-F systems).
- Techwell software-based compression cards (Optima system).

The list of compression cards installed on the server is always accessible in the **Settings** window on the **Boards** tab. Each device in the list is identified by one of the following icons:

-  The card is functioning normally, no errors detected.
-  Errors have been detected during the operation of the card (To see the errors in more detail, open the tab for the corresponding card).



- [\*Installing compression cards\*](#)
- [\*Configuring device settings\*](#)
- [\*Channel settings\*](#)
- [\*IP devices\*](#)

## Configuring device settings

After adding a device to the system, you can configure it, e.g. indicate the mode and settings to be used for video recording.

To configure a device, select it in the **Settings window**.

Setup Help

Model: AC-D7121R1v2  
Device Name: AC-D7121R1v2

IP Address: 172.16.13.164 Port: 8000 User: admin [Setup connection](#)

☐ Economy Mode

[Web interface](#)

State: **Connected**  
HDD: **absent**

	Codec	Resolution	GOP	FPS Limit	Compression	Bitrate	Type
AC-D7121R1v2 2	h264	1080p	30	25	Minimum	4096	Variable
	Sub Stream	CIF	30	25	Minimum	256	Variable

Current status:  
Video: 30.2 FPS, 578.2 MB/s  
Sub Stream: 30.2 FPS, 25.2 MB/s

[Channel Settings](#)

**GPIO Inputs**

Name	Normal State
<input checked="" type="checkbox"/> Enable Input Input 1	Low is normal

**GPIO Outputs**

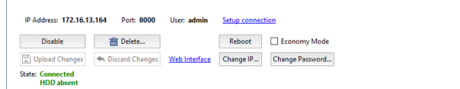
Name	Startup State
<input checked="" type="checkbox"/> Enable Output Output 1	Store in settings

**Internal PTZ Implementation**

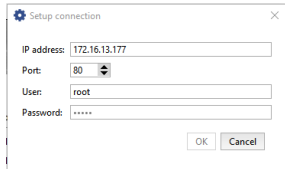
- **Model** - The device model.
- **Device name** - The name that will be displayed in the device list. By default, this is the same as the device model.

## Connection parameters settings

Devices connected to TRASSIR over a network have a number of other settings:

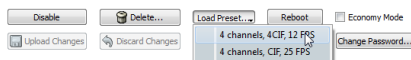


- **Network connection parameters** - IP-address, port and user name. Press **Setup Connection** to modify parameters.



Please remember that the user whose data is stored on the device should be entered.

- The **Disable** button lets you temporarily disconnect a device. All of the device's channels will drop off the channel list. If an archive recording was being made for a channel, it will be added to the list of lost channels. When the device is turned on, all settings made before it was disconnected will be preserved and the previously recorded archive will be available.
- Clicking **Delete...** will permanently delete the device from the system. The archive for this device's channels will be available in the list of lost channels. If the device is added again, TRASSIR will consider it an entirely new device – all of its previous settings will be lost. If a device is incorrectly or accidentally deleted, you can use the configuration recovery feature, which is described on the [main server settings](#) tab.
- **Load Preset**. Some devices - IP video recorders made by Lanser, in particular - use preinstalled modes. The **Load Preset** lets you choose the mode you want from a list.



For such devices, the settings **Resolution** and **FPS Limit** must only be changed using the **Load Preset** menu.

- **Upload Changes** and **Discard Changes** - After making any changes to an IP device's settings, you must confirm the changes by clicking **Upload Changes**. If there was a mistake, you can restore the device's previous settings using the **Discard Changes** button.



If a preinstalled mode is being used (**Load Preset**), you do not need to click **Upload Changes** – the settings will be sent to the device automatically.

- To go to the camera web-interface, click the **web-interface** link. It will open in external browser.



In TRASSIR OS camera web-interface will open in internal manual viewer.

- The **Reboot** button sends a reboot command to the device (required to apply settings to some devices).
- **Economy mode** - This checkbox specifies whether or not the device should use economy mode. Economy mode is used for slow, unstable, and/or costly transmission channels. Only device events are transmitted in this mode. In economy mode, video from the devices only transmitted on demand.



Note that not all devices support economy mode. When using economy mode, you must disable recording the archive to the server's disk. To do this, go to the [channel settings](#) and in the **Recording** group, select "Disable" for the **Recording to server disks** setting.

Device IP Setup

IP Address: 172.16.13.162

Port: 80

Netmask: 255.255.255.0

Gateway: 172.16.13.1

DNS1: 172.16.2.1

DNS2:

Device will be rebooted in order to apply these settings

OK Cancel

- **Add virtual channel** is used to allot an area of the image into an independent video channel. This function can be used to dewarp video received from Fisheye-camera into several separate channels. See in details in the section [Image dewarp into several channels](#).
- The **Change IP...** button will open network settings dialog. You can change address, port, subnet mask, default gateway and DNS there.
- The **Change password...** button will open camera password change dialog.

Device Password Setup

New Password: \*\*\*\*

Confirm Password: \*\*\*\*

Ok Cancel



After password change connection to the camera will automatically use new password.

- **Software Update** button opens the device software update file selection window.

Reboot ☐ Economy Mode

Change IP... Change Password...

Update firmware



This feature is not supported by all the devices.  
After the file selection confirmation device status will change to **Software update....**  
In case of successful completion the device will reload.

- The **State:** field displays the current state of the connection to the device.

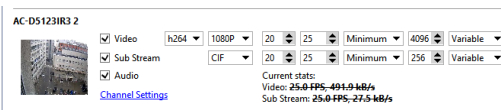
## Stream settings

Devices connected to TRASSIR transmit the following data streams:

- **Mainstream** is a high quality video data used for detailed viewing of video signal originated from the camera. This stream will be recorded to archive.
- **Additional Stream** or **Substream** is the video data of low (comparing to major stream) quality used in the case when it is necessary to display signals from numerous cameras on the screen. In this case high quality of video to display signal from the camera is not required. When transiting from the general scene viewing to detailed viewing of selected scene automatic switchover from additional to the major stream will be done. Substream enables the substantial decrease of load to the server and the network (in case connection to TRASSIR server over the network using TRASSIR client).
- **Audio stream** is audio data received from device.



Only certain devices support video data transfer via additional stream.



Left from stream settings picture and name of channel settings of which you are modifying is displayed. Go to **Channel settings** to access *its settings*. You can set independent settings for each stream:

- **Video** - Settings for the main video stream.
- **Substream** - the additional stream parameters. In case the **Substream** box is not checked, high quality video will be transmitted in both cases.
- **Audio** - Settings for the audio stream.

The following settings must be specified for the main stream and substream:

- **Codec** - The compression codec being used (the setting is the same for both streams).
- **Resolution** - The frame size (the list of possible values may be different between the main stream and substream).
- **GOP (Group of pictures)** - The size of a group of frames that contains a single keyframe. The smaller the value, the more keyframes there will be.
- **FPS Limit** - The maximum number of frames per second.
- **Compression** - The level of video compression (affects image quality and network traffic). The smaller the compression level, the greater the image quality.
- **Bitrate** - Data coding. The greater the value is, the better is the image quality and the greater is the network traffic.
- **Type** - Either a constant or a variable bit rate. If a constant bit rate is chosen, network traffic will be constant and limited by the value of the **Bit rate** field. Given a variable bit rate, network traffic will depend on the nature of the video stream.

**Current stats** field displays the number of frames per second and the bitrate of the stream which is recorded to the archive.



The number of settings available varies depending on the device model. When changing a device's settings, bear in mind its technical capabilities. If you enter settings that are not compatible with the given device model, the **State** field will display "The settings exceed the device's capabilities".

## Alarm input and output settings

If necessary you can define the device to detectors interaction parameters via GPIO inputs and outputs. The availability and the number of available inputs and outputs depend on device model.

GPIO Inputs		Name	Normal State
<input checked="" type="checkbox"/>	Enable Input	Input 1	Low is normal ▼

GPIO Outputs		Name	Startup State
<input checked="" type="checkbox"/>	Enable Output	Output 1	Store in settings ▼

Internal PTZ implementation	
<input type="checkbox"/>	Don't use ▼

If you're going to use this feature, you must set the checkbox to activate the required device input or output. For convenience, "Name" can be changed to any desired value. Then specify the normal state ("open" or "closed") for inputs and the start-up state for outputs ("off" or "on" or "store in settings").



To quickly monitor the state of alarm inputs and manage alarm outputs, place them on a [map](#). You can also create a [rule or script](#) to be run if the state of alarm input or output changes.



- [IP devices](#)
- [Boards](#)
- [Channel settings](#)



## Serial port settings

To set up serial ports, select **Devices** -> **Serial ports** menu item. In this menu you can set connection of analog tilting cameras (PTZ-devices) to the video surveillance system.

To set up a PTZ-device which is directly connected to the serial port of server press **Add serial port**. For device controlled through network converter press **Add MOXA serial port**.



Depending on the operating system, network converter port is added:

- **Windows:** as regular serial port.
- **TRASSIR OS:** - as separate network device.

Further on establish serial port settings:

- **Port name** - name of the serial port of server to which the device is connected.
- **Rate, Data bits, Parity, Stop bits, Stream control** are parameters of the port to which PTZ-device is connected.

Or network converter:

- **Address** and **Password** - IP-address of the network converter and password to connect to it.
- **Rate, Data bits, Parity, Stop bits, Stream control** are parameters of the port to which PTZ-device is connected.
- Press **Apply** button to connect to the network converter. Herewith connection result shall be displayed in the **Status** field.
- Clicking the **Web-interface** link you will directly change to network converter settings.



See details of PTZ-device connection in the section [Connecting analog PTZ cameras](#).

Now add single or several PTZ-devices:

1. Click **Add PTZ-device** link.
2. Select the channel from the dropdown list **Associated channel**.
3. Choose protocol for the tilting camera in **PTZ protocol** drop down list (it is determined by the camera model).
4. Enter unique identified for PTZ-device in **Device ID** field. A number of cameras can be bound to single serial port, each camera will be identified by the system by the unique identifier.



The device ID is adjusted on the camera using jumpers. When specifying camera settings and TRASSIR, note that the value of the **Device ID** field must match the camera's setup.

Setup Help

Serial Ports: PTZ, Access Control Panels

Name	Baud rate	Data bits	Parity	Stop bits	Flow control	
COM1	19200	8	None	1	None	Remove...

Associated Channel	PTZ Protocol	Device ID	
AC-DZ103IR3 2	Hikvision	0	Remove...
AC-D5123IR3 2		0	Remove...

[Add PTZ](#)  
[Add Access Control Panel](#)

## Remote Controls Settings

To set up a remote control select **Devices** -> **Remote controls** menu item. In this menu you can set remote control connection to the video surveillance system.



**Sensitivity** slider lets set mouse cursor motion rate when controlled with a joystick.

To connect a remote control to TRASSIR, press **Add remote control**, select the **Type** and check **TCP port** or **UDP port** - port to transfer data.

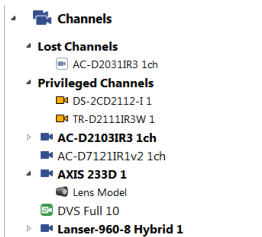


Before connection a remote control, for example **Hikvision DS-1100KI**, TRASSIR IP-address and data transfer port should be set on it.

See setting details in User's Manual of a particular remote control.

## Channels

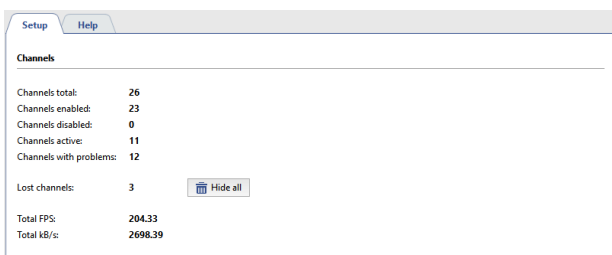
A list of all of the server's channels is always available in the **Settings** window on the **Channels** tab.



There are following types of the channels:

- Local channels** are channels of devices that are directly connected to the server. They are located at the top level of the settings tree. Each channel in the list is identified by one of the following icons:
  - the channel is functioning normally; no errors detected.
  - errors have been detected during the operation of the channel. To see the errors in more detail, open the tab for the corresponding channel.
  - a channel of a disconnected device.
- Privileged channels** are special local channels for which *different depth of the primary flow archive* is set. These channels are grouped into a separate **Privileged channels** folder.
  - privileged channel.
  - errors have been detected during the operation of the privileged channel.
- Network.** TRASSIR Server allows recording archive from the devices, connected to another TRASSIR server, as if these devices would be connected to it directly.
  - a network channel.
- Lost** are the channels for which there the system has an archive, but the video recording device in the system is missing (deleted). These channels are grouped in a separate **Lost channels** folder.
  - a lost channel.

The channel summarizes information about all of the system's local channels. Information about network channels is displayed on the **Recording network channels** tab of the server's settings.



If there are many lost channels in the system, but their archive is not required anymore, they can be hidden with **Hide all** button. You can hide a particular lost channel in this channel **Settings** by pressing **Hide lost channel archive**.

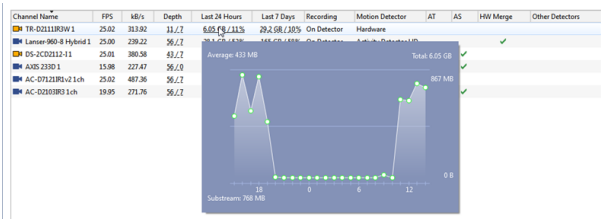
Detailed information for each local channel is displayed in the table below.

Channel Name	FPS	kB/s	Depth	Last 24 Hours	Last 7 Days	Recording	Motion Detector	AI	AS	HW Merge	Other Detectors
TR-02111R3W 1	25.00	317.64	31.2	6.05 GB / 13.5%	20.3 GB / 1.05%	On Detector	Hardware				
Lanser-960-8 Hybrid 1	25.00	252.24	36.2	28.1 GB / 1.52%	165.0 GB / 58%	On Detector	Activity Detector HD				
DS-2CD2112-1	25.00	378.30	63.2	7.61 GB / 1.14%	9.08 GB / 1.34%	On Detector	Hardware				
AXIS 2330 1	16.14	247.82	36.0	6.23 GB / 1.13%	28.6 GB / 1.32%	On Detector	Activity Detector HD				
AC-07121R1v2 1ch	25.02	488.59	36.2	5.63 GB / 1.05%	28.6 GB / 1.32%	On Detector	Hardware				
AC-02031R3 1ch	19.99	243.04	36.2	963.9 GB / 3.27%	6.15 GB / 2.22%	On Detector	SMART				

Icons next to the channel (similar to the icons of the channels in the settings tree) show its status. The table can be sorted by the parameter required.

The **Depth** column displays the depth of the archive of each channel connected to the server.

In **Last 24 Hours** and **Last 7 Days** columns you will find visual statistics of the distribution / volume of records by the hour / day for each channel. Move the cursor over the value and you will see a graph by which you can understand how intensively the archive of this channel was written in the last 24 hours or 7 days.



You can change some channel settings simply selecting it in the table. If you want to change the same parameter on several channels at the same time, select them with the cursor and change the parameter on one of them. This parameter will change on all selected channels.

Channel Name	FPS	kb/s	Depth	Last 24 Hours	Last 7 Days	Recording	Motion Detector	AT	AS	HW Merge	Other Detectors
TR-0211182W 1	25.02	311.82	31.7	6.05 GB / 11%	29.6 GB / 10%	On Detector	Hardware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Laser 980-8 Hybrid 1	25.00	239.22	36.7	28.4 GB / 13%	105.6 GB / 18%	On Detector	Activity Detector H	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
DS-2C02112-11	25.01	366.56	32.7	78.1 GB / 32%	185.0 GB / 58%	On Detector	Hardware	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
AS05-2330 1	15.98	227.47	36.7	7.43 GB / 14%	9.69 GB / 34%	On Detector	Hardware	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
AC-0712183-v2 1ch	25.02	487.36	36.7	6.21 GB / 11%	28.6 GB / 13%	On Detector	Disable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AC-0203083 1ch	19.95	271.76	36.7	5.82 GB / 10%	38.6 GB / 13%	On Detector	Hardware	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
				963 MB / 2.2%	633 GB / 2.2%	On Detector	Activity Detector HD	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
							SMART	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

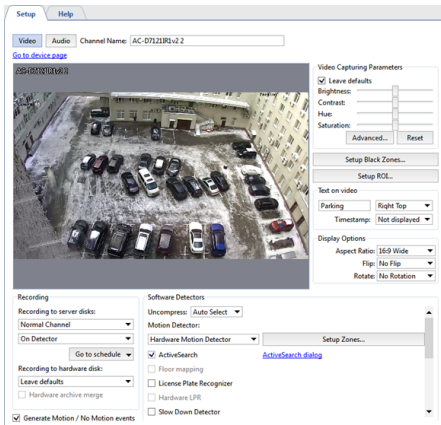


- [Channel settings](#)
- [Channel recording settings](#)
- [Motion detector settings](#)
- [Recording network channels](#)
- [Lost channels](#)

## Channel settings

The **Channel settings** tab lets you change the channel name, control the recording mode, and configure video analysis. It also lets you configure the audio channel.

To **configure the audio channel**, click the **Audio** button.



Clicking on **Go to device settings** will take you to the **settings tab** of the device to which the channel directly belongs. The **Channel settings** window is divided into several areas:

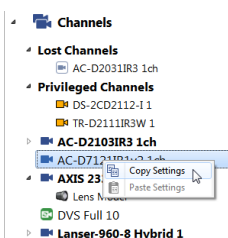
- The central part of the window has a real-time picture and you can control the camera just as you would in operator mode (for example, by using a camera's PTZ mechanism).
- **Recording**
- **Video Capturing Parameters**
- **Setup black zones**
- **Text on video (watermarks)**
- **Display options**
- **Software Detectors**

You can read more about the settings in each of these areas in the corresponding sections of the manual.

If the **Generate motion / No Motion events** checkbox is set, each time motion is detected a new event will be written to the database. It may be necessary to disable this feature to reduce the load on the database.



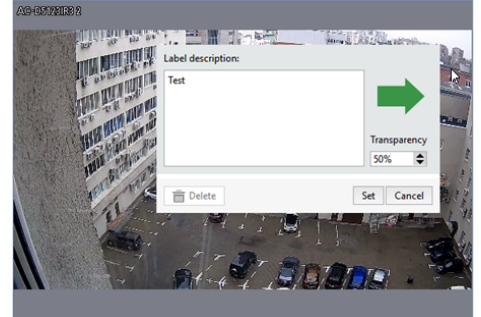
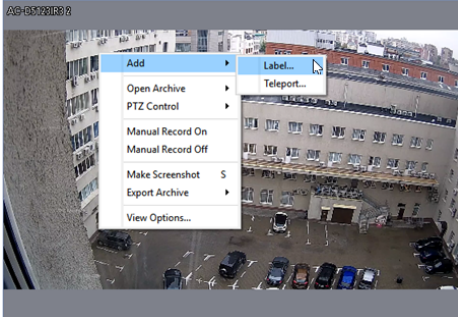
All the settings are applied "on-the-fly", and you can see all the changes in real-time.



After configuring a channel, you can copy it settings to a different channel. To do this, right-click with the mouse on the desired channel and select **Copy Settings**. To apply the copied settings to a different channel, bring up the context menu for the desired channel and select **Paste Settings**.

## Adding labels

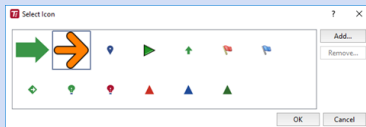
To analyze the scene in the camera image an operator may need to know what is placed on the given shelf, where does this door lead, etc. With the help of labels you can add all this information right on the image. Moreover, the label contents will display mouseover only. You can also adjust the label's transparency, so it won't cover the image. To add a label, right click on the image and select **Add -> Label....** In the opened window select the label's icon, adjust transparency, and enter text that will be displayed upon mouseover.



Place the label as you need. To do this, left click on the label and drag it. Right click will open label editor window.




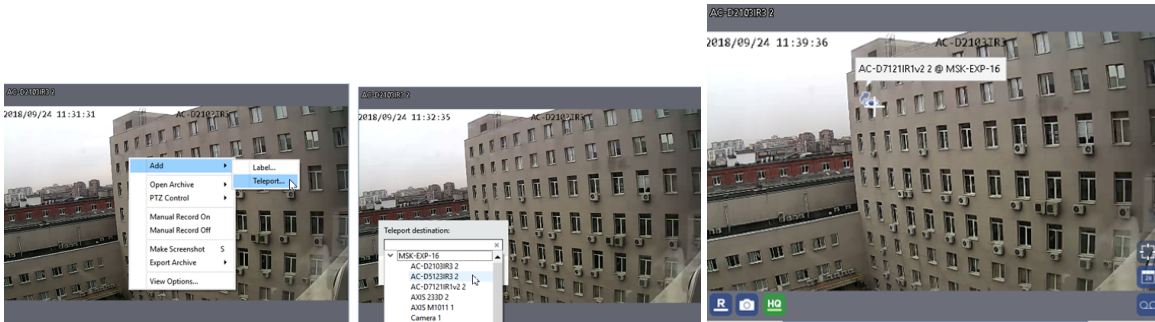
You can select the label's icon or upload your image as an icon. To do this, press **Add** and select the image.



## Creation of teleports from camera to camera

In operator's mode, to switch quickly between channels, you can use a teleport. To add a teleport, right click on the image and select **Add -> Teleport...** in the context menu.

In the window that opens, select the name of the channel that should open when the teleport button  on the video frame is pressed.



If needed, move the teleport icon to the desired location. To do this, click and drag it.

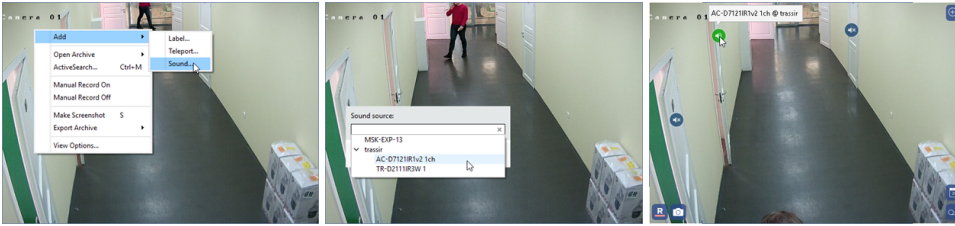
You can read more about using of TV ports, see the "Operator's manual" ([Using teleports when viewing the archive](#)).



## Adding multiple audio sources to a channel




In case there are several devices, recording both video- and audiostreams in one room installed, TRASSIR lets switch between these devices' audiostreams, without switching the channels.

To add an audio switch icon to a channel, choose in the right click menu **Add** -> **Audio**. In the opened window choose the channel the audiostream of which should be added.



After that an icon will appear on the video preview. Click the icon to turn on the channel audio stream. You can move to any place on the preview. To do this, left click and drag the icon.

The color of the icon indicates the status of the audio stream:

-  - sound is on.
-  - sound is off.
-  - the connection to the audio source is lost.



Make sure that the flag **Audio** is checked in the device settings in order for the device to appear in the list of the available audio sources. Read more in [Configuring device settings](#).



- [Channels](#)
- [Lost channels](#)

## Channel recording settings


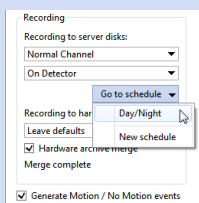
The **Recording** area lets you configure how the archive is recorded for a specific channel.

### Archive recording to server drives

By default, all channels are "normal." When the server runs out of free disk space, these channels automatically begin to be overwritten. You can mark a channel as "privileged", which causes the channel's archive depth to be determined using special [archive settings](#).

The **Recording to server disks** dropdown list controls the mode for writing to the local archive of the server to which the device is attached. There are four modes:

- **Disable** - Nothing will be written to the video surveillance archive from this channel.
- **Permanent** - The channel will be continuously written to the video surveillance archive.
- **Manual** - The channel will be written to the archive only upon the operator's on-the-fly commands ("Start manual recording"/"Stop manual recording").
- **On Detector** - The channel will be written to the archive only when detectors register events. Accordingly, if no detectors are defined for the channel, it will not be written to the archive.

If **Continuous recording** is used, then you can use the **Go to schedule** dropdown list, if needed, to go to advanced settings for the time intervals for continuous or detector-based recording. Learn more about setting a schedule in [Schedules](#).



If the device is operating in economy mode, then recording to the server's disk must be disabled.

### Archive recording to the built-in drive

Some video surveillance devices are equipped with their own archive. **Recording to hardware disk** and **Hardware archive merge** settings allow to select the mode of operation with the archive of the device:

In the **Recording to the device drive** setting, select the archive recording mode on the device:

- **Leave defaults** - The archive will be recorded to the device's disk in accordance with the device's internal settings. When establishing a connection with the device, TRASSIR sends it its own settings, including settings for recording the archive to the device's disk. If you select this option, the device's current settings will not change. This option

may be used, for example, if the recording settings were previously configured on the device itself and there is no need to change them.

- **Disable** - The archive will not be written to the device's disk.
- **Permanent** - The archive will be continuously written to the device's disk.
- **On Detector** - The channel will be written to the device's disk only when detectors register events. Note that the device will only receive information about motion detection based on its own hardware-based detector.

Turn on **Synchronization with archive on the device** function and in case of a failure, loss of communication or power failure, the missing parts of the recording on the TRASSIR server will be restored from the built-in drive of the device.

The archive recorded before the flag is set will not be synchronized.

Maximum depth of the downloaded from the device archive is 72 hours.

If there is no connection with the device for a long time (more than 3 days), only the last 72 hours will be synchronized after its restoration. The rest of the archive you can view on the device only.



Not all devices support working with a remote archive or the remote archive recording control feature.

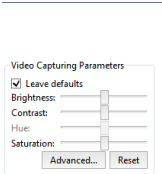


- [Archive setup on the server](#)
- [Channels](#)
- [Channel settings](#)
- [Motion detector settings](#)
- [Video capturing parameters](#)
- [Watermarks](#)
- [Black zones](#)
- [Changing image rotation and aspect ratio](#)

## Video capturing parameters

The image received from the camera may not be easy to discern. This may be a result of an unfortunate camera placement, external light sources, or the camera's own settings. You can try to achieve acceptable image quality by changing the default values for brightness, contrast, hue, and saturation.

These settings are in the **Video capturing parameters** area of the **Channel settings** window. When the sliders are adjusted, TRASSIR sends the settings to the device. Consequently, changes to the sliders' positions may change the picture from camera with some delay rather than instantly.

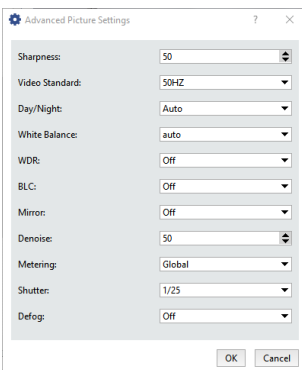


Depending on the device being used, one or more settings may be unavailable.

**Leave defaults** to not send the settings to the device. If you select this option, the device's current settings will not change. This option may be used, for example, if these settings were previously changed in an IP-camera's web interface.

The **Reset** button returns the settings sliders to their initial (Central) positions and restores the picture from the camera to its initial appearance.

Button **Advanced...** opens advanced image settings. Settings depend on the device type.



- [Channels](#)
- [Channel settings](#)
- [Channel recording settings](#)
- [Motion detector settings](#)
- [Watermarks](#)
- [Black zones](#)
- [Changing image rotation and aspect ratio](#)

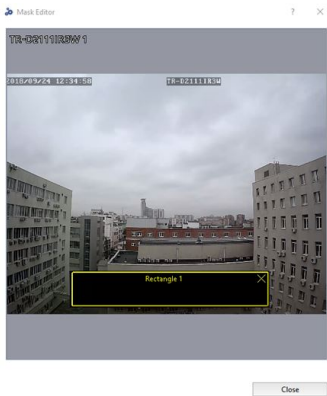
## Black zones

Black zones (or privacy zones) are designed to protect critical parts of a frame from video surveillance. These critical parts may be, for example, a door access panel or a computer keyboard. To prevent then video surveillance operator from seeing the password or any other protected information, you can "black out" the desired area, thus preventing leaks of confidential information.



Black zones cannot be used on all devices.

If a device supports black zones, then in the [channel settings](#) window the **Setup Black Zones...** button will be enabled. Click on the button to open the zone editor.



To create a zone, left-click with the mouse and drag to define the size of the black zone. There can be several zones. You can arbitrarily move them, change their size, and delete them.



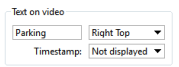
Black zones are shown over the video in both real time mode as well as in archive recording.



- [Channels](#)
- [Channel settings](#)
- [Channel recording settings](#)
- [Motion detector settings](#)
- [Video capturing parameters](#)
- [Watermarks](#)
- [Changing image rotation and aspect ratio](#)

## Watermarks

Hardware-based compression cards (DVS and DVS2) support watermarks, which makes it possible to superimpose arbitrary text and the current date and time. Watermarks can be used to prove the authenticity of video and protect an archive from being replaced.



In the **Text on video** area, you can enter arbitrary text (for example, the name of the camera) and select a position. You can also superimpose the current date and time on an archive.



Note that when viewing a channel on the server, the watermarks will not be visible. Watermarks can be superimposed on video in an archive in our displayed when connecting to a channel over a network.

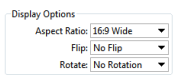


The Latin alphabet is used to display text over video; displaying text using the Cyrillic alphabet is not supported.



- [Channels](#)
- [Channel settings](#)
- [Channel recording settings](#)
- [Motion detector settings](#)
- [Video capturing parameters](#)
- [Black zones](#)
- [Lost channels](#)

## Changing image rotation and aspect ratio



In the **Display Options** area of the **Channel settings** window, you can change the following display settings for the channel:

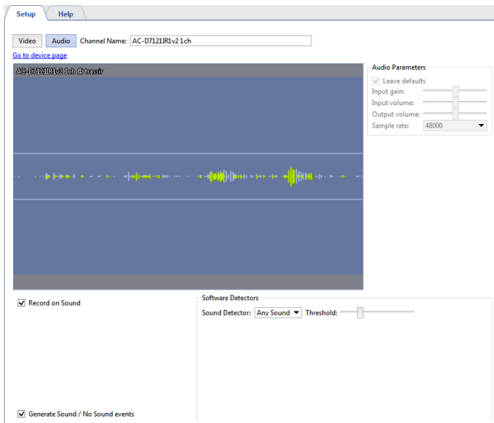
- **Aspect ratio** - Lets you select the image's aspect ratio: **Standard 4:3** or **Widescreen 16:9**;
- **Flip** - Reflects a mirror image **Horizontally** or **Vertically**;
- **Rotate** - Rotates the image by 90, 180 or 270 degrees.



- [Channels](#)
- [Channel settings](#)
- [Channel recording settings](#)
- [Motion detector settings](#)
- [Video capturing parameters](#)
- [Black zones](#)
- [Watermarks](#)
- [Lost channels](#)

## Audio channel settings

Clicking on **Go to device settings** will take you to the **settings tab** of the device to which the channel directly belongs. To **configure the video channel**, click the **Video** button.



The **Audio channel settings** window is divided into several areas. In the middle of the window you will see an oscilloscope representation of the audio coming from the camera's microphone.

You can set the volume level and quality of the audio stream in the **Audio parameters** group of settings. TRASSIR sends the moves of the sliders to the device, that's why the sliders can change the camera sound with a slight delay. If the **Leave defaults** flag is set, that volume and quality of the audiostream are defined by the parameters set in IP camera's web interface.

If the device audio stream is of poor quality, or the sound is off or missing, you can choose audio stream of any channel which will be played during the video review, from the **Default Sound** list. If the archive record on the channel, set as an audio source, is on, its audio stream will be also played during the archive review.



Make sure that the flag **Audio** is checked in the device's settings for the audio channel to appear in the list of the available audio sources. Read more in [Configuring device settings](#).

In the **Software Detectors** settings group, you can enable and configure the detector in the **Sound Detector**:

- **Disable** - Turns off sound detection on this channel.
- **Any sound** - Enables detection of any sound.

The activation threshold is depicted on the oscilloscope diagram in the form of two horizontal lines. When the sound level exceeds these lines the oscilloscope representation changes from green to red. Use the slider to adjust the **Threshold**. The sound detector will only be activated when the sound level exceeds the specified threshold. In other words, if there is a source of constant sound, such a road, near the camera's microphone, then in order to avoid activating the detector when a car passes by, set the activation threshold above the sound level of a passing car.

Set the **Record on Sound** to start recording to the archive when sound is detected.

If the **Generate Sound events** checkbox is set, each time sound is detected a new event will be written to the database. It may be necessary to disable this feature to reduce the load on the database.



Depending on the device being used, one or more settings may be unavailable.

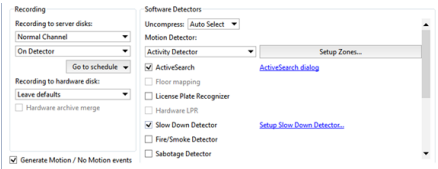


- [Archive setup on the server](#)
- [Channels](#)
- [Channel settings](#)
- [Motion detector settings](#)



## Motion detector settings

Motion detectors may either be hardware-based or software-based. Hardware-based detectors do not require any server resources, i.e. video processing is performed on the device itself. Software-based detectors use server resources. Moreover, some devices do not have hardware-based detector or a hardware-based detector may not be supported for a given device.



The **Decompress** parameter selects which of the streams – the primary stream or the substream – will be used by the software-based motion detector. In most cases, the quality of the auxiliary stream's video is good enough for the software-based motion detector. Selecting this stream conserves a substantial amount of server's processing power.



For the **Uncompress** setting, we recommend selecting **Auto Select**. In this case, TRASSIR will automatically select the best stream to decompress, depending on the motion detector and video analysis systems being used.

The **Motion detector** settings group lets you select which detector will be used.

- **Disable** - turns off motion detection on this channel.
- **Hardware Motion Detector** - The device's integrated hardware-based detector will be used for motion detection.
- **Activity Detector** - TRASSIR's free software-based detector will be used for motion detection. This detector suitable for most scenes.
- **HD activity detector** - TRASSIR's free software-based detector designed for detecting the motion of small objects in large spaces will be used for motion detection.
- **Moving Object Detector (SIMT)** - The SIMT software-based detector will be used for motion detection.



After the type of detector is selected, it must be configured. You can read more about the settings for each type of detector in the corresponding section.

You can enable use of one or more video analytics modules on the channel:

- **ActiveSearch**
- **Floor mapping**
- **License Plate Recognition**
- **Hardware LPR**
- **Slow Down detector**
- **Fire/Smoke Detector**
- **Sabotage Detector**
- **Face Detector**
- **Face recognizer**
- **Empty Shelf Detector**
- **Neural Empty Shelf Detector**

- *Queue Detector*
- *Head Tracker*
- *Workplace Detector*
- *Neuro detector*
- *ArUco Detector*
- *Bags counter*
- *Abandoned items neural detector*
- *Pose detector*



**Hardware LPR** is displayed in the channel settings if a camera with hardware LPR support is connected to the server. The module works in the same way as the built into the TRASSIR **License Plate Recognition**. However, its adjustment is performed directly on the camera.



You can read more about the settings for each type of detector in the corresponding section.



- *Channel settings*

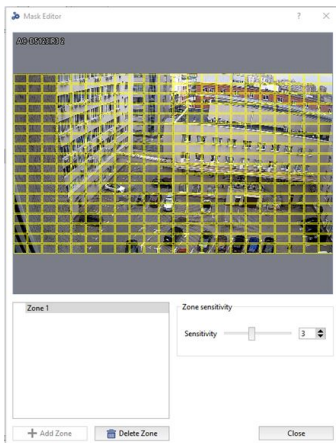
## Hardware-based motion detector settings

TRASSIR can receive information from cameras' and compression cards' hardware-based detectors. This conserves a substantial amount of video surveillance server resources.



Note that not all devices have an integrated hardware-based motion detector supported by TRASSIR. A device's hardware-based detector must be configured exclusively from TRASSIR and not through the device's web interface.

To configure a hardware-based detector, in the *Software Detectors* area of the *Channel settings* window, select *Hardware Motion Detector* in the *Motion detector* dropdown list and click *Setup Zones...*



To add a new zone, click *Add zone* or select an existing zone from the list. You can specify arbitrary areas within zones. To create an area, left-click with the mouse and drag to define the size of the area. You can move areas within a zone, change their size, and delete them.

All of a zone's areas share a common collection of detector sensitivity settings. If an area requires specific settings, then you must create a new zone.



Note that the maximum number of zones and areas as well as the number of settings available depends on the technical capabilities of the device itself.



- *Channel settings*
- *Motion detector settings*

## Software-based motion detector settings

If the camera doesn't have a hardware-based motion detector or if its quality is unsatisfactory, you can use TRASSIR's free software-based detector.

The TRASSIR software-based detector is provided in two forms: **Activity detector** and **HD activity detector**. **Activity detector** is appropriate for most scenes except large spaces; to detect the motion of small objects in large spaces, use **HD activity detector**.

<b>Recording</b> Recording to server disks: Normal Channel On Detector	<b>Software Detectors</b> Uncompress: Auto Select Motion Detector: Activity Detector
---	---

or

<b>Recording</b> Recording to server disks: Normal Channel On Detector	<b>Software Detectors</b> Uncompress: Auto Select Motion Detector: Activity Detector HD
---	--

To enable a software-based detector, in the **Software-based detectors** area of the **Channel settings** window, select **Activity detector** or **HD activity detector** in the **Motion detector** dropdown list. Clicking **Setup Zones...** will open the settings window.



Then add a new zone by clicking **Add zone** or edit an existing zone. Use the left mouse button to select the areas for motion detection. Use the right mouse button to adjust the areas.

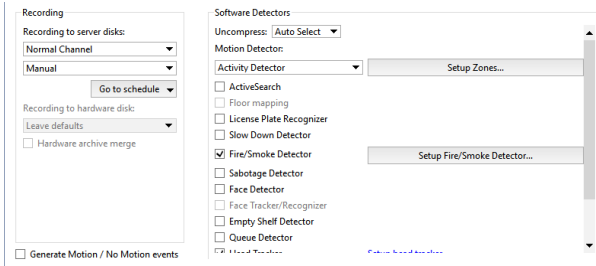
To configure the detector's sensitivity, change the value of the **Object size** slider. The sensitivity settings are specified separately for each zone. Up to five independent detection zones can be created.



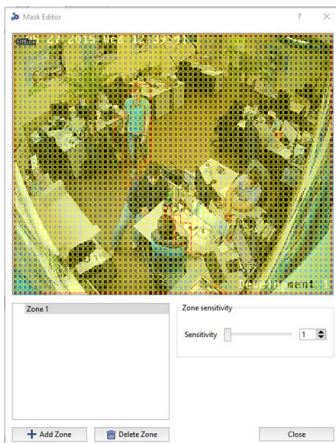
- [Channel settings](#)
- [Motion detector settings](#)

## Fire/smoke detector settings

To connect and configure a fire/smoke detector, in the *Channel settings* set the **Fire/Smoke Detector** checkbox and click **Setup Fire/Smoke Detector...**



Then add a new zone by clicking the **Add Zone** button or edit an existing zone. Use the left mouse button to highlight areas for fire/smoke detection. Use the right mouse button to adjust the areas.



Use the **Sensitivity** slider to adjust the detector's sensitivity. The sensitivity settings are specified separately for each zone. Up to five independent detection zones can be created.



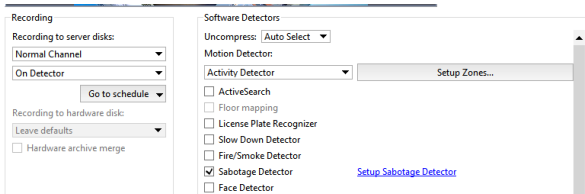
- [Channel settings](#)
- [Motion detector settings](#)

## "Sabotage detector" module settings

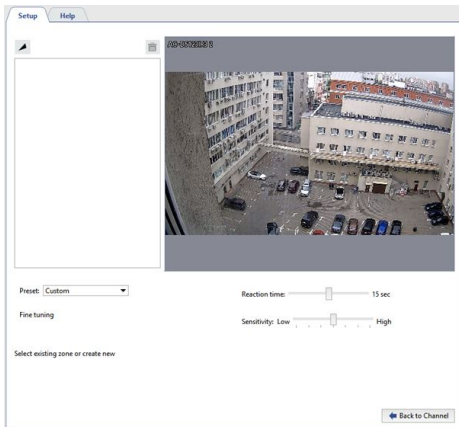
TRASSIR detects the following activities with camera as a sabotage:

- **Shift** - A change in the direction of the camera;
- **Misfocusing** - shooting area dimension change;
- **Flash** - heavy increase of shooting object illumination;
- **Closure** - heavy decrease of shooting object lighting.

To enable the detector, go the [Channel settings](#) to the [Software detectors](#) area and select the **Sabotage detector**. Click **Setup Sabotage detector** to open the settings window.




Detector settings window:



## Settings

1. Specify the **Reaction time** - the time period that will elapse between the sabotage detection and the notification. The minimum value of this parameter allows getting information about the sabotage promptly. At the same time, the probability of false alarms of the detector may increase.

While setting up this parameter, the following aspects should be taken into account:

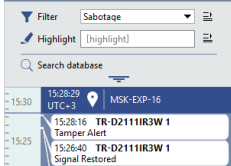
- Refrain from setting high value of this parameter as detector needs certain time to analyse the image and it will last for **Reaction time \* 3**. Thus, in case response time is 20 sec., detector will need 60 sec. for analysis. That is sabotage can be detected only in 1 minute following camera activation. In addition, following one sabotage detecting, the subsequent sabotage will be detected also in 1 minute.
  - In case the **Reaction time** will be less than it takes the camera to switch from the night mode to the day mode and vice versa, the sabotage detector will activate.
2. The **Sensitivity** parameter determines detector sensitivity degree. The higher the value is the higher is the probability of sabotage detection. We recommend to set the high sensitivity. In case false activation of detector the sensitivity value need to be decreased.
  3. Create **Active zones** to prevent the detector from being triggered by events that are not sabotage. For example, the detector may trigger on a door that opens sharply and widely. In this case, you can define the door opening zone as an active zone. To do this, press the button  the button and specify the zone borders on the image.



The active zones total coverage area should not exceed 40% of the frame. Otherwise, the detector will not be able to detect actual sabotage cases.

## Detector status monitoring

Detector status can be traced in real time in the *Event log*.



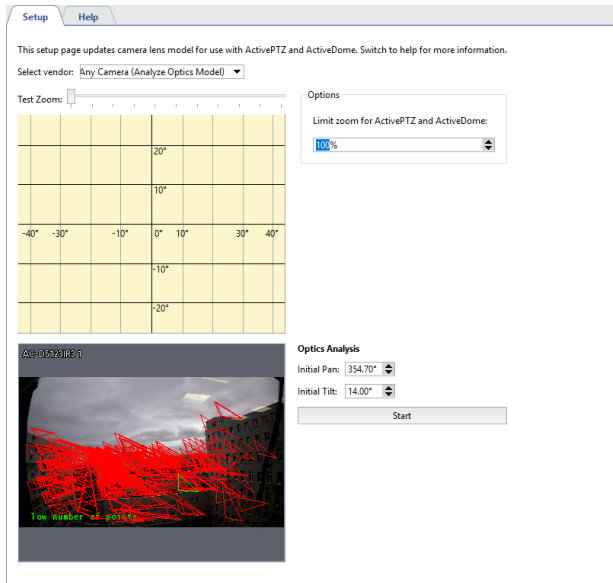
To provide the appropriate detector tracing, you can create *rule or script* which trigger on its status changing.



- *Channel settings*
- *Motion detector settings*

## Choosing an optics model and calibrating PTZ camera optics

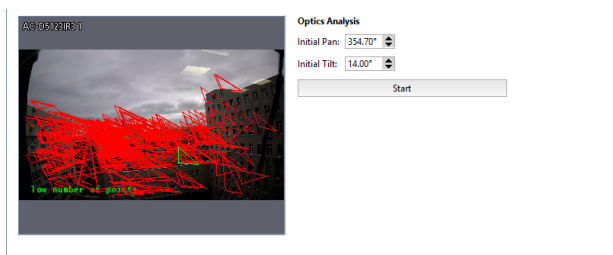
In order to correctly position the PTZ camera in ActivePTZ mode and in order for a PTZ camera to operate properly as part of the ActiveDome module, the camera's optics must first be calibrated.



If your camera's model is in the "Select vendor" dropdown list, then simply select it from the list. Otherwise:

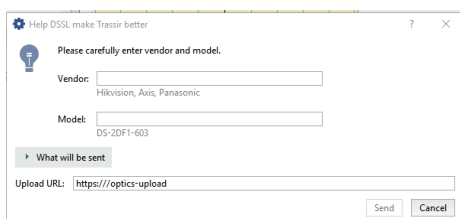
1. Select "Any camera (Analyze Optics Model)" in the "Select vendor" dropdown list.
2. Arrange the camera such that the image contains as many contrasting areas as possible.
3. Click "Start".

The automatic optics calibration process will begin (it may take several minutes). During the calibration process, the camera will be pointed at different points in the scene. When the calibration is complete, the grid will appear above the image along with a button to "Send optics model to DSSL"




Preferably, there should not be motion and external noise (rain, snow, swaying trees) in the camera's field of view during the optics analysis.

If you would like to help us improve our software, you can send your calibration results to DSSL over the Internet by clicking "Send optics model to DSSL". And dialog will open where you can enter the camera's manufacturer and model, and see exactly what information will be sent. Leave the default value in the "To be sent to" field. The information will be sent when you click "Send".





The additional setting "Limit zoom for ActivePTZ and ActiveDome" lets you control the camera's maximum zoom level. The default value is "0%" (no restriction). If the value "100%" is specified, the camera will rotate into the desired direction without any zoom.



Options

Limit zoom for ActivePTZ and ActiveDome:

100%




To test the calibration results, try to direct the camera at several points in *ActivePTZ mode*.



- *ActiveDome - Automated PTZ-camera control*

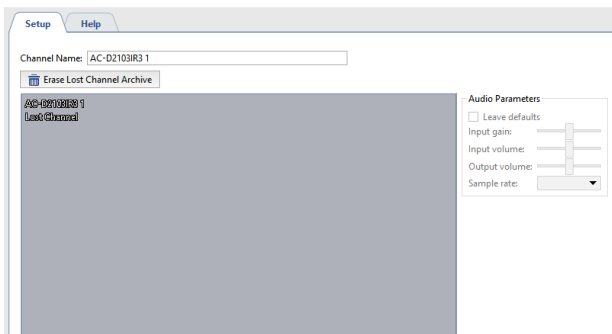
## Lost channels

Lost channels - is a unique TRASSIR feature that simplifies the work with an archive significantly. If a device is deleted or disconnected, the archive recorded by the device will be accessible as lost channels. They are identified in the TRASSIR interface by this icon  (You can read more about the possible colors of channel icons in the [Operator's Guide](#)).

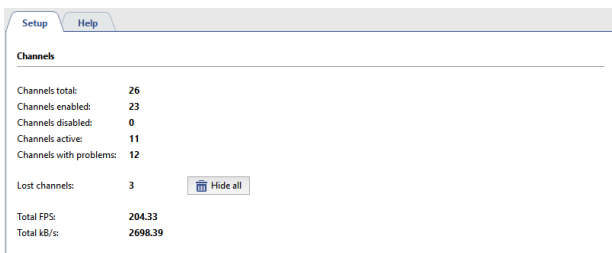
You can view and export the archive for these channels without any limitations; no additional steps or settings are necessary. And as usual, loss channels are available over the network given a client-server connection.

This feature also supports viewing an archive recorded on a different server in a video surveillance system. For example, if you copy an archive from one computer onto a disk, flash drive, or network drive and then connect the drive to another computer with TRASSIR installed, the list of the archive's channels will appear on the second computer (You can read more about connecting a new disk in the [Archive](#) section [Archive setup on the server](#)).

You can hide a particular lost channel in the [Channel settings](#), by pressing **Erase Lost Channel Archive**.



To hide all lost channels click **Hide all** in the **Channels** tab.



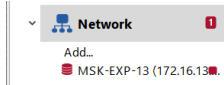
You can use both TRASSIR Server and TRASSIR Client to manage lost channels. You can read more about working with TRASSIR Archive in the [Operator's Guide](#).



- [Archive setup on the server](#)
- [Channels](#)
- [Channel settings](#)




## Network

TRASSIR is distributed video surveillance system. Its architecture supports connecting an arbitrary number of video servers to a single network.



Each server controls specific TRASSIR objects: IP devices, compression cards, etc. Accordingly, by configuring the connection between servers you can easily access TRASSIR objects on the local network or across the Internet. For example, one of the servers might be identified as the main server and used as the control center for all video surveillance objects; or be connected to all of the servers using TRASSIR Client.

You can find a list of the current connections with other TRASSIR servers on the **Network** tab of the **Settings** window. When TRASSIR is installed, the list of connections will be empty. The list will grow as connections are created, and each connection in the list will be identified by one of the following icons:

-  Connection with server is on. No errors pending
-  An error has occurred when connecting to the server (open the connection tab to see the details of an error).
-  Connection to the server is inactive (disconnected by user).

You can connect to TRASSIR servers in two ways: directly, by specifying the IP-address or using **CloudConnect**.

**CloudConnect** is a technology based on UPnP network protocols allowing to arrange direct P2P-connection between the servers operating not only in different local networks, but located very far from each other. CloudConnect creates endless opportunities to construct video surveillance systems of any volume and complexity. Using CloudConnect you do not need to apply static IP-addresses or set VPN-connection any more.



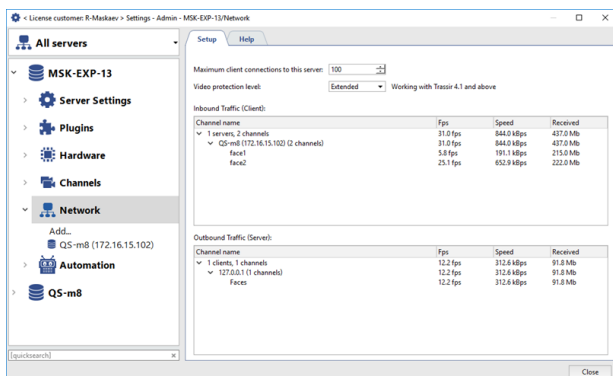
There are some cases when CloudConnect-connection will be *arranged via TRASSIR Cloud service*:

- TRASSIR cannot establish direct CloudConnect connection with the cloud camera or server within 10 seconds;
- While monitoring CloudConnect-connection errors have been detected which does not allow to carry out stable data transfer between TRASSIR.



CloudConnect technology use is possible only further to *connection to TRASSIR Cloud service*.

Network statistics are displayed in the right part of the window. You can see real-time statistics for servers to which you are connected and for clients and servers connected to you.



Please note that in the interest of the network throughput TRASSIR server streams only those devices where the client-based action is currently taking place (watching video in real time, working with archive data, *recording network channels*.) Moreover, the setup of the **Maximum client connections to this server** parameter allows to limit the number of clients that will be able to connect to the given server.

The **Video protection level** setting lets you select the protection method, which will be used for data transfer between the client and the server:


- **Base** - for all TRASSIR versions.
- **Extended** - for TRASSIR 4.1+.



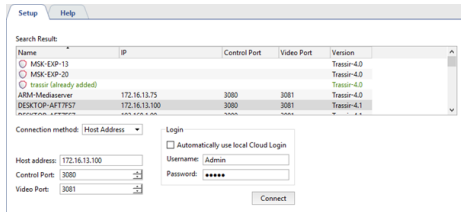
- *Connecting to a new server*
- *Changing the connection settings*

## Connecting to a new server

To add a connection with another server, select **Network** -> **Add** in the system settings.

The right part of the window displays a table with a list of automatically discovered servers on the local network, as well as servers connected to TRASSIR Cloud. Connected servers found in TRASSIR Cloud are marked with .

The table displays the following information: server name, IP address, ports used for control/connection and video transmission, and software version.



Server connection settings are located at the bottom of the window. To fill them in, simply select and click the server to be connected to from the list of available servers. If the desired server is not in the list, you can enter the settings manually.

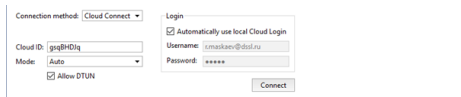
The settings can vary depending on the **Connection method**:

- Through **Host address**:



The DNS name or IP address, which is specified in the **IP address** field, can be used to connect to the server. In addition, the TCP/IP server ports, through which the video will be controlled and transmitted, should be selected in the **Control Port** and **Video Port** fields. You can read about TCP/IP ports settings in the [Local server settings](#).

- Through **Cloud Connect**:



A server identifier, which is created during [server connection to TRASSIR Cloud service](#) is used to connect to the server. The identifier should be entered into the **Cloud ID** field.

You can select one of the methods to provide secure connection:

- Auto** - a data transmission mode, in which the connection stability is provided by TRASSIR Cloud service. In case the direct connection is disabled, TRASSIR cloud will establish a new one, with the help of its services. You can read more about this mode in [Connection through TRASSIR Cloud](#).
- P2P only** - a direct data transmission mode between server and client.

TRASSIR can also use **DTUN(DirectTUNnel)** technique to establish the reliable peer-to-peer connection between client and server. If the **Allow DTUN** flag is checked, TRASSIR will create peer-to-peer connection between client and server, in which the data will be transmitted by UDP protocol.



Not all internet providers support UDP protocol. In this case, **DTUN technique is not recommended for use to connect to the servers using mobile or modem connection.**



Both connection methods require **Username** and **Password**, which are specified in the **Login** area. Each server has its own user list. For this purpose, on server to which the connection is established a user with the specified login and password *should be created*.

In case you don't want to create new users on each connected server, *connect to TRASSIR Cloud service* and check the **Automatically use local Cloud login** flag to use the authorized cloud user rights for connection.

Press **Connect** to establish a new connection and the added server settings tab will be automatically opened. You'll see the **Server certificate fingerprint check dialogue**. The server certificate fingerprint check is required for server authentication. Make sure that the fingerprint matches and press **Continue**.



You can learn the value of a server's fingerprint in the *Server settings* window.

The connection status will change to **Connected**.



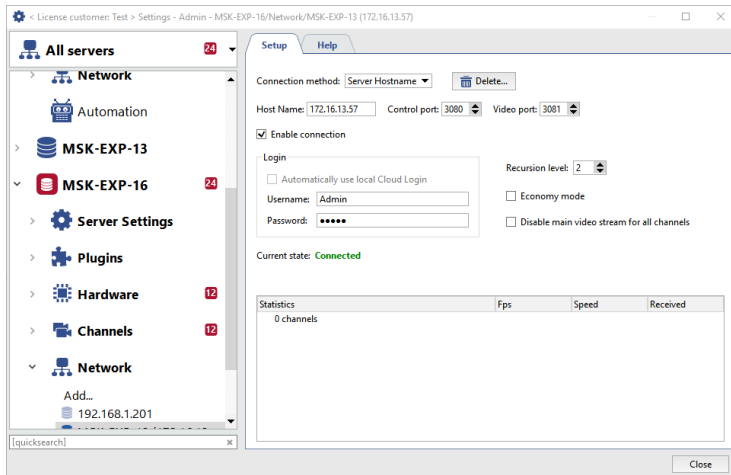
While connecting to TRASSIR server of 3.2 software version you'll see the message **Restricted connection**, the description of which you will find in the section *Restrictions to connection to servers with TRASSIR 3.2 installed*.



- *Network*
- *Changing the connection settings*
- *Connection through TRASSIR Cloud*

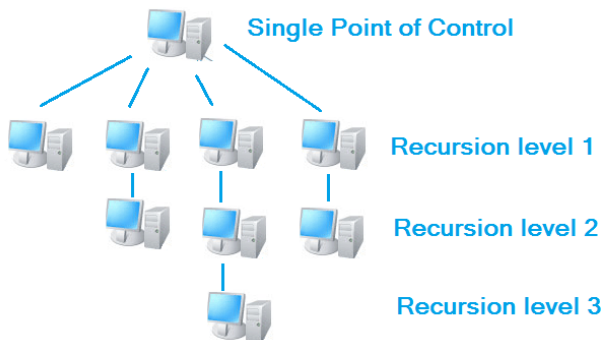
## Changing the connection settings

In order to change server connection settings, selected it the list on the **Network** tab of the settings tree.



On this tab you can change connection settings such as: the server's IP address, the ports used, and the credentials for signing in.

TRASSIR lets you organize video gateways and control servers over network connections nested up to three levels. The maximum nesting depth is determined by the value of the **Recursion level**. In other words, you can connect to a TRASSIR server through an intermediate server rather than connecting directly. **Recursion level** - 1 means that a connection will be made only the server to which you are directly connecting. **Recursion level** - 2 means that a connection will be made to the server to which you are connecting as well as all servers to which it is connected.



**Economy mode** - A special connection mode that reduces network traffic. In this mode, the server transmits the minimum amount of information, including service information.

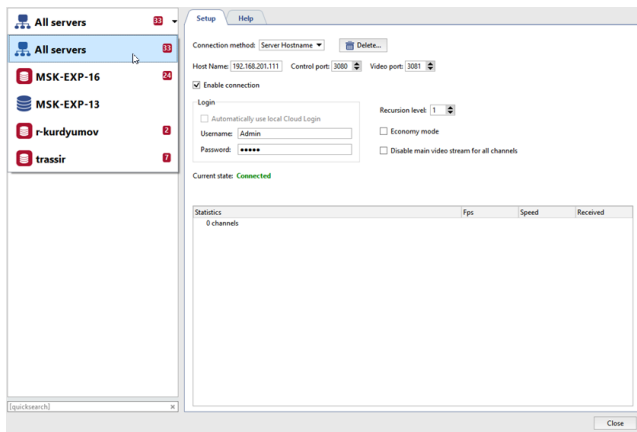
**Disallow main video stream** - Blocks reception of the mainstream from all channels. When viewing a camera's feed the substream will always be displayed, regardless of other TRASSIR settings; and if there is no substream – the number of frames displayed per second will drop to between one and two.

The table displays real-time statistics for the server connection. It includes information about the number of frames per second, the bit rate, and the volume of data transmitted for each channel individually as well as collectively for the server.

Statistics	Fps	Speed	Received
# 3 channels	100.0 fps	807.8 kbps	36.7 Mb
DS-2CD0212-11	0.0 fps	0.0 kbps	0.0 Kb
DS-2CD0834FWD-E1	25.3 fps	542.5 kbps	24.5 Mb
DS-2CD0834FWD-E1	24.7 fps	31.4 kbps	1.6 Mb
DVS Full 1	25.0 fps	15.1 kbps	668.1 Kb
DVS Full 1	25.0 fps	218.7 kbps	10.0 Mb

To disconnect from the server, simply clear the **Enable connection** checkbox. If the server connection is no longer required, you can delete it with the corresponding button.

If a large number of servers are connected to your server, you can only select and display one server in the settings tree. Select **All servers** to display the settings for all connected servers.



- *Network*
- *Connecting to a new server*

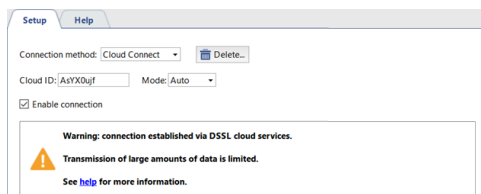


## Connection through TRASSIR Cloud

CloudConnect-connection will be arranged via TRASSIR Cloud service:

- in case TRASSIR is unable to arrange direct CloudConnect-connection with a cloud camera or server within 10 seconds;
- in case any errors have been detected during CloudConnect-connection monitoring, which interfere with the stable data transfer between TRASSIR.

You will see the following message in the settings window:



Restrictions at data transfer by TRASSIR Cloud server:

- Maximum data transfer speed between servers is 10 Mb/sec.
- *Live video view* - 5 minutes.
- *Archive review* - 1 minute.
- *Archive export* maximum length is 10 minutes.
- *Network channels record* is unavailable.



To disable connection via TRASSIR Cloud check **Mode** value **P2P only** setting box.



- *Connecting to a new server*
- *Changing the connection settings*

## Restrictions to connection to servers with TRASSIR 3.2 installed

- Archive of the channels connected to servers with TRASSIR 3.2 is not displayed in the event log *on the same timeline*.
- *Tabs* are not displayed in archive of channels connected to servers with TRASSIR 3.2..
- Simultaneous archive review from several channels is possible only for the channels connected to servers with the same software version.



- *Connecting to a new server*
- *Changing the connection settings*

## Automation

TRASSIR implements a versatile system of [rules](#) and [scripts](#). **Automation** greatly simplifies the work of an operator by configuring responses to interesting- and/or alarm events. You can construct rules using the built-in wizard or independently create individual responses to specific events using the integrated Python script system. On the page entitled [Examples of the rules and scripts](#), you can review real examples of rules and scripts along with corresponding descriptions and explanations.

Automation also lets you create [schedules](#) with three zone types. Schedules can be used, for example, to control camera recording or control arbitrary objects using rules and scripts.

As a response to a system event, you might choose to send an email with information about the event along with screenshots and/or exported video segments from the desired cameras. To do this, in the **Automation** section, [create an email account](#), and select sending email with the created account as the desired response in a rule or script.

Additionally, TRASSIR supports **cyclic view templates**. **Cyclic view templates** lets you open specific views on any monitor's screen in any order using a hotkey. You can create an unlimited number of **cyclic view templates** and run them using F1-F12 and/or an arbitrary combination of modifiers (Ctrl, Shift, Alt) and F1-F12.

## Scripts

Scripts are one of TRASSIR's strong points. Scripts make it possible to automate common operations, simplify an operator's work, and perform integration. What's more, scripts are fun!

Scripts are written in the **Python** language.

- Python is the easiest language to learn and it has a simple [language syntax](#). Moreover, Python is a general language; you aren't limited to a predefined set of functions. You can use it to do whatever you want, i.e. file reading, network communication, etc. For more information, see [python.org](#).
- A script can [read and change TRASSIR settings](#), [invoke objects' methods](#), take screenshots, export video, and [interact with the user](#).
- [Functions activation \(calling\)](#) can be done by various events: by object status change, by button pressing, [via call from context menu](#), [by the event in the log](#), [by AutoTRASSIR event](#), [by ActivePOS event](#), [by timeout](#).
- Thanks to the user-friendly interface you can [set parameters](#) with a script and use [additional resources and libraries](#) in the script itself.
- To protect the script as your intellectual property, it can be [encrypted](#).

Where do you begin?

Start with the examples. The button to load examples is located below the editor. The first four examples are pedagogical; the remaining examples offer various interesting ideas.

You can also begin with the rule editor. Internally, rules work by creating scripts. At the bottom of the editor, there is a button to [copy the script's code to the clipboard](#). The copied code can be pasted into a script and edited.



- [Rules](#)
- [Schedules](#)
- [Adding an email account](#)
- [Examples of the rules and scripts](#)

## Python syntax

Simple examples of language syntax. If you need more complete description of the language, you should refer to [python.org](https://python.org).



Indentation as part of the language. Indentation determines where the body of a loop or function ends.

### Branching:

```
if x+y > 5:
    alert("The sum x + y is enormous!")
elif x<0 or y<0:
    error("Invalid x and y values")
else:
    message("The sum x + y is okay: %i" % (x+y))
```

### Loops:

```
for i in range(5):
    message(i+1)
message("A rabbit went for a walk")

i = 10
while i>=0:
    message(i)
    i -= 1
alert("Start!")
```

### Functions:

```
def f1():
    alert("Function without parameters")

def f2(x, y):
    alert("Function with parameters x=%s, y=%s" % (x,y))
    if x > 5:
        alert("Come on, x is greater than 5!")

f1()
f2(3, 4)
```

### Lists:

```
lst = ["pastries", "ice cream", "cookies"]
lst.append("candies")
for x in lst:
    alert("I want %s!" % x)
lst.pop(1)
lst += ["cucumbers", "tomatoes"]
alert("And %s!" % lst[4])
first = lst[0]
last = lst[-1]
first_three = lst[:3]
last_three = lst[-3:]
middle = lst[2:3]

lst = [x for x in range(1,5)]
squared = [y*y for y in lst]
file = [x.strip() for x in open("readme.txt")]
words = "we use spaces to split a string into words".split(" ")
```

### Strings:

```
x = "Vasily"
y = "Pupkin"
z = x+y
alert(z)
z = " ".join([x,y])
alert(z)
```

### Formatting strings:

```
pi = 3.1415926
alert("PI accurate to 2 decimal places: %0.2f" % pi)
```

```
s = "PI accurate to 3 decimal places: %0.3f" % pi
alert(s)
name = "Vasya"
age = 25
s = "Hi, %s. You're probably %i" % (name, age)
alert(s)
```

### Formatting time:

```
import time
message(time.strftime("%H:%M:%S %d.%m.%Y", time.localtime()))
```

Lambda expressions let you construct a function call using local variables. The function call can then be returned to be used later. This approach is helpful when *interacting with the user* and during *long operations*:

```
def hello(name, answer, correct):
    if answer==correct: message("Correct, %s!" % name)
    else: message("Actually, it's %s!" % correct)
def check_user_math(name):
    ask("Dear %s, what is 5 x 5?" % name,
        lambda x: hello(name, x, "25"),
        lambda: message("Again nobody wants to talk to a robot."))
ask("What's your name?", check_user_math, None)
```

Global variables are easier to understand than lambda expressions:

```
def hello(answer):
    global name
    if answer==25: message("Correct, %s!" % name)
    else: message("Actually, it's 25!")
def check_user_math(n):
    global name
    name = n
    ask("Dear %s, what is 5 x 5?" % name,
        hello,
        None)
ask("What's your name?", check_user_math, None)
```



- [Activation](#)
- [Settings](#)
- [Objects](#)

## Integrated script editor

TRASSIR has an integrated script editor that consists of the following functional areas:

- Script management area

In the **Script name** field, enter the name of the script that will be displayed in the TRASSIR settings.

Set the **Enable script** checkbox to activate the script.

The script may be deleted, if needed. To do this, click the **Delete** button.

The **Run count** and **Error count** fields will respectively show the number of times the script has run and the number of times errors have occurred.

- The script editing area may be displayed in two ways:  
as a script editor:

```
1 # This script reminds about empty administrator password and other
2 # installation problems.
3 #
4 # Disable or delete this script if you're tired of this messages.
5 #
6 ""
7 <parameters>
8 .....<company>DSSL</company>
9 .....<title>Password Reminder</title>
10 .....<version>2.0</version>
11 </parameters>
12 ""
13
14 admin_folder = settings("users/Admin")
15 F10 = "<br><br>" + _("Press <b>F10</b> to turn off this messages")
16
17 def check_admin():
```

as a list of script parameters:

- Additional buttons

Clicking the **Save and Run** button saves the script. Click the **Revert** button to revert any changes made.

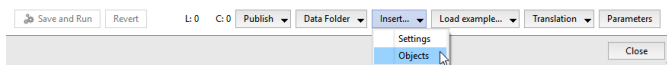
To save the script to a file, click the **Publish** button and select the desired option: in encrypted form - **To file...** or as is **To file (unencoded)...**



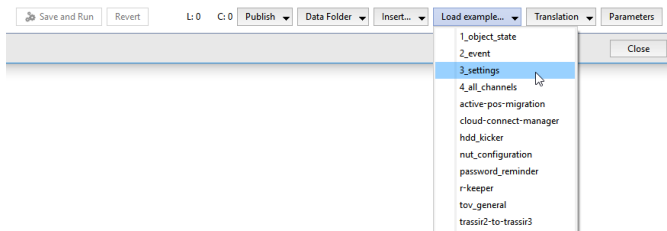
When saved in encrypted form, the text of the script displayed in the editor is encrypted. This feature will help you to protect your intellectual property and to prevent unauthorized changes to the script.

If you need to save data to a folder on the hard drive while a script is running, click the **Data Folder** button and select **Create** to create a folder. To open an existing folder, select **Open**. If you need to insert the path to the folder in the script, then click **Copy path** to copy it to the clipboard.

If you click **Insert...** and select **Settings**, then in the window that opens you can select the setting you want to insert into the script. To insert a method into the script, select **Objects**.



To load a previously saved script or an example script, click the **Load example...** and select **From file...** or the name of the example.

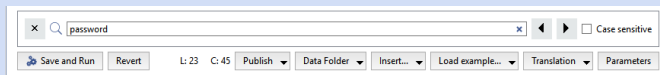


Built-in editor supports multi-language scripts creation. You can create the script interface of which will be displayed same language with TRASSIR or the other language you need. Language file is created using *Qt Linguist* program. You can add new language file, edit existing one, update or select script language pressing **Translation** button and selecting the required operation.

The **Editor** / **Parameters** button switches the script editing area.



To display the search bar, press **CTRL+F**.



The rights of the user Script affect scripts' ability to read and write individual fields in the settings.



If you click **F4** in the settings window, you can bypass the dialog boxes and get into a special mode for changing settings. This mode lets you experiment to see how the system will behave given any particular change to the settings.



- [Activation](#)
- [Settings](#)
- [Objects](#)
- [Parameters and resources in scripts](#)



## Activation

In order to execute a function at the desired time, you must bind it to a system event:

- Activation based on object state:

```
cam1 = object("Camera 1")
def f():
    message("Motion: %s" % cam1.state["motion"])
cam1.activate_on_state_changes(f)
```

- Activation based on changed settings:

```
h = settings("health")
def f():
    message("Database health: %s" % h["db_connected"])
h.activate_on_changes(f)
```

- Activation based on keypresses:

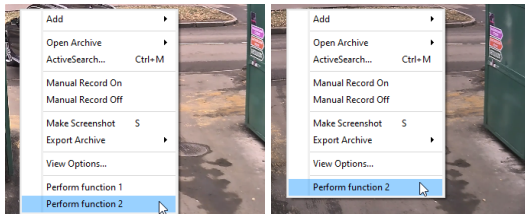
```
def f():
    message("Hello world!")
activate_on_shortcut("F9", f)
```

Only keys F1-F12 and modifiers Ctrl, Alt, and Shift are available for scripts and rules. Joystick buttons also work. Open the rule editor to see the names of keys.

- Activation from the context menu:

```
def func1(guid):
    alert(guid.name)
def func2(guid):
    alert(guid.name)
action1 = activate_on_context_menu("xeLzkjpd", "Perform function 1", func1)
action2 = activate_on_context_menu("Channel", "Perform function 2", func2)
```

Herewith **Perform function 2** item will appear in context menus called on each device of "Channel" class, and **Perform function 1** item - only on one device with GUID "xeLzkjpd".



- Activation based on an event in the log:

```
def f(ev):
    message("Event %s" % ev.type)
activate_on_events("", "", f)
```

Note that the function must have a parameter to pass in the event. For more information, see the **2\_event** example. The button to load examples is located below the code editor.

- Activation based on a timeout:

Sometimes a script needs a delay. The function `time.sleep()` is not appropriate, because causes the program to hang for the specified time. To wait, use `timeout()`. The indicated function will be called after the specified time:

```
def f():
    alert("2 seconds have passed!")
    timeout(3000, g)
def g():
    alert("And another 3!")
    timeout(1000, lambda: h(1,2,3))
def h(param1, param2, param3):
    alert("To continue running after the delay, I need the " +
        "parameters %i, %i, %i" % (param1, param2, param3))
    timeout(2000, f)
```

- Activation based on an AutoTRASSIR event:

```
def f(ev):  
    message("Vehicle with license plate number %s passed" % ev.plate)  
    activate_on_lpr_events(f)
```

- Activation based on an ActivePOS event:

```
def f(ev):  
    if ev.type=="POS_POSITION_ADD":  
        message("%s added to receipt" % ev.text)  
    activate_on_pos_events(f)
```

- Activation on the event of *ArUco Detector*:

```
def f(ev):  
    for detection in ev.detections:  
        message("The following marker has been detected: %s" % detection.decoded_value)  
  
    activate_on_aruco_detection_events(f)
```

To find out what other fields an event holds, it use `dir()`

```
def f(ev):  
    alert( dir(ev) )
```



- *Integrated script editor*

## Working with settings

By changing settings from a script, you can automate almost everything that can be done using a mouse and keyboard in the settings windows (administrator interface).

```
s = settings("ip_cameras/My favorite IP camera")
s = settings("/Different server/ip_cameras/Camera on a different server")
```

The **settings()** function will find the desired settings folder. The folder has values that can be read and written using square brackets.

```
x = s["channel00_fps"]
s["channel01_fps"] = 25
```

The **activate\_on\_changes()** function lets you track changes in the folder:

```
s = settings("channels/Camera 1/stats")
def f():
    alert( s["fps"] )
s.activate_on_changes(f)
```

You can substantially change the server's configuration by working with settings. As an example, use a script to convert TRASSIR 2 settings to TRASSIR 3.



- *Integrated script editor*

## Working with objects

IP-cameras, channels, templates, inputs, outputs, servers, SIMT areas and many other objects are packed together in a tree. Object tree can be seen in operator's interface displaying **Objects tree (CMS)** in the pattern or add to script by pressing the button **Insert -> Objects** in **scripts editor**.

All the objects are combined into classes:

- **Folder** - class of parental objects ("Channels", "IP Devices", "Templates") which own all the other classes;
- **Server** - connected servers class;
- **IP Device** - connected IP-devices class;
- **Channel** - connected channels class;
- **GPIO Input** - alarm inputs class;
- **GPIO Output** - alarm outputs class;
- **OperatorGUI** - operator's interface class;
- **Template** - class of templates.

In order to poll class objects list, one shall call function `objects_list()`.

```
alert(objects_list("Channel"))
```

Message will show massive consisting of "Channel" class objects.

```
[
('AC-D1050 1', 'Qmez0La2', 'Channel', 'p0aDXZdXC'),
('DVS Full 8', 'nBSAqWT1', 'Channel', 'p0aDXZdXC'),
('DVS Full 1', 'xeLzkjpd', 'Channel', 'p0aDXZdXC')
]
```

In the given example the answer contains:

- **'AC-D1050 1'** - object name;
- **'Qmez0La2'** - unique guid of the object;
- **'Channel'** - object class;
- **'p0aDXZdXC'** - parental guid of the object which given object belongs to.

In addition, each object has status and methods, that is functions which can be called.

Finding an object in a script is easy:

```
obj = object("Camera 1")
```

Call the `state()` function to find out an object's state. Each object has several states (a state vector). For example, a channel has states for "motion", "signal", "recording", and "recording\_on\_device".

```
m = obj.state("motion")
if m=="No Motion":
    alert("No motion")
```

To find out what states an object has, call `state()` with a random string. When the statement is executed, the error text will contain the names of the elements in the state vector.

To learn about state changes, use **activation based on changed state**:

```
cam1 = object("Camera 1")
def f():
    message("Motion: %s" % cam1.state["motion"])
cam1.activate_on_state_changes(f)
```

In addition to its state, you can learn an object's name, identifier, and class.

```
alert(obj.name)
alert(obj.guid)
alert(obj.class_name)
```

List of methods can be also received using `dir()` function which outputs the contents of any structure in Python.

```
alert(dir(obj))
```

### "Channel" class object methods

```
cam1 = object("Camera 1")
```

- Start channel archive record

```
obj.manual_record_start()
```

- Stop channel archive record

```
obj.manual_record_stop()
```

- Receive PTZ camera position

```
obj.ptz_position_query()
```

Values are saved in camera settings:

```
settings("channels/[GUID_channel]/ptz/current_pan")
settings("channels/[GUID_channel]/ptz/current_tilt")
settings("channels/[GUID_channel]/ptz/current_zoom")
```

- Move PTZ camera for presetting [preset]

```
obj.ptz_preset([preset])
```

- Start record

```
obj.record(True or False)
```

- Stop archive manual record

```
obj.record_off()
```

- Start channel archive manual record

```
obj.record_on()
```

- Save screenshot

```
obj.screenshot()
```

- Save screenshot from archive

```
obj.screenshot_ex("[timestamp]", "[directory]")
```

[timestamp] - time of the frame from archive;

[directory] - directory on the server where screenshot is saved.

- Save screenshot from archive

```
obj.screenshot_v2("[time]", "[filename]", "[directory]", [make_thumb])
```

[time] - time of the frame from archive;

[filename] - name of the screenshot being saved;

[directory] - directory on server where screenshot is saved;

[make\_thumb] - create thumbnail (0 - no).

- Add text to video

```
obj.set_watermark("[text]", [text_pos], [time_pos])
```

[text] - user-defined text;

[text\_pos] and [time\_pos] - text and time location angle: 1-upper left, 2-upper right, 3-lower left, 4-lower right.

- Main/additional stream export from the channel archive

```
obj.export_archive("[start_time]", "[end_time]", "[filename]", "[options]")
```

[start\_time] and [end\_time] -start and end time of the exported fragment of the archive in the format YYYYMMDD\_HHMMSS;

[filename] - name of the saved file;

[options] - additional options transmitted in the format "name" : value:

- "is\_hardware" - export archive from the device (0 - no)
- "want\_ss" - export additional stream (0 - no)
- "video\_codec" - recode video in codec ("MPEG4" or "WMV")
- "video\_bitrate" - recode using bitrate (value in Kbit/s)
- "video\_resolution" - resample video ("2560x1920", "2048x1536", "1920x1080", "1600x1200", "1280x1024", "1280x960", "1280x720", "1024x768", "800x600", "720x576", "704x576", "640x480", "352x288", "320x240", "176x144")
- "audio\_codec" - codec for audio ("PCM")
- "audio\_bitrate" - bitrate for audio (64, 128) Kbit/s
- "need\_channel\_name\_watermark" - enter channel name to video (0 - no)
- "need\_timestamp\_watermark" - insert to video shooting time (0 - no)
- "need\_fliprotate" - use image angling settings from the channel (0 - no)
- "watermark\_need\_figures" - add figures (0 -no)
- "watermark\_align" - inserted text location (1 - at the upper left, 2 - at the upper right, 3 - at the lower left, 4 - at the lower right)

### "Operator's interface" class object methods

```
obj = object("Operator's interface maskaev-pc")
```

- Main/additional stream export from the channel archive

```
obj.archive_export("[channel]", "[start_time]", "[end_time]", "[filename]", [on_device])  
obj.archive_export_ss("[channel]", "[start_time]", "[end_time]", "[filename]", [on_device])
```

[channel] - channel name or its GUID;

[start\_time] and [end\_time] -beginning and end time of the exported archive segment;

[filename] - name of the saved file;

[on\_device] - archive export from the device (not 0).

- Open channel archive

```
obj.archive_open_inplace("[channel]", "[start_time]")
```

[channel] - channel name or its GUID;

[start\_time] - positioning time.

- Add channels to monitor

```
obj.assign_channels("[csv_channels]", [monitor_n])
```

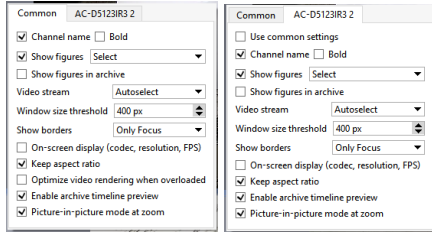
[csv\_channels] - list pf channels separated by commas;

[monitor\_n] - monitor number.

- Change settings of the camera window view same way as in the view settings window.

```
obj.change_view_settings("[name]", "[value]")
```

[name] - settings name:



```
"opts_[GUID_channel]_use_common"
"opts_[GUID_channel]_figures_on"
"opts_[GUID_channel]_figures_mode"
"opts_[GUID_channel]_border_mode"
"opts_[GUID_channel]_keep_ratio"
"opts_[GUID_channel]_show_osd"
"opts_[GUID_channel]_show_channel_name"
"opts_[GUID_channel]_show_channel_bold"
"opts_[GUID_channel]_switch_to_ss_pixels"
"opts_[GUID_channel]_turtle_enable"
```



In case you need to change the view settings of all the cameras, then, instead of [GUID\_channel] use common.

For example:

```
obj = object("Operator's interface maskaev-pc")
obj.change_view_settings("opts_common_figures_on", "1")
obj.change_view_settings("opts_common_figures_mode", "3")
obj.change_view_settings("opts_syQURNtf_show_osd", "1")
obj.change_view_settings("opts_syQURNtf_show_channel_name", "0")
```

[value] - setting value.

- Switch economy mode on/off

```
obj.eco_start("[channel]", [monitor_n])
obj.eco_stop("[channel]", [monitor_n])
```

[channel] - channel name or its GUID;

[monitor\_n] - monitor number.

- Activate/deactivate PTZ-camera control

```
obj.ptz_start("[channel]", [monitor_n])
obj.ptz_stop("[channel]", [monitor_n])
```

[channel] - channel name or its GUID;

[monitor\_n] - number of monitor to control PTZ-camera.

- Control PTZ-camera

```
obj.ptz_focus_auto("[channel]", [monitor_n])
obj.ptz_iris_auto("[channel]", [monitor_n])
obj.ptz_set_coordinates("[channel]", [monitor_n], [pan], [tilt], [zoom])
obj.ptz_set_focus("[channel]", [monitor_n], [speed])
obj.ptz_set_iris("[channel]", [monitor_n], [speed])
obj.ptz_set_zoom("[channel]", [monitor_n], [speed])
obj.ptz_start("[channel]", [monitor_n])
obj.ptz_stop("[channel]", [monitor_n])
obj.ptz_turn_x("[channel]", [monitor_n], [speed_pan])
obj.ptz_turn_y("[channel]", [monitor_n], [speed_tilt])
```

[channel] - channel name or its GUID;

[monitor\_n] - number of the monitor to control PTZ-camera;

[pan], [tilt], [zoom] - tilt coordinates (fractional);

[speed], [speed\_pan], [speed\_tilt] - tilt rate (integral).

- Show monitor on top of all windows

```
obj.raise_monitor([monitor_n])
```

[monitor\_n] - monitor number.

- Save screenshot from archive

```
obj.screenshot("[channel]", "[time]", "[filename]")
obj.screenshot_ex("[channel]", "[time]", "[filename]", "[directory]", [make_thumb])
```

[channel] - channel name or its GUID;

[time] - time of the frame from archive;

[filename] - name of the screenshot being saved;

[directory] - directory on server where screenshot is saved;

[make\_thumb] - create thumbnail (0 - no).

- Show channel or template on display

```
obj.show("[name]", [monitor_n])
obj.show_channel("[name]", [monitor_n])
obj.show_template("[name]", [monitor_n])
obj.show_template_by_guid("[name]", [monitor_n])
```

[name] - name of channel or template;

[monitor\_n] - monitor number.

- Show channel archive on monitor or in the template

```
obj.show_archive("[name]", [monitor_n], "[start_time]", "[end_time]")
```

[name] - name of channel or template;

[monitor\_n] - monitor number;

[start\_time] and [end\_time] - archive fragment start and end time.

- Show html-page on the monitor or in the template

```
obj.show_html("[source]", "[url]")
obj.show_html_on_monitor([monitor_n], "[source]", "[url]")
obj.show_html_on_template([monitor_n], "[name]", "[source]", "[url]")
```

[monitor\_n] - monitor number;

[name] - template name;

[source] - minibrowser's identifier;

[url] - displayed HTML-page address.

- Update current screen

```
obj.update_active_monitor([csv_channels])
```

[csv\_channels] - list of channels separated by comma.



- *Integrated script editor*



## Interacting with the user

Ask a user to enter a string with the `ask()` function

```
def hello(n):  
    message("Hello, %s!" % n)  
def fail():  
    alert("The operator refuses to respond!")  
ask("What is your name?", hello, fail)  
ask("What is your name?", hello, fail, 60, "Vasily")
```

Upon completion the dialog will call one of the function. The first one should have a parameter which contains a response to the question. The other one will be called if the "Cancel" button or Esc is pressed. The timeout period, after which the window will be closed, can be specified in seconds. You can also specify the initial string.

Ask to select one of several options using the `question()` function

```
def yes(): message(1)  
def no(): message(2)  
def dont_know(): message(3)  
def other(): message(4)  
question("Have you been drinking cognac in the mornings for a long time?",  
        "Yes", yes,  
        "No", no,  
        "I don't know", dont_know,  
        "Other", other,  
        60)
```

There should be several buttons in the response. The first button is a default one, which is selected by pressing "Enter". You can specify the timeout period, after which the first option will be selected.



You can see more extended example of a dialog with the user in the **tov\_general** script, by uploading it to the built-in [script editor](#).

## Events in scripts

To subscribe to the events in the system log, use `activate_on_events()`

```
def f(ev):
    message("Event %s" % ev.type)
    activate_on_events("", "", f)
    activate_on_events("Motion Start", "", f)
    activate_on_events("", "Camera 1", f)
```

The first parameter can be an event type filter. You can view the possible event types in the rule editor. The second parameter can be a name filter or object identifier. Both filters can be passed together.

An event contains an event type, time, event source object, as well as the parameters p1, p2, and p3.

```
def f(ev):
    message("Event %s" % ev.type)
    message("Object identifier: %s" % ev.origin)
    message("Object name: %s" % ev.origin_object.name)
    message("Time: %s" % time.strftime("%H:%M:%S %d.%m.%Y",
        time.localtime(ev.ts/1000000)))
    activate_on_events("", "", f)
```

You can work with the `origin_object` just *like any other object*.

The values of p1, p2, and p3 depend on the event type. For example, the "Login Successful, %1 from %2" event has two parameters which can be found in p1 and p2.

## Parameters and resources in scripts

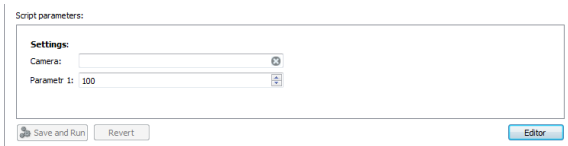
To create a parameter block in a script and/or add additional resources to a script, insert the following block at the beginning of the code:

```
"""
<parameters>
  <company>My Company</company>
  <title>My Script</title>
  <version>1.0</version>

  <parameter>
    <type>caption</type>
    <name>Settings</name>
  </parameter>
  <parameter>
    <type>channel</type>
    <id>param_channel_1</id>
    <name>Camera</name>
    <value></value>
  </parameter>
  <parameter>
    <type>integer</type>
    <name>Parametr 1</name>
    <id>param_1</id>
    <value>100</value>
    <min>1</min>
    <max>100000</max>
  </parameter>

  <resources>
    <resource>httpserver.py</resource>
    <resource>index.html</resource>
  </resources>
</parameters>
"""
```

The parameter tab in the script editor will look like this:



After that, the parameter value specified in the **value** tags can be used in the script using the parameter identifier specified in the **id** tags:

```
def f():
    message("Camera %s" % param_channel_1)
    message("Parametr 1 = %s" % param_1)
f()
```

The following values may be used as the parameter type specified in the **type** tags:

- **caption** - A name (for example, the name of a group of parameters)

```
<parameter>
  <type>caption</type>
  <name>Settings</name>
</parameter>
```

- **integer** - An integer

```
<parameter>
  <type>integer</type>
  <name>Parametr 1</name>
  <id>param_1</id>
  <value>100</value>
  <min>1</min>
  <max>100000</max>
</parameter>
```

- **float** - A real number

```
<parameter>
```

```
<type>float</type>
<name>Parametr 1</name>
<id>param_2</id>
<value>6.00</value>
<min>1.00</min>
<max>10.00</max>
</parameter>
```

- **string** - A string (for example, a template name)

```
<parameter>
  <type>string</type>
  <name>Template to generate current report</name>
  <id>tpl_for_events</id>
  <value>AutoTRASSIR</value>
</parameter>
```

- **boolean** - A logical expression

```
<parameter>
  <type>boolean</type>
  <id>autoupdate_events</id>
  <name>Autoupdate of measurements</name>
  <value>0</value>
</parameter>
```

- **date** - A date

```
<parameter>
  <type>date</type>
  <id>date_start</id>
  <name>Start date</name>
  <value>2014-03-01</value>
</parameter>
```

- **time** - Time

```
<parameter>
  <type>time</type>
  <id>time_start</id>
  <name>Start time</name>
  <value>10:00:00</value>
</parameter>
```

- **string\_list** - A comma-separated value list

```
<parameter>
  <type>string_list</type>
  <id>cams</id>
  <name>Cameras</name>
  <value>cam1,cam2,cam3</value>
</parameter>
```

- **string\_from\_list** - A list of values to choose from

```
<parameter>
  <type>string_from_list</type>
  <id>user_function</id>
  <name>User function</name>
  <value>U1</value>
  <string_list>U1,U2,U3,U4,U5,U6,U7,U8,U9,U10</string_list>
</parameter>
```

- **channel** - A field to select one of the channels connected to a TRASSIR server

```
<parameter>
  <type>channel</type>
  <id>channel_id</id>
  <name>Camera</name>
  <value></value>
</parameter>
```

- **objects** - A field for selecting TRASSIR objects

```
<parameter>
  <type>objects</type>
  <id>objects_id</id>
```

```
<name>Objects</name>
<value></value>
</parameter>
```

- **server** - A field for selecting a TRASSIR server

```
<parameter>
  <type>server</type>
  <id>server_id</id>
  <name>Server</name>
  <value></value>
</parameter>
```

In the **resources** tags, specify the relative path to the file that will be run together with the script.

## Using ActivePOS in scripts

The `activate_on_post_events()` function is used to get ActivePOS events

```
import time
def f(ev):
    message("Unique event number: %s" % ev.op_id)
    message("Event type: %s" % ev.type)
    message("Terminal ID: %s" % ev.pos_terminal)
    message("Terminal name: %s" % ev.pos_terminal_name)
    message("Associated video channel: %s" % ev.associated_channel)
    message("Flags: %s" % ev.flags)
    message("Position number: %s" % ev.position)
    message("Text: %s" % ev.text)
    message("Price per unit: %0.2f" % (ev.price/100.0))
    message("Weight: %0.3f" % (ev.weight/1000.0))
    message("Quantity: %s" % ev.quantity)
    message("Article: %s" % ev.article)
    message("Barcode: %s" % ev.barcode)
    message("Location: %s" % ev.location)
    message("Time of arrival on server: %s" %
            time.strftime("%H:%M:%S %d.%m.%Y",
                time.localtime(ev.ts_received/1000000)))
    message("Time indicated on receipt: %s" %
            time.strftime("%H:%M:%S %d.%m.%Y",
                time.localtime(ev.ts_in_receipt/1000000)))
activate_on_pos_events(f)
```

The price is given in whole numbers in pennies, and the weight is given in grams. The reception time of the message may differ from the time recorded on the point-of-sale terminal. The reception is used to find the required moment in a video archive, while the time on the monitored cash register is used for searching.

A script can find suspicious situations. You can use the `pos_fraud()` function to attract the operator's attention and record an alarm event on a receipt. You can create a filter to search and highlight based on the presence of such event in a receipt.

```
import time
def f(ev):
    if time.localtime().tm_hour < 23: return
    if ev.type!="POS_POSITION_ADD": return

    u = ev.text.decode("utf-8").upper().encode("utf-8")
    for w in ["BEER", "WINE", "VODKA", "COGNAC"]:
        if u.find(w) != -1:
            pos_fraud(ev, "Alcohol after 11pm")
            return

activate_on_pos_events(f)
```

The `upper()` function converts a string to uppercase (all capital letters). In order for the conversion to work, the string must be in the Unicode (strings in TRASSIR are encoded in UTF-8).



- [ActivePOS - Point-of-sale operations monitoring](#)
- [DSSL XML for ActivePOS](#)
- [Examples of the rules and scripts](#)

## Using AutoTRASSIR in scripts

To respond to AutoTRASSIR events use the `activate_on_lpr_events()` function

```
def f(ev):
    message("Unique event number: %s" % ev.id)
    message("Number: %s" % ev.plate)
    message("Recognition confidence: %s" % ev.quality)
    message("Country: %s" % ev.country)
    message("Template: %s" % ev.tpl)
    message("Time of entry into frame: %s" % ev.time_enter)
    message("Time of best view: %s" % ev.time_bestview)
    message("Time of departure from frame: %s" % ev.time_leave)
    message("Channel identifier: %s" % ev.channel)
    message("Server identifier: %s" % ev.server)
    message("Speed (if using radar): %s" % ev.radar_speed)
    message("Found on lists: %s" % ev.found_on_lists)
    message("Flags: %x" % ev.flags)
activate_on_lpr_events(f)
```

You can apply bitwise logic to the flags using "&" and the `LPR_*` constants.

```
def f(ev):
    message("Vehicle license plate number: %s" % ev.plate)
    if ev.flags & LPR_UP: message("Heading up from the camera")
    if ev.flags & LPR_DOWN: message("Heading down from the camera")
    if ev.flags & LPR_BLACKLIST: message("On the blacklist")
    if ev.flags & LPR_WHITELIST: message("On the whitelist")
    if ev.flags & LPR_INFO: message("On the informational list")
    if ev.flags & LPR_EXT_DB_ERROR: message("External database error")
    if ev.flags & LPR_CORRECTED: message("Number corrected by operator")
activate_on_lpr_events(f)
```

## Rules

The rule creation wizard is designed to easily construct rules in the TRASSIR video surveillance system. It makes it possible to specify the desired response to any particular event in the system, with just a few clicks and without the need to go deeply into the [script system](#).

Every rule consists of an **activation** and an **action**. Rules can also include one or more **conditions**.

**Activation** - This is the event that triggers execution of the rule. The following **activation** types are available:

1. **On event** - The rule will be executed when the specified event is sent from any object. You can specify one or more event types that will execute the rule. You can also use the **Filter** link to select specific objects whose events will execute the rule.

2. **On hotkey** - The rule will be executed when the operator presses a hotkey. For example:

3. **On schedule** - Makes it possible to execute a rule at the specific time. The [schedule](#) should be created before the rule.

4. **On state change** - The rule will be executed when the state of a specific object changes. For example, when a channel's state changed.

5. **On settings change** - The rule will be executed upon any system settings change, for example if the FPS for some card or IP device is changed:

A rule can perform up to five **Actions** as a response to an event-activator. You can add the following actions:

1. **Wait** - Specifies a wait time between actions. You can also choose to make the first action a wait; then the rule will be run with the delay. The wait is given in seconds; the maximum wait time is 24 hours (86,400 seconds):

2. **Call method** - Controls objects in the system. For example, you can enable continuous recording on one of the channels:

3. **Play sound** - Plays one of the preinstalled audio files.

4. **Change settings** - Changes the settings for one of the objects in the system. For example, you can change the FPS for one of the channels:

5. **Export video** - Exports a video from the archive of the selected camera for n seconds from the present moment.



6. **Save frame** - take a screenshot n seconds before, for the selected camera.

7. **Send email** - Sends an email to the specified address. A configured [email account](#) is required for this action. You can briefly describe the event in the **Subject** field. In the body of the email, describe the situation in more detail along with potential ways to resolve it. If previous **Actions** included exporting an archive, the exported file can be attached to the email.

8. **Send SMS** - Sends a text message with the notification. This functionality is not currently supported.

**Condition** - This is a logical expression that can be used to give the rule a specific, narrow range of operation. The values of settings or object states can be used as conditions. For each specific activation type, you can assign a name and/or unique sender ID (GUID). You can also specify a specific event type if several different event types were used as the activator. For example, if the rule should only run during specific hours, you can create an appropriate schedule and indicate the required schedule state in the conditions:

There is no limit on the number of conditions allowed and you can connect them with the conjunctions **and** and **or**. **and** means the rule will be run when both conditions are satisfied. **or** means the rule will be run when at least one of the conditions is satisfied. You can combine both types of conjunctions in the desired order, for example Condition1 **and** Condition2 **or** Condition3 **and** Condition4. In this case, the rule will be run when conditions 1 and 2 are satisfied OR conditions 3 and 4 are satisfied.

The following is an example of a condition with the conjunction **and**. The rule will be activated when all four channels change to "No signal". According to the condition, the rule will only be run if all four channels have the state "No signal".

Here is an example of a condition with the conjunction **or**. The activator of this rule is the "Health Turns Bad" event. According to the condition, the rule will only run if the event was caused by a disk error or a loss of the database connection.

Below is an example of a condition with the conjunctions **or** and **and**. The rule will be activated if the specific combinations of channels change to "No signal". According to the condition, the rule will only run if the first and second channels simultaneously have "No signal" or if the third and fourth channels simultaneously have "No signal".

**Activation on state change**

Please, select objects:

Objects: | AC-D2103IR3 2; AC-D5123IR3 2; AC-D7121IR1v2 2; AXIS 233D 2

**Condition**

☒ AND ☐ OR

☐ AND ☒ OR

☒ AND ☐ OR



- [Scripts](#)
- [Schedules](#)
- [Adding an email account](#)
- [Examples of the rules and scripts](#)

## Schedules

Each schedule can have three types of zones: green, red, and blue. The zones can be arbitrarily interleaved one after another. There can be any number of zones.

You can create the required number of schedules on a server and then automate the server by using rules to apply the schedules to TRASSIR objects.

To create a new schedule:

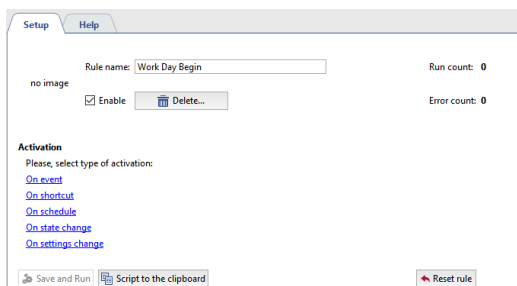
1. Open the **Settings** window.
2. Select **Automation**.
3. Click the **Create new schedule...** link.
4. Name a schedule.
5. Set the **Snap to 30 minutes** checkbox if you want the schedule divided into 30-minute zones. If this checkbox is cleared, the schedule will not be divided and the actual zone size will be determined by highlighting an area with the mouse.  
Regardless of the checkbox's state, you can manually correct the beginning and ending of a zone using the "from" and "to" fields.
6. Divide the days of the week and each day itself into zones. To create a zone:
  - Use the mouse to select a rectangular area;
  - If necessary, manually correct the zone's temporal boundaries;
  - Click the zone fill button.
7. Set the **Enable schedule** checkbox. If a schedule is disabled, then the system will not generate events when the schedule enters any given zone. Therefore, the schedule will not work.

Once a schedule has been created, it can be used, for example, to enable and disable video camera recording. Moreover, one schedule can be used to control an arbitrary number of objects (not only cameras). To use a schedule, create a rule with the "On schedule" activation type and define the actions to be executed when the schedule enters the various zones.

For example: A camera records a facility during nonworking hours (at night). We need to stop recording the camera when the workday begins.

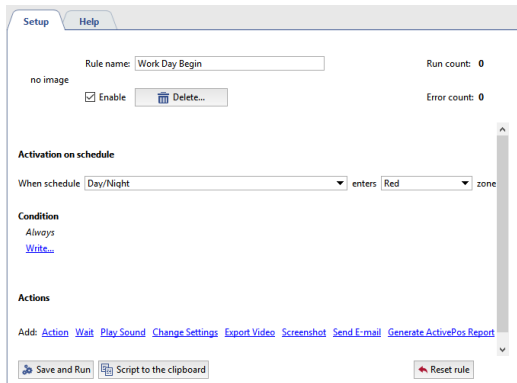
To use a schedule:

1. Create a new schedule in accordance with the previously described procedure.
2. In the **Settings** window, select **Scripts**.
3. Click the **Create new rule...** link.
4. Give the rule in name and select the "On schedule" activation type.

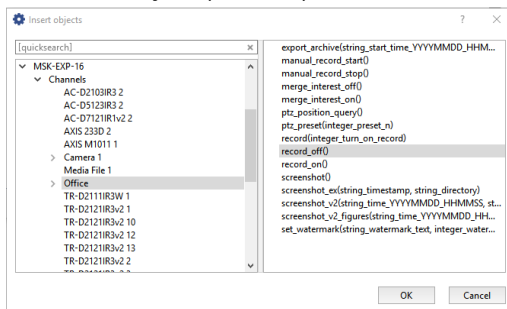


5. Select the previously created schedule from the **When schedule** list and select the zone that, when entered, should trigger execution of the action.

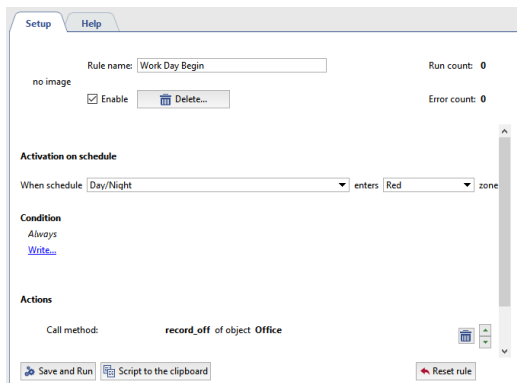
6. If necessary, specify condition for the execution of the rule, or leave the default value (the rule will always be executed when the schedule enters the specified zone).
7. In the list of possible actions, click the **Call method** link.



8. Select an object (camera) and action to be executed (record\_off).

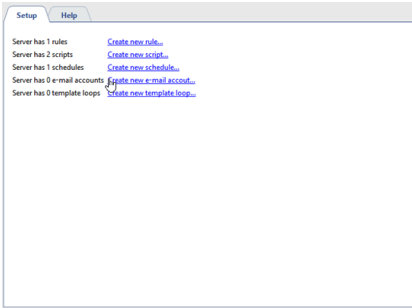


9. Verify that the rule has been correctly constructed and click **Save and run**. The rule will be active in the system, and recording will be disabled for the Lancam-CD812 camera when the schedule enters the specified zone.



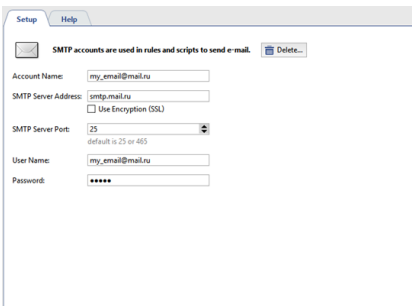
## Adding an email account

To add an account, open the settings and select **Automation**. Then click **New email account**



Specify the following information in the account settings:

1. **Account name** - Can be anything. For convenience, you can enter the full email address.
2. **SMTP server address** - Specify the address of the SMTP server used by the account. For example, for the email address my\_email@mail.ru, the SMTP server is "smtp.mail.ru".
3. **SMTP port** - The port used by the SMTP server. You can find out what the port is on the help page for the email account.
4. **Username** - Specify the username for authentication on the SMTP server. For a mail.ru account, the username matches the full email address, e.g. "my\_email@mail.ru" in our example.
5. **Password** - Specify the password for authentication on the SMTP server. This is the password used to sign into the email account through its web interface.



- [Rules](#)
- [Scripts](#)
- [Schedules](#)
- [Examples of the rules and scripts](#)

## Examples of the rules and scripts

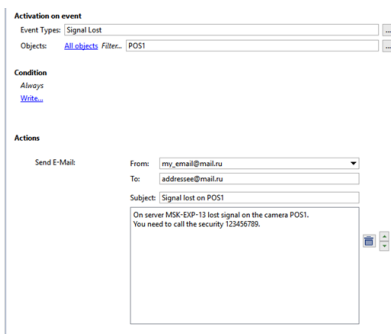
This section presents examples of the most popular rules and scripts. These real examples will help you understand how TRASSIR is automated and let you automate your own video surveillance system. Each example includes a description and an explanation of how the rule/script might be used.

## Rules

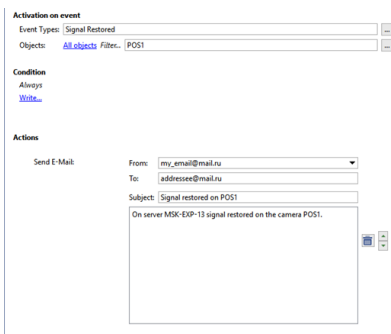
### Sending email upon loss of a camera's signal

This example considers a rule designed to quickly report server problems, in particular the lack of a signal from one of a system's high priority cameras: When the signal from the selected camera is lost, and email notification of the event will be sent.

1. Beforehand, you should create an [e-mail account](#). After that, [Create a new rule](#) and choose **On Event** activation. Find the **Channel** in the opened window and check the **Signal Lost** box.
2. After that select the events of objects, on which the rule will be activated. To do this, click **Filter** and select the required camera in the object list. In this case, this camera is called "Warehouse".
3. Then click **Send email** - the email template window will open. You'll get the following message as a result:



The following image depicts an example of a rule with the opposite behavior: in this case, if the "Warehouse" camera's signal is restored, an email will be sent reporting that the camera's signal has been restored.



Below is an example of a script with extended functionality: An email will be sent when any camera's signal is lost, and the email will indicate the name of the corresponding channel:

```
def send_message(event):
    message_text = '''The server [server name] has lost the signal to camera "%s".\
    Call security at 123456789.'''\
    % event.origin_object.name
    send_mail_from_account("sender@mail.ru", ["addressee@mail.ru"],\
    "Email subject: No signal from camera '%s'" % event.origin_object.name,\
    message_text, [])

    activate_on_events("Signal Lost", "", send_message)
```

### Displaying a camera in fullscreen mode when motion is detected

In this example we consider a rule designed to attract the operator's attention to those cameras for which the very presence of motion is an alarm event: when motion occurs on the specified camera, it will expand to fullscreen on the selected monitor.

1. You must first enable generation of motion events on the desired camera. To do this, go to the **Channels** section of the server settings, select the desired **channel** and place a checkmark in the **Generate motion events** checkbox. Motion events will then begin to be recorded in the event log for the given channel.
2. Next [create a new rule](#) and select the **On event** activation type. In the window that opens, find the **Channel** section and put a checkmark in the **Motion detected** checkbox.

- Then you must determine the objects whose events the rule will respond to. To do this, click the **Filter** link in the rule window and select the desired camera. In our example, this camera is named "Cold store".
- Next click the **Invoke action** link. In the window that appears, select the **Operator [server name]'s interface** section on the left and the **show\_channel** line on the right. You will then be able to specify the channel and monitor in the rule.

The screenshot shows a rule configuration window with the following sections:

- Activation on event:** Event Types: Motion Start; Objects: All objects Filter... Camera 1
- Condition:** Always; [Write...](#)
- Actions:** Call method: show\_channel of object operator via transir. Below this, there are input fields for channel name (Camera 1) and monitor n (1).

Below is an example of a script with extended functionality: any camera where motion occurs will go fullscreen on a second monitor. To do this, set the **Generate motion events** checkbox in the settings for the desired channels. Then create a new script and insert the following code:

```
def show_channel_with_motion(event):
    object("Operator [server name]'s interface").\
    show_channel(event.origin,2)

activate_on_events("Motion Start", "", show_channel_with_motion)
```

### Play a sound when an alarm input is tripped

In this example we consider a rule designed to attract the operator's attention to an alarm situation by playing an audio file. According to the example, when an alarm input is tripped, an audio notification will play. You can use an alarm input to monitor, for example, a door, window, or various sensors.

- Create a new rule** and select the **On event** activation type. In the window that opens, find the **GPIO input** section and put a checkmark in the **Signal on input loss** checkbox.
- Then click the **Filter** link and, in the object list, select the alarm input that interests you. In our example, this object is named "West exit (door)".
- Then click the **Play sound** link and, in the dropdown list, select one of the preinstalled sounds.

The screenshot shows a rule configuration window with the following sections:

- Activation on event:** Event Types: Input High to Low; Objects: All objects Filter...
- Condition:** Always; [Write...](#)
- Actions:** Play sound: C:\DSS\Trasir-4.0-611\sounds\alarm.wav

Below is an example of a rule with opposite activation: in this case, if the alarm input is closed, then an audio file will be played to notify the operator that the door of the west exit has been closed.

The screenshot shows a rule configuration window with the following sections:

- Activation on event:** Event Types: Input Low to High; Objects: All objects Filter... Input 1
- Condition:** Always; [Write...](#)
- Actions:** Play sound: C:\DSS\Trasir-4.0-611\sounds\bell.wav

### Increasing the FPS on a camera when the state of an Orion device changes

In this example we consider a rule designed to increase the detail of a video sequence when an alarm situation occurs, for the purpose of a subsequent in-depth analysis. According to the rule, when the state of an Orion workstation device changes, the FPS of one of the cameras will increase.

- Create a new rule** and select the **On state change** activation type. In the window that opens, find the **Orion** and put a checkmark in the checkbox for the desired device.



- Then click the **Change settings** link. In the **Insert settings** window, expand the **IP devices** section and select the desired IP device. Select the **channel00\_fps** string. Then select the desired number of frames per second in the window that appears.

Activation on state change

Please, select objects:

Objects: Door 1 - Sensor 1; Door 1 - Sensor 2

Condition

Always

Write...

Actions

Change setting: ip\_cameras/Auto Cam#1/channel00\_fps

25

Below is an example of a script with extended functionality. According to the example, when the state of an Orion workstation device changes, the FPS will increase for all cameras.

```
def set_fps_on_all_devices(fps):
    for d in settings("ip_cameras").ls():
        if d.type != "Grabber": continue
        for c in range(0, 16):
            d["channel%02d_fps" % c] = fps
    for b in settings("boards").ls():
        for i in range(0, 16):
            b["channel%02d_fps" % i] = fps

def condition():
    if object_shlp127.state("state") == "Alarm":
        set_fps_on_all_devices(25)
    elif object_shlp127.state("state") == "Armed":
        set_fps_on_all_devices(12)

object_shlp127 = object("Alarm Circuit 1, Device 127")
object_shlp127.activate_on_state_changes(condition)
```

### Send an email when a server's health metric changes

This example considers a rule which says that when the database is disconnected and/or there are disk errors on the server, an email notification will be sent.

- First it is necessary to create an **email account**. Next **add new rule** and select **By event** activation type, find **Server** in the appeared window and check the box **Server health turns bad**.
- As a next step press **Filter** and check the box of the required server in **Object** window.
- To ensure that the letters are sent only in case data base disconnection and/or under disk errors, the appropriate **conditions** shall be provided:
  - Find the **Health** section and select the **disks\_error\_count** string. Then specify a value for the disk\_error\_count parameter by entering " == 1" in the text field, without quotation marks.
  - Find the **Health** section and select the **db\_connected** string. Then specify a value for the db\_connected parameter by entering " == 0" in the text field, without quotation marks.

Select the conjunction **or** between each condition.
- After that press **Send email** and the form to create letter template will appear. In the result you shall have the rule of approximately as follows:

**Activation on event**

Event Types: Health Turns Bad

Objects: All objects Filter... MSK-EXP-16

**Condition**

`settings["health"]["disk_error_count"] == 1` Insert

☐ AND ☒ OR

`settings["health"]["db_connected"] == 0`

+ Add condition

**Actions**

Send E-Mail

From: my\_email@mail.ru

To: addressee@mail.ru

Subject: Health turns bad

Health turns on server MSK-EXP-16 bad.  
We recommend to find the cause of the fail and fix it to avoid data loss.

Below is a rule that says that when the server's state changes to normal, and email notification reporting this fact will be sent.

**Activation on event**

Event Types: Health Turns Good

Objects: All objects Filter... MSK-EXP-16

**Condition**

Always

[Write...](#)

**Actions**

Send E-Mail

From: my\_email@mail.ru

To: addressee@mail.ru

Subject: Health turns good

Health turns on server MSK-EXP-16 good.  
In case this happened without user intervention, we recommend to identify the cause of the failure and fix it.

### Enabling continuous recording when a SIMT border is intersected on a weekend

This example considers a rule which says that when a border is intersected on a weekend, continuous recording will be enabled on one of the cameras. This rule is designed to guarantee a recording of what transpires if somebody breaks into a locked site on a weekend.

1. First it is necessary to set the **SIMT** border. To do this open **Channels** in the settings and select the required **channel**. Further on in **Motion detector** dropdown list select **Moving objects detector (SIMT)** line and follow **SIMT areas** link.

Recording

Recording to server disks: Normal Channel

On Detector

Go to schedule

Recording to hardware disk: Leave defaults

Software Detectors

Uncompress: Main stream

Motion Detector:

Moving Objects Detector (SIMT) **Setup SIMT zones 2**

Disable

Hardware Motion Detector

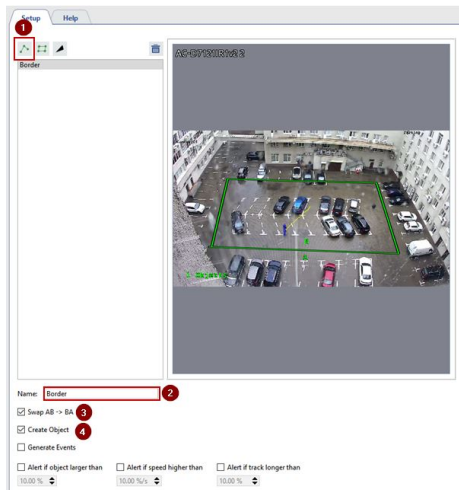
Activity Detector

Activity Detector HD

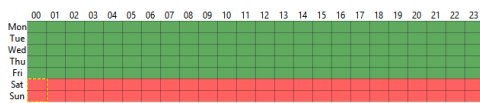
Moving Objects Detector (SIMT)

2. After that do the following:

- a. Create a border in the desired location.
- b. Enter a name for the new border.
- c. Put a checkmark in the **Create object** checkbox. This is necessary for the border to exist in the system as an object.
- d. Put a checkmark in the **Generate events** checkbox. This is necessary for events to be recorded in the event log.



3. After that *schedule* need to be created.

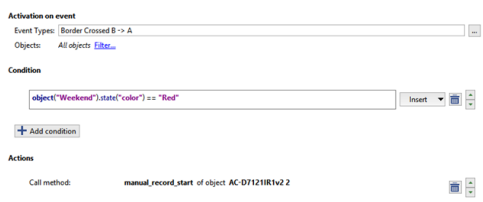


Then *create a new rule* and select the *On event* activation type. In the *Insert event* window, expand the *SIMT borders* section, and put a checkmark in the *Border intersection B -> A* checkbox.

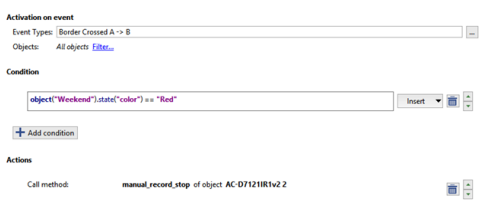
4. Next press *Filter* and check the box of the boundary created before in the *Object* window.

5. Then we need to tie this rule to the schedule in such a way as to ensure its operation on week ends only. To do this in the *Conditions* select *Object state* line, specify earlier created timetable, press *color* and select red color.

6. After that click on *Action* in *Object* link, select the channel where continuous recording shall be activated and *manual\_record\_start* line.



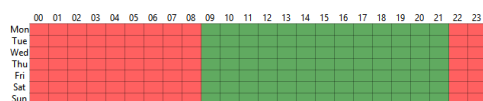
You can also create a counteracting rule. Below is an example a rule that says that when the border is intersected in the opposite direction (A -> B, e.g. exiting the area) on weekends, continuous recording will be disabled on the camera.



### Enable sirens when an alarm input is tripped at night

In this example we consider a rule designed to set off an alarm if there is a break-in at a site at night. This example uses a schedule, and alarm input on the door of the west exit, and alarm output connected to a siren. Thus, if the door of the west exit is opened at night, the siren will be enabled.

1. A *Schedule* needs to be created beforehand.



- Next **create a new rule** and select **On event**, activation type. In the window which will appear find **GPIO input** and check **Input signal lost** box.
- Then click on **Filter** and in the **Object** window check alarm input box, in our case it is "Emergency exit(door)".
- Further on we need to connect this rule with the schedule in such a way as to ensure its operation in night time only. To do this in the **Condition** select **Objects state** line, define timetable created earlier, click **color** and select red.
- After that, click **Action** in the window of the rule, in the window **Object** select emergency exit to which audible horn is connected and **set\_output\_high** line. In the result the rule shall look like as follows:

**Activation on event**

Event Types:

Objects:

**Condition**

**Actions**

Call method:

Below is an example of a rule with opposite activation: if the door of the west exit is closed (the alarm input is closed), then the siren will be shut off after five seconds (the alarm output will be opened).

**Activation on event**

Event Types:

Objects:

**Condition**

**Actions**

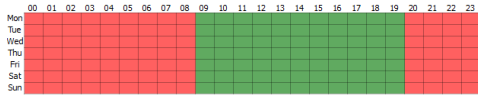
Wait (seconds):

Call method:

## Scripts

### Changing FPS for all channels at night

In this example, we consider a script designed to change the FPS for all channels according to a schedule: when night falls, the frame rate for all channels will be changed to 12 fps; when morning comes, it will be changed to 25 fps. First, you must create a [schedule](#). The screenshot below shows a schedule for this example.



Then create a new script and copy the following code to it.

```
def set_fps_on_all_devices(fps):
    for d in settings("ip_cameras").ls():
        if d.type != "Grabber": continue
        for c in range(16):
            d["channel%02d_fps" % c] = fps
    for b in settings("boards").ls():
        for i in range(16):
            b["channel%02d_fps" % i] = fps

def condition():
    if (object_schedule.state("color") == "Red") :
        set_fps_on_all_devices(12)
    elif (object_schedule.state("color") == "Green") :
        set_fps_on_all_devices(25)

object_schedule = object("Night")
object_schedule.activate_on_state_changes(condition)
```

Let's examine a few parts in more detail.

1. In this part of the script the activator is specified, and the schedule serves as activators. It is sufficient to change the schedule name to connect the script to any other schedule `object("Night")`.

```
object_schedule = object("Night")
object_schedule.activate_on_state_changes(condition)
```

2. The 'condition' function defines a condition whereby if the schedule is in the red zone, the variable "fps" is assigned the value "12"; but if it is in the green zone, the variable is assigned the value "25".

```
def condition():
    if (object_schedule.state("color") == "Red") :
        set_fps_on_all_devices(12)
    elif (object_schedule.state("color") == "Green") :
        set_fps_on_all_devices(25)
```

3. In this part of the script, the frame rate of all channels for all devices is set equal to the value of the variable "fps".

```
def set_fps_on_all_devices(fps):
    for d in settings("ip_cameras").ls():
        if d.type != "Grabber": continue
        for c in range(16):
            d["channel%02d_fps" % c] = fps
    for b in settings("boards").ls():
        for i in range(16):
            b["channel%02d_fps" % i] = fps
```

Below is a simplified version of the script in which the hotkeys F5 and F6 are the activator.

```
def set_fps_on_all_devices(fps):
    for d in settings("ip_cameras").ls():
        if d.type != "Grabber": continue
        for c in range(16):
            d["channel%02d_fps" % c] = fps
    for b in settings("boards").ls():
        for i in range(16):
            b["channel%02d_fps" % i] = fps

def channel_fps_25():
    set_fps_on_all_devices(25)

def channel_fps_12():
```

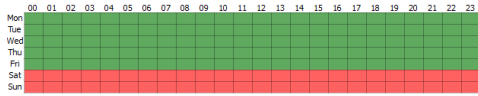
```
set_fps_on_all_devices(12)

activate_on_shortcut("F5", channel_fps_25)
activate_on_shortcut("F6", channel_fps_12)
```

### Enabling economy mode on weekends for all devices in the Lanser family

In this example, we consider a script that will cause all devices in the Lanser family to operate in normal mode on weekdays and in the economy mode on weekends.

First, you must create a [schedule](#). The screenshot below shows a schedule for this example.



Then create a new script and copy the following code to it.

```
def economy_mode_on_all_nvr(on):
    for d in settings("ip_cameras").ls():
        if d.type != "Grabber": continue
        if d["family"] == "NVR":
            d["economy_mode"] = on

def condition():
    if (object_schedule.state("color") == "Red") :
        economy_mode_on_all_nvr(1)
    elif (object_schedule.state("color") == "Green") :
        economy_mode_on_all_nvr(0)

object_schedule = object("Weekends")
object_schedule.activate_on_state_changes(condition)
```

Let's examine a few parts in more detail.

1. In this part of the script the activator is specified, and the schedule is an activator. It is sufficient to change the schedule name to connect the script to any other schedule object("Weekend")

```
object_schedule = object("Weekend")
object_schedule.activate_on_state_changes(condition)
```

2. The 'condition' function defines a condition whereby if the schedule is in the red zone, the variable "on" is assigned the value 1; but if it is in the green zone, the variable is assigned the value 0.

```
def condition():
    if (object_schedule.state("color") == "Red") :
        economy_mode_on_all_nvr(1)
    elif (object_schedule.state("color") == "Green") :
        economy_mode_on_all_nvr(0)
```

3. In this part of the script, the parameter "economy\_mode" is assigned the value of the variable "on" for all devices in the Lanser family.

```
def economy_mode_on_all_nvr(on):
    for d in settings("ip_cameras").ls():
        if d.type != "Grabber": continue
        if d["family"] == "NVR":
            d["economy_mode"] = on
```

Below is an example of a simplified script that will switch Lanser devices in and out of economy mode using the hotkeys F5 and F6, respectively.

```
def economy_mode_on_all_nvr(on):
    for d in settings("ip_cameras").ls():
        if d.type != "Grabber": continue
        if d["family"] == "NVR":
            d["economy_mode"] = on

def economy_mode_on():
    economy_mode_on_all_nvr(1)

def economy_mode_off():
    economy_mode_on_all_nvr(0)

activate_on_shortcut("F5", economy_mode_on)
activate_on_shortcut("F6", economy_mode_off)
```

### Locking an alarm output when a car on a AutoTRASSIR whitelist passes

In this example, we're going to review a script designed to automatically control the swing barrier. When a machine on a whitelist drives by, the swing barrier will open. The implementation uses *AutoTRASSIR's* whitelist functionality and an alarm output.

It is necessary to configure *internal license plate number lists* or *connect external list* beforehand. After that you should create a new script and copy and paste the following code.

```
lock = False

class TaskLocker:
    def __init__(self):
        global lock
        if lock:
            self.have_lock = False
            return
        else:
            self.have_lock = True
            lock = True
            gates_open(self)

    def __del__(self):
        if self.have_lock:
            global lock
            lock = not 1

def gates_close(lock):
    object("Output 1").set_output_low()

def waiting(lock):
    timeout(10 * 1000, lambda: gates_close(lock))

def gates_open(lock):
    object("Output 1").set_output_high()
    waiting(lock)

def acquire_lock():
    TaskLocker()

def the_lpr_handler(event):
    if event.flags & LPR_WHITELIST:
        acquire_lock()

activate_on_lpr_events(the_lpr_handler)
```

Let's examine a few blocks in more detail.

1. This part of the script indicates the activator; in this case, the activator is an event from AutoTRASSIR.

```
activate_on_lpr_events(the_lpr_handler)
```

2. The function `the_lpr_handler(event)` checks to see if the number is on the whitelist. If the recognized license plate numbers on the white list, then the `acquire_lock()` function is run.

```
def the_lpr_handler(event):
    if event.flags & LPR_WHITELIST:
        aquire_lock()
    message("Vehicle on white list")
```

3. The `acquire_lock()` function calls the `TaskLocker()` class.

```
def aquire_lock():
    TaskLocker()
```

4. The `TaskLocker` class is designed to allow the script to run to completion. If the actions in the script take a long time to complete and the script is invoked before the previous instance of itself finishes executing, the `TaskLocker` class prevents the script from being run again until the original instance of the script has run to completion.

```
lock = False

class TaskLocker:
    def __init__(self):
        global lock
        if lock:
            self.have_lock = False
```

```
        return
    else:
        self.have_lock = True
        lock = True
        gates_open(self)

    def __del__(self):
        if self.have_lock:
            global lock
            lock = not 1
```

5. The function `gates_open(lock)` locks alarm output "Output 1" and calls `waiting(lock)`.

```
def gates_open(lock):
    object("Output 1").set_output_high()
    waiting(lock)
```

6. The function `waiting(lock)` waits for 10 seconds and then calls `gates_close(lock)`.

```
def waiting(lock):
    timeout(10 * 1000, lambda: gates_close(lock))
```

7. The function `gates_close(lock)` unlocks alarm output "Output 1".

```
def gates_close(lock):
    object("Output 1").set_output_low()
```

Below is the script that will plan audiophile when a license plate number on the blacklist is recognized.

```
def play_sound(filename):
    import platform
    if platform.system() == 'Windows':
        import winsound
        winsound.PlaySound(filename, winsound.SND_FILENAME\
            | winsound.SND_ASYNC | winsound.SND_NOWAIT)
    else:
        alert('Not implemented')

def the_lpr_handler(event):
    if event.flags & LPR_BLACKLIST:
        play_sound(r"C:\DSSL\Trassir-3.0.2239\sounds\alarm.wav")

activate_on_lpr_events(the_lpr_handler)
```

### Saving AutoTRASSIR screenshots to different folders

In this example we consider a script designed to save screenshots of vehicles from the whitelist and blacklist, or whose license plate numbers were poorly recognized, to different folders. The implementation uses [AutoTRASSIR](#) lists and the screenshot saving functionality.

You should configure [internal license plate number lists](#) or [connect external list](#) beforehand. After that create a new script and copy and paste the following code.

```
def condition(event):
    if event.quality == 0 :
        obj(event.channel).screenshot_ex("", r"C:\DSSL\Screenshots\Low_quality")
    elif event.flags & LPR_WHITELIST :
        obj(event.channel).screenshot_ex("", r"C:\DSSL\Screenshots\Whitelist")
    elif event.flags & LPR_BLACKLIST :
        obj(event.channel).screenshot_ex("", r"C:\DSSL\Screenshots\Blacklist")

activate_on_lpr_events(condition)
```

Let's examine a few parts in more detail.

1. This part of the script indicates the activator; in this case, the activator is an event from AutoTRASSIR.

```
activate_on_lpr_events(condition)
```

2. The function 'condition' defines a condition whereby:

- if the recognition confidence of any one symbol on the license plate is zero, a screenshot will be captured and placed in the "C:\DSSL\Screenshots\Low\_quality" folder

```
if event.quality == 0 :
    obj(event.channel).screenshot_ex\
```



```
("", r"C:\DSSL\Screenshots\Low_quality")
```

- If the recognized number is on the whitelist, a screenshot will be captured and placed in the "C:\DSSL\Screenshots\Whitelist" folder

```
elif event.flags & LPR_WHITELIST :
    obj(event.channel).screenshot_ex\
    ("", r"C:\DSSL\Screenshots\Whitelist")
```

- If the recognized number is on the blacklist, a screenshot will be captured and placed in the "C:\DSSL\Screenshots\Blacklist" folder

```
elif event.flags & LPR_BLACKLIST :
    obj(event.channel).screenshot_ex\
    ("", r"C:\DSSL\Screenshots\Blacklist")
```

### Screenshot when a cashier signs in

In this example, we consider a script that will be activated based on an event from the ActivePOS point-of-sale operations control system. The specified event is a cashier signing in, and the action is to save a screenshot from the associated channel. Thus, when a cashier signs into a cash register, a screenshot with the cashier will be saved; this makes it possible to verify the identity of the cashier, if necessary.

```
def shot(event):
    if event.type == "POS_CASHIER_REGISTRATION":
        obj(event.associated_channel).screenshot_ex("", r"C:\DSSL\Shots\Cashiers")

activate_on_pos_events(shot)
```

1. This part of the script indicates the activator; in this case, the activator is an event from ActivePOS.

```
activate_on_pos_events(shot)
```

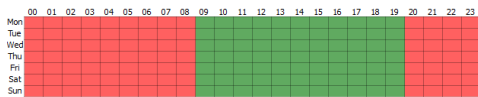
2. The function shot(event) defines a condition whereby if the event is a cashier signing in, then a screenshot from the associated channel is saved to "C:\DSSL\Shots\Cashiers".

```
def shot(event):
    if event.type == "POS_CASHIER_REGISTRATION":
        obj(event.associated_channel).screenshot_ex\
        ("", r"C:\DSSL\Shots\Cashiers")
```

### Placing a warning flag on a receipt when alcohol is sold at night

Each store has its own event scenarios which are considered alarmed and need check. TRASSIR ActivePOS lets mark these events with the bookmarks and add comments to them. After that these events can be selected for the further analysis. In this example we'll review a script marking selling alcohol at night time as an alarmed event.

First, you must create a [schedule](#). The screenshot below shows a schedule for this example.



Then create a new script and insert the following code:

```
def condition(ev):
    if (object("Night").state("color") == "Red"): return
    if ev.type!="POS_POSITION_ADD": return
    u = ev.text.decode("utf-8").upper().encode("utf-8")
    for w in ["BEER", "WINE", "VODKA", "COGNAC"]:
        if u.find(w) != -1:
            pos_fraud(ev, "Warning! Unlawful sale of alcohol!")
            return

activate_on_pos_events(condition)
```

Let's examine a few parts in more detail.

1. This part of the script indicates the activator; in this case, the activator is an event from ActivePOS.

```
activate_on_pos_events(condition)
```

2. The condition function checks if the "Night" schedule is in the red area and if the event is item adding. In case the result is positive, search for the following words in the goods name is done: "BEER", "WINE", "VODKA",

"BRANDY"(the other names which are used for the goods being sold in your store can be added). In case one of these words are found in the name of the goods, troubling tab will be inserted into the receipt using **pos\_fraud** method, and troubling event will be accompanied with pre-set comment.

```
def condition(ev):
    if (object("Night").state("color") == "Red"): return
    if ev.type!="POS_POSITION_ADD": return

    u = ev.text.decode("utf-8").upper().encode("utf-8")
    for w in ["BEER", "WINE", "VODKA", "BRANDY"]:
        if u.find(w) != -1:
            pos_fraud(ev, "Attention! Illegal sale of alcohol!")
            return
```

### Export archive when a receipt is canceled

In this example, we consider a script that will export the archive from the camera over a cash register when a receipt or position is canceled; the recording will go into an electronic file that will include 15 seconds before the event and 15 seconds after it.

To begin, create a new script and copy the following code to it.

```
from time import strftime
from time import time
from time import localtime
from os import path

def export_wait(filename, callback):
    status = get_archive_export_status(path.basename(filename))
    if status==1:
        timeout(1000, lambda: export_wait(filename, callback))
    elif status==0 or status==2:
        alert("AVI export failed")
        callback()
    else:
        if not path.exists(decode(filename)):
            alert("Exported file %s not found!" % filename)
            callback()

def action0_2():
    pass

def start_export(ev, t1, t2, filename):
    object("Operator m-gilyazov's interface").archive_export\
    (ev.associated_channel, t1, t2, path.basename(filename), 0)
    timeout(1000, lambda: export_wait(filename, lambda: action0_2()))

def condition(event):
    if event.type == "POS_RECEIPT_CANCEL"\
    or event.type == "POS_POSITION_CANCEL":
        t = time()
        t1 = '%.0f' % ((t-30)*1000000)
        t2 = '%.0f' % (t*1000000)
        shots_path = r"C:\DSSL\Screenshots\cancel"
        filename = event.pos_terminal_name + strftime('%Y%m%d_%H%M%S',\
        localtime(t)) + '.avi'
        filename = shots_path + '/' + filename
        timeout(15000, lambda: start_export(event, t1, t2, filename))

activate_on_pos_events(condition)
```

Let's examine a few parts in more detail.

1. This part of the script indicates the activator; in this case, the activator is an event from ActivePOS.

```
activate_on_pos_events(condition)
```

2. The 'condition' function determines if the event is a canceled position or canceled receipt. If it is, the start\_export function is executed. The 'condition' function also specifies a 30-second wait, and output filename, and the path to the folder where the electronic file will be saved.

```
def condition(event):
    if event.type == "POS_RECEIPT_CANCEL"\
    or event.type == "POS_POSITION_CANCEL":
        t = time()
        t1 = '%.0f' % ((t-30)*1000000)
```

```
t2 = '%.0f' % (t*1000000)
shots_path = r"C:\DSSL\Screenshots\cancel"
filename = event.pos_terminal_name + \
    strftime('%Y%m%d_%H%M%S', localtime(t)) + '.avi'
filename = shots_path + '/' + filename
exported_files[event.pos_terminal_name] = filename
timeouts(15000, lambda: start_export\
(event, t1, t2, filename))
```

3. The `start_export` function starts exporting the archive with the previously specified settings and invokes the `export_wait` function.

```
def start_export(ev, t1, t2, filename):
    object("Operator's interface m-gilyazov").archive_export\
        (ev.associated_channel, t1, t2, path.basename(filename), 0)
    timeout(1000, lambda: export_wait(filename, lambda: action0_2()))
```

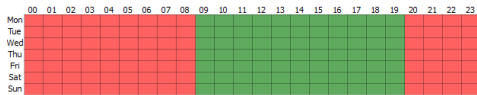
4. The 'export\_wait' function determines if an archive export is currently underway from a previous instance of the script; if it is not, then action0\_2 is executed.

```
def start_export(ev, t1, t2, filename):
    object("Operator's interface m-gilyazov").archive_export\
    (ev.associated_channel, t1, t2, path.basename(filename), 0)
    timeout(1000, lambda: export wait(filename, lambda: action0 2()))
```

## Changing the sensitivity of a detector according to a schedule

In this example, we consider a script designed to change the sensitivity of a motion detector according to a schedule. It can reduce the number of false positives due to noise at night.

First, you must create a *schedule*. The screenshot below shows a schedule for this example.



Then create a new script and copy the following code to it.

[illegible]

Let's examine a few parts in more detail.

- 253

## Recovering a server's state during an extended period of high processor load

To begin, create a new script and copy the following code to it.

254

```
t = 30000 #sample frequency in ms
k = 85 #critical processor load

def iter_func():
    global a, i, l, t, k

    if len(a) >= 1:
        a.popleft()
        i = settings("health")["cpu_usage"]
        a.append(i)

    s = 0
    c = 0
    for j in xrange(0, len(a)):
        s += a[j]

    c = s / l
    if c >= k :
        settings("health")["user_defined_health_indicator"] = 0
    else :
        settings("health")["user_defined_health_indicator"] = -1
    timeout(t, iter_func)

def start_script():
    iter_func()

start_script()
```

Let's examine a few parts in more detail.

1. In this part of the script, the length of queue **a** is checked and the latest processor load value is written to it.

```
if len(a) >= 1:
    a.popleft()
    a.append(i)
    i = settings("health")["cpu_usage"]
```

2. In the next part of the script, all of the elements of double-ended queue **a** are added together.

```
s = 0
c = 0
for j in xrange(0, len(a)):
    s += a[j]
```

3. In this part of the script, the average processor load **c** is computed and compared with critical value **k**. If the average value is greater than or equal to the critical value, the server's state is manually downgraded. If the average value is less than the critical value, the server's state is switch to normal.

```
c = s / l
if c >= k :
    settings("health")["user_defined_health_indicator"] = 0
else :
    settings("health")["user_defined_health_indicator"] = -1
    timeout(t, iter_func)
```



- [Rules](#)
- [Scripts](#)
- [Schedules](#)
- [Adding an email account](#)

# Plugins

You can extend TRASSIR's basic functionality by configuring the following add-on modules:

- *ActiveDome* is a module for automated control of PTZ cameras.
- *ActivePOS* is a module for monitoring point-of-sale operations.
- *AutoTRASSIR* is a module for automatic license plate number recognition.
- *Integration with one or several Access Control Systems or Security and Fire Alarm Systems* - events receipt from Access Control System or Security and Fire Alarm System devices.
- *SIMT* is an smart object-tracking detector.
- *ActiveSearch* is a revolutionary tool for searching an archive.
- *Slow down detector* is a module that discovers suspicious or lost objects in the shooting area.
- *Face Tracker/Recognizer* is an intelligent module intended for detecting and recognizing faces in the frame.
- *Empty shelf detector* is a module that allows analyzing and informing about the store shelves condition.
- *Queue detector and Workplace detector* are the modules intended for crowd detection and the employees office hours tracking.
- *Head Tracker* is a module for counting the number of people intersecting the border in one of the preset directions.
- *Neuro Detector* is an intelligent module for recognizing various object classes on video. It is designed for building of complex security systems.
- *ArUco Detector* is a module designed for special bar codes recognition.
- *Bags counter* is a module which allows to get information on the number of bags on the conveyer belt.
- *Abandoned items neural detector* is a plugin designed for identifying suspicious or forgotten objects in the shooting area.
- *Pose detector* is a plugin that can determine a person's posture based on movement and behavior algorithms.



The availability of any of the modules described is determined by your license.

## ActiveDome - Automated PTZ-camera control

ActiveDome is a module for automated control of PTZ cameras. It can instantly point a PTZ camera at any desired object. There are *two modes* for object tracking: manual and automatic. A *SIMT* software-based detector is used in automatic mode.

The basic idea behind the module is to use information from objects in the overview camera's frames to control the PTZ camera, regardless of their relative orientation. Additionally, any combination or quantity of overview- and PTZ cameras may be used.

To configure the ActiveDome system:

1. In TRASSIR, install and configure the cameras that will be used in ActiveDome.
2. If an analog PTZ camera is being used, be sure that the *RS-485 converter connection* is correct and *configure* the server's serial port.
3. Select an optics model or *calibrate the optics* of the PTZ cameras.
4. *Create a scene* by adding overview- and PTZ cameras.
5. *Establish the correspondence* between each pair of overview- and PTZ cameras.



This section provides recommendations on how to configure the ActiveDome system. See the Operator's Guide (???) for information about how to arrange cameras in a template or use the module itself.

ActiveDome features:

- Independent positioning of the overview- and PTZ cameras. Configuring ActiveDome does not require a specific relative orientation between the cameras. A calibration system based on "smart" algorithms is used to establish associations.
- Coordinates are automatically recalculated given the zoom level and transmitted to the PTZ camera.
- The PTZ camera can be positioned to an unlimited number of points on the screen.
- Simple positioning of a camera by single-clicking with the mouse or highlighting the desired area of the screen. The positioning speed is only limited by the camera's speed.
- Tracking objects both in manual and automatic mode using an intelligent *SIMT* motion detector or *Neurodetector*.



- *ActiveDome's manual and automatic operating modes*
- *Choosing an optics model and calibrating PTZ camera optics*
- *Creating an ActiveDome scene*
- *Comparison of overview cameras and PTZ cameras*
- *Connecting analog PTZ cameras*
- *Serial port settings*



## ActiveDome's manual and automatic operating modes

When the operator selects an arbitrary point, the PTZ camera's control parameters are automatically calculated. Consequently, the PTZ camera is positioned not only to the desired location but with the required zoom level as well. The **manual mode** lets the operator highlight an object on a camera image which allows to point a PTZ camera to this object. An image scale is also calculated, if needed. ActiveDome manual mode can be successfully implemented in mass movement zones and where the constant operator's attention is required: squares, railway stations, airports, shopping malls, etc.

There are two ways to point the camera in manual mode:

- A simple click of the mouse - the selected location on the screen will be displayed at the required zoom level;
- Highlighting a rectangular area - the selected area will be displayed on the entire screen.

**Automatic mode** can be implemented for vast poorly visited areas security, where an appearance of a person or a vehicle is considered an alarm: warehouses and their surrounding areas, oil depots, military facilities, bridges, railroad exclusion zones, etc.

In automatic mode the information about the object transfers to PTZ camera from *SIMT* intellectual motion detector as well as from *Neuro detector*. Moreover, the modules transmit object coordinates to ActiveDome with consideration of their future shift during camera rotation. They're also capable to differ objects from one another and remember their history (track) which allows pointing cameras at them turn by turn to capture a detailed image of each. A camera switches between objects, following them during the period which is called "Switch timeout" and configured in the *scene settings*.

**ActiveDome** and **Neuro Detector** joint use allows configuring effective tracking of people with the same identification: the uniform color or absence of a headwear (hardhat).



The possibility to use smart modules in ActiveDome is determined by the appropriate module license.



- [ActiveDome - Automated PTZ-camera control](#)
- [Choosing an optics model and calibrating PTZ camera optics](#)
- [Creating an ActiveDome scene](#)
- [Comparison of overview cameras and PTZ cameras](#)

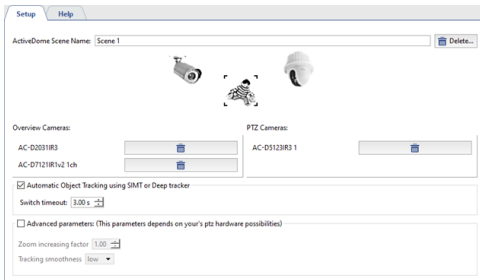
## Creating an ActiveDome scene

The basic element of configuring ActiveDome is the scene. A scene is a system of connected overview- and PTZ cameras that provide video surveillance for a specific zone. One scene can simultaneously use up to 4 overview cameras and 4 PTZ cameras in any combination. The number of scenes is unlimited.



- Overview camera - A fixed-position camera that gives a wide shot.
- PTZ camera - A high-speed dome camera that points immediately at a desired object.

For example, a single PTZ camera and four wide-angle overview cameras can provide 360° monitoring of a space. After clicking **Create new...**, a window will open where you can configure the new ActiveDome scene. This window supports changing the scene's name, adding overview- and PTZ cameras, and deleting the scene.

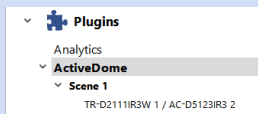


An inventory of available PTZ cameras is generated from the list of PTZ devices that have been bound to an appropriate *serial port*. Additionally, you can use SpeedDome PTZ IP-cameras. IP cameras are added and configured just like other *IP devices*.

- The **Automatic Object Tracking using SIMT of Deep tracker** options enables *Automatic ActiveDome mode*.
- The **Switch timeout** parameter determines the amount of time for which an object will be tracked before the camera will switch to a different target (if one exists). The values range between 1 and 10 seconds.
- Next, *establish the correspondence between the overview- and PTZ cameras*.



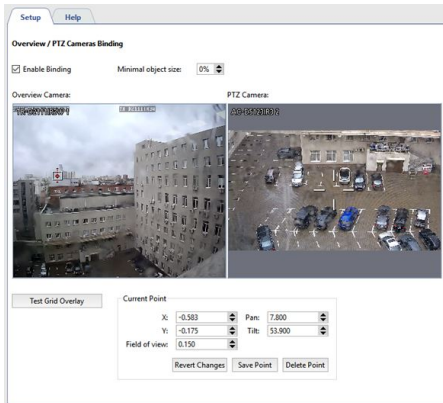
A list of all created scenes is shown in the settings tree.



- *ActiveDome - Automated PTZ-camera control*
- *Choosing an optics model and calibrating PTZ camera optics*
- *Comparison of overview cameras and PTZ cameras*

## Comparison of overview cameras and PTZ cameras

When adding cameras to an ActiveDome scene, every possible combination of overview- and PTZ cameras are created automatically.



You will need to add a few points and indicate the correspondence between them on the overview- and PTZ cameras. To do this:

1. Double-click in the overview camera window to add a calibration point.
2. Orient the lens of the PTZ camera so that the crosshairs point exactly at the point specified in the overview camera window.
3. Click **Save point**.

The **X** and **Y** parameters make it possible to more precisely move the point on the overview camera. The **Pan** and **Tilt** parameters facilitate more accurate positioning of the PTZ camera. The **Field of view** parameter specifies the zoom level at the given point. The parameter's value should be chosen based on the assumption that the height of the icon is approximately the same as the height of a person.



At least 3 points must be provided. Verify the position of the PTZ camera in various areas. If the camera is not positioned accurately in a given area, then create an additional point there. For example, more precise configuration may be necessary if the overview- and PTZ camera are a significant distance from each other.

After configuring the correspondence between the overview and PTZ camera, you can check for gross errors by clicking **Show correspondence grid**. Abrupt breaks in the grid indicate the presence of a gross error.

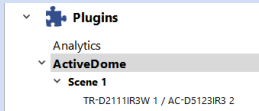
Example of a correctly configured grid:



Example of a grid with a gross error:



The complete list of combinations of overview- and PTZ cameras is shown in the settings tree.



- *ActiveDome - Automated PTZ-camera control*
- *Choosing an optics model and calibrating PTZ camera optics*
- *Creating an ActiveDome scene*

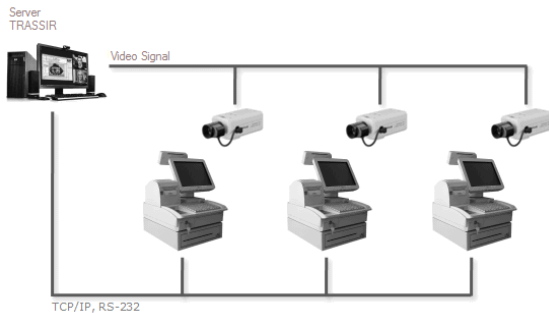
## ActivePOS - Point-of-sale operations monitoring

The ActivePOS module is designed for monitoring point-of-sale operations in order to suppress fraud by cashiers and store staff and help resolve conflicts with customers. The module can be used in major supermarket chains, movie theaters, hair salons, gas stations, as well as any small retail outlets.

A versatile receipt filter and synchronized video from a surveillance camera make it possible to detect virtually any theft scheme, while convenient archive management tools let you immediately response to any irregular situation.

Point-of-sale operations are monitored in the following manner:

1. Point-of-sale terminals and a TRASSIR server are connected to a local network.
2. A nearby video camera monitors each point-of-sale terminal.
3. Each point-of-sale terminal is assigned an IP address and a server port to which data about completed transactions is sent.
4. In the server's settings, each point-of-sale terminal is bound to the signal from a camera near the cashier.
5. The video for each point-of-sale terminal is supplemented with a synchronized description of operations being performed (captions).
6. All of the video is saved in the archive.
7. If needed, the TRASSIR administrator customizes filters for suspicious events that require additional attention from controllers.



- [ActivePOS features](#)
- [Trading systems and equipment compatible with ActivePOS](#)
- [ActivePOS incidents and detectors](#)
- [Configuring POS terminals](#)
- [Configuring R-Keeper POS terminals](#)
- [DSSL XML for ActivePOS](#)
- [Using ActivePOS in scripts](#)

## ActivePOS features

The ActivePOS module provides:

- A breakdown of a receipt's continuous text into a collection of events representing all of the cashier's actions, not all of which are displayed on the customer's receipt: cashbox operations, cashier sign-in, discount calculation, generation of a report with and without a reset, etc.
- Ability to configure a response to any point-of-sale terminal event.
- Ability to save events for sales, cancellations, returns, annulments, etc. in a database and search for them in any combination while overlaying a receipt number, cashier's name, time interval, purchase total, etc.
- Binding of events to a video sequence with the ability to search by event for a particular video frame.
- Color highlighting of alarm- and knowingly suspicious operations as soon as they occur; the operator sees the situation in real-time.
- Quick search in the event archive.
- Statistics and analytical reports about sales (canceled goods, calculations of discounts, average receipt total).



- [\*ActivePOS - Point-of-sale operations monitoring\*](#)
- [\*Trading systems and equipment compatible with ActivePOS\*](#)
- [\*ActivePOS incidents and detectors\*](#)
- [\*Configuring POS terminals\*](#)
- [\*Configuring R-Keeper POS terminals\*](#)
- [\*DSSL XML for ActivePOS\*](#)
- [\*Using ActivePOS in scripts\*](#)

## Trading systems and equipment compatible with ActivePOS

ActivePOS operates both with full scale trading-POS systems as well as with separate devices:

- **POS systems:**

- Cashier workplace Artix:POS (artix.su)
- Frontol software (atol.ru)
- R-Keeper(ucs.ru)
- dStore POS of MICROS company (micros-fidelio.it)
- SuperMag UKM 4 cash desk system (servplus.ru)
- SHTRIH-LIGHTPOS POS-system (shtrih-m.ru)
- IBS GAS software package
- Set Retail cash program (crystals.ru)
- MARKET SOFTWARE + from Soft Market company
- POS-2000 computer cash desk

- **Weighting equipment:**

- SKI-12 weight indicator
- CAS CI-200A weight indicator
- CAS-CL5000J sticker printing POS-scales
- CAS-DBII(E), CAS-CI2001A floor scales

- **Counting machines and sorters:**

- Numeron and BPS banknote sorters
- Glory GFR-220, USF100 and USF 51 banknote counters
- Glory (Talaris) MACH-6 coin sorter
- Kisan Newton-FS, Newton-VS, Newton-F(v3.22) and K-500Pro banknote counters and sorters
- Laurel K4 and Laurel K8 banknote sorters
- Perconta Sortovit MS10 DB coin sorter
- Magner 150 Digital and Magner 350 Digital banknote sorters
- DoCash DC-50V and DoCash DC-50F banknote counters

Additionally, the ActivePOS module can receive events using TCP or UDP from any other system, provided that the events adhere to the [DSSL XML](#) format.

In order to configure the transmission of events from point-of-sale terminals, you must specify the TRASSIR server's IP address, port number, and protocol in the retail system's software. Please see the point-of-sale vendor's software documentation for information on how to configure each of the supported retail systems.



- *ActivePOS - Point-of-sale operations monitoring*
- *ActivePOS features*
- *ActivePOS incidents and detectors*
- *Configuring POS terminals*
- *Configuring R-Keeper POS terminals*
- *DSSL XML for ActivePOS*
- *Using ActivePOS in scripts*

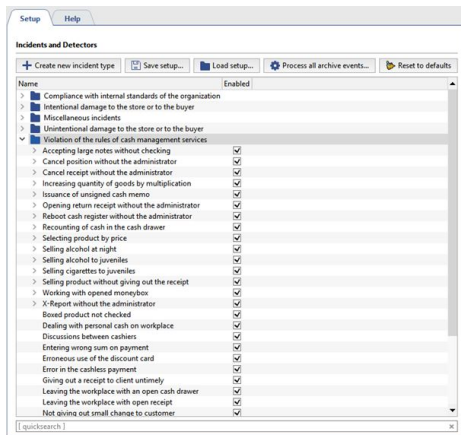



## ActivePOS incidents and detectors

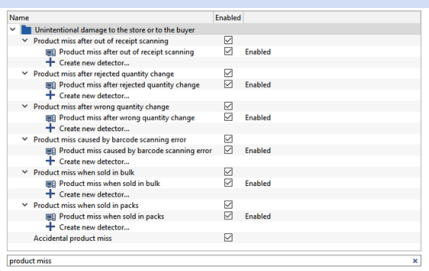
Incidents are special events resulting from an analysis of personnel actions. They represent violations of a retail outlet's established operating rules.

For example:

- Violation of cash-handling rules: "Sale receipt printed without signature", "Product released without receipt", etc.
- Violations causing intentional or unintentional harm to the organization or customers: "Simulated product scanning", "Product sold with understated weight", etc.
- Violations resulting from failure to comply with internal company standards: "Store opened late", "Cell phone used", etc.
- And so forth.



 You can use quick contextual search to quickly find an incident.



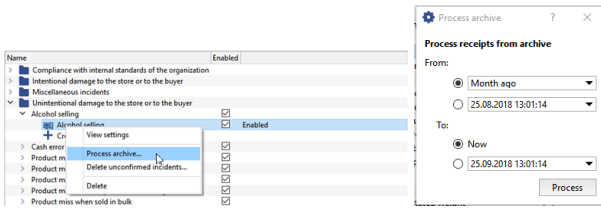
The following types of incidents are used in TRASSIR:

- **Automatically detected** - Incidents are detected using configured detectors.
- **Manually detected** - Incidents whose confirmation requires operator involvement. See the Operator's Guide (???) for a description of manually detected incidents and how to confirm them.

To begin incident detection, set the checkbox next to the desired incident. When using automatically detected incidents, set the checkbox for the corresponding detector.

In order to create incident and detector settings backup copy and transfer them to the other server, press **Save settings...** button and select the folder. On default setting will be saved to the file `pos_detectors.xml`. Press **Load settings...** button in the other server's settings and select the file saved earlier.

In case in the course of TRASSIR operation any detector has been deactivated and staff activities analysis has not been done using this detector, you can activate it at any time and process with it archive of receipt which has been already saved. To do this mark required detector in the list and select **Archive processing...** item in context menu. Specify period of time receipts of which shall be processed by this detector in the opened window and press **Process** button.



In order to process the whole archive of events, press **Process all archived events...** button.



In order to reset all done settings of incidents and detectors used by them, press **Restore default values** button.



- [ActivePOS - Point-of-sale operations monitoring](#)
- [ActivePOS features](#)
- [Trading systems and equipment compatible with ActivePOS](#)
- [Configuring POS terminals](#)

## Personal incidents and detectors creation

TRASSIR allows to create unrestricted number of the types of incidents and detectors to detect them. In order to create incident press **Create new incident type** button or select **Create new incident type...** item in the context menu. Enter **Name** and **Description** of incident in the opened window.

All created incidents can be grouped into the folders. In order to do this drag and drop them to available folders or create new folders clicking **Create new folder** item in the context menu.

In order to edit detector parameters open incident, click twice on detector or click **View description** in the context menu. You can modify incident detection in the opened window.

If necessary you can create you on set of incidents and detectors to detect them. In order to do this, open incident and click twice on **Create new detector...** item.

For example, we need to trace sales when "Gift handling out" and "sale with discount card" are present in the receipt. In order to do this, we will use **Events filter detector** from **Other incidents** folder. We will specify the events which are required as parameters: **Adding gift to receipt** and **Discount card sale** and check **Examine for all events entry** box.



It makes sense to use checking **Process all archive events** box only for the events appearing within one receipt.

In case the box is not checked, it means that detector will activate in case occurrence of any event selected in **Filter by events** field.

Activate the detector.

Now if a cashier will register discount card sales and hand out gift to the client, we will see it in the incident report (see section ??? in "Operator's Manual").



*ActivePOS incidents and detectors*

## Configuring POS terminals

In order to add POS-terminal click **ActivePOS** -> **Terminals** menu items and press **Add POS** button.

Specify the following in the point-of-sale terminal's settings window:

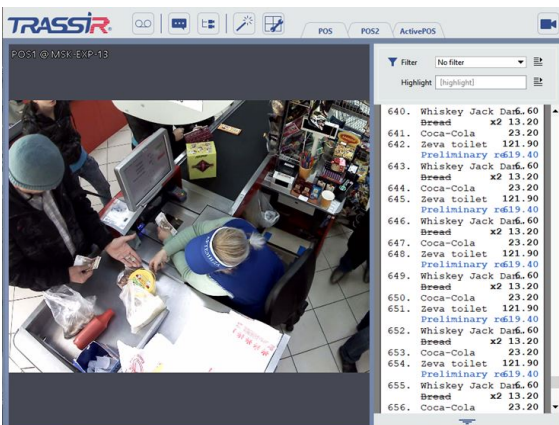
- **Name** - The terminal's display name in the system.
- **IP address** - The address of the server providing information about transactions.
- **Port** - The server port.
- **TCP/UDP** - The transport protocol.
- **Channel** - The camera to which the point-of-sale terminal will be bound.
- **Protocol** - The protocol used by the retail system (point-of-sale terminal).
- **Subtitles** - coordinates of upper left and lower right angles of rectangle where subtitles will be outputted (POS operations content).
- **Char in line** - The maximum number of symbols to display on a single line. The size of the area for displaying captions is considered when displaying lines.

Subtitles from one POS-terminal can be distributed into several video channels. Accomplish this adding additional channels and set **Subtitles position**.



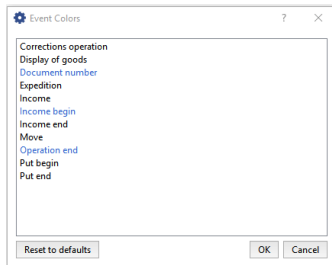
The number of additional channels is determined by corresponding software license.

If the setup is correct the events generated by POS-terminal will be displayed in TRASSIR interface in POS events log and on the chose channel (see the Figure).

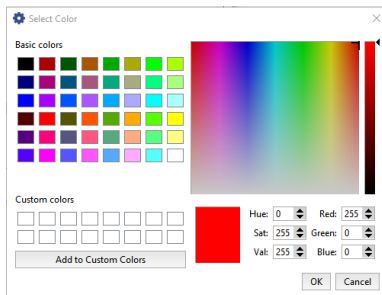


If necessary, assign colors and the font for events generated by point-of-sale terminals. To do this:

- In the **Font size** field, enter the font height in points;
- To select an event color, click the **Event colors...** button
- in the opened window, click on the event you want to sign a color to



- Double-click on the event and select the desired color in the window that opens

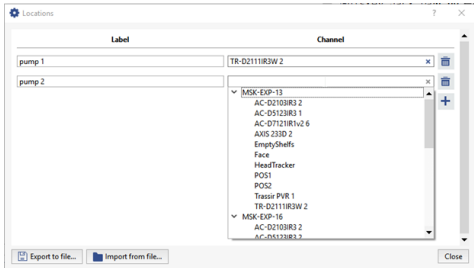


## Location settings

Locations allow to associate certain image from the camera with operations done on POS.

For example, a gas station is equipped with several cameras directed directed on fuel dispensers. Using special identifiers transmitted to TRASSIR along with payment data, you will bind payment receipt with certain video channel. In such a way information concerning payment the fuel dispensed by this dispenser will overlap the image of each fuel dispenser.

To do this press **Location settings...** button and establish matching of **Identifiers** and **Video channel**.



To transfer location settings from one TRASSIR server to another one, you can use **Export to file...** and **Import from file...** buttons.



Location settings can be done only by using **DSSL\_XML** protocol (see section **DSSL XML for ActivePOS**).



- *ActivePOS - Point-of-sale operations monitoring*
- *ActivePOS features*
- *Trading systems and equipment compatible with ActivePOS*
- *ActivePOS incidents and detectors*
- *Configuring R-Keeper POS terminals*
- *Using ActivePOS in scripts*

## Configuring R-Keeper POS terminals

Unlike other retail systems, R-Keeper uses a fixed port to receive data packets from several terminal devices or cash registers; The terminal number is written in the transaction packet.

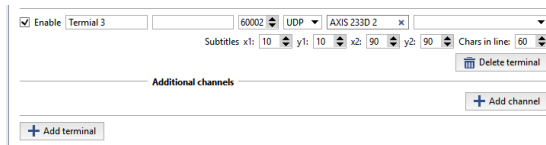
TRASSIR handles this peculiarity with an automation script that receives R-Keeper transactions, analyzes their contents, and redirects them to the appropriate ActivePOS terminal.

Configuring TRASSIR for the R-Keeper protocol consists of three steps:

### 1. Terminal configuration

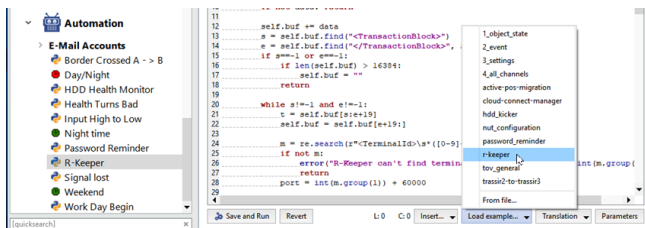
R-Keeper POS-terminals must be configured as follows:

- **IP address** - blank
- **Port** 60,000 more than the terminal number (for example, for terminal 13, the port is 60013; for terminal 37, the port is 60037)
- **TCP/UDP** - UDP

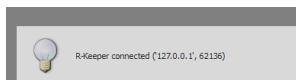


### 2. Redirection script

You can find the redirection script in the examples:



When an R-Keeper terminal is connected to the script a pop-up message will appear:



By default, TRASSIR waits for data on port 4444; If needed, you can change this port number by editing the following lines:

```
cont = Container()
cont.server = EchoServer('', 4444)
cont.server_thread = ServerThread()
cont.server_thread.quit_flag = 0
cont.server_thread.start()
```

### 3. Editing the configuration file

In order to correctly process R-Keeper transactions, you must edit **pos-rkeeper.ini**, which is located in the TRASSIR folder.

The file is written in the INI format and has the following structure:

- **[CashMachines]**
  - Name of a group of terminals (for example, [Group1])
- **terminal\_ids="1,2,5,7"**
  - A list of the terminals in the group

The line 'terminal\_ids=""' signifies the numbers of all terminals that have not been explicitly indicated in the configuration file
- **date\_format="dd.MM.yyyy"**
  - The date format
- **time\_format="h:mm:ss"**
  - The time format



- FN\_RECEIPT\_BEGIN\_MIN=100  
FN\_RECEIPT\_BEGIN\_MAX=100  
- The range of FunctionNumber for the "New receipt" event
- FN\_RECEIPT\_END\_MIN=10  
FN\_RECEIPT\_END\_MAX=10  
- The range of FunctionNumber for the "Receipt closed"
- FN\_POSITION\_ADD\_MIN=101  
FN\_POSITION\_ADD\_MAX=105  
- The range of FunctionNumber for the "Position added" event
- FN\_PRINT\_MIN=200  
FN\_PRINT\_MAX=999  
- The range of FunctionNumber for the "Comments" event
- FN\_RECEIPT\_DISCOUNT\_MIN=4  
FN\_RECEIPT\_DISCOUNT\_MAX=4  
- The range of FunctionNumber for the "Discount applied to receipt" event
- FN\_CANCEL\_BEGIN\_MIN=0  
FN\_CANCEL\_BEGIN\_MAX=0  
- The range of FunctionNumber for the "Canceled receipt opened" event
- FN\_CANCEL\_POSITION\_MIN=6  
FN\_CANCEL\_POSITION\_MAX=6  
- The range of FunctionNumber for the "Position canceled" event
- FN\_CANCEL\_END\_MIN=0  
FN\_CANCEL\_END\_MAX=0  
- The range of FunctionNumber for the "Canceled receipt closed" event



A sample configuration can be found in pos-rkeeper.sample.ini in the TRASSIR folder

To determine the range values, you must either analyze protocol dumps or refer to the documentation and settings of the devices being used.



All of the settings must be specified for each group of terminals. If you do not know the range, fill it with zeros.



In order for TRASSIR to work properly, the ranges of different events must not overlap.



Lines beginning with ";" in the settings file are comments and are not analyzed by TRASSIR.

You do not need to restart TRASSIR to verify the changed settings – just cycle the configured ActivePOS terminal on and off.



- *ActivePOS - Point-of-sale operations monitoring*
- *ActivePOS features*
- *Trading systems and equipment compatible with ActivePOS*
- *ActivePOS incidents and detectors*
- *Configuring POS terminals*
- *DSSL XML for ActivePOS*
- *Using ActivePOS in scripts*

## DSSL XML for ActivePOS

This format allows you to send events to ActivePOS on behalf of the POS terminal. The messages in this format can be sent both via TCP and UDP.

As can be seen from its name, this protocol is based on XML. Each event that happens on at point-of-sale terminal is represented by a transaction block:

```
<?xml version="1.0" encoding="utf-8"?>
<transaction>
  <event_type>POSNG_RECEIPT_OPEN</event_type>
  <operation_id>E44D0F4A</operation_id>
  <cashier>Ivanov I</cashier>
  <date>11/01/2017</date>
  <time>16:40:08</time>
  <location>cas_1</location>
</transaction>
<?xml version="1.0" encoding="utf-8"?>
<transaction>
  <event_type>POSNG_POSITION_ADD</event_type>
  <operation_id>E44D0F4A</operation_id>
  <cashier>Ivanov I</cashier>
  <date>11/01/2017</date>
  <time>16:40:10</time>
  <position>1</position>
  <weight>1.234</weight>
  <barcode>1149990037</barcode>
  <text>Rollton LBE chicken Caesar 65g (Mareven Food Central): 24</text>
  <price>185.4</price>
  <location>cas_1</location>
</transaction>
<?xml version="1.0" encoding="utf-8"?>
<transaction>
  <event_type>POSNG_POSITION_ADD</event_type>
  <operation_id>E44D0F4A</operation_id>
  <cashier>Ivanov I</cashier>
  <date>11/01/2017</date>
  <time>16:40:15</time>
  <position>2</position>
  <quantity>2</quantity>
  <price_per_unit>51.99</price_per_unit>
  <barcode>0760557822035</barcode>
  <text>Buttermilk milk ster.1,5% 0,95l t / brik (Unimilk): 1.12</text>
  <price>103.98</price>
  <location>cas_1</location>
</transaction>
<?xml version="1.0" encoding="utf-8"?>
<transaction>
  <event_type>POSNG_POSITION_ADD</event_type>
  <operation_id>E44D0F4A</operation_id>
  <cashier>Ivanov I</cashier>
  <date>11/01/2017</date>
  <time>16:40:15</time>
  <position>3</position>
  <volume>10.723</volume>
  <barcode>12843745092347</barcode>
  <text>Benzin AI95</text>
  <price>76.45</price>
  <location>cas_1</location>
</transaction>
<?xml version="1.0" encoding="utf-8"?>
<transaction>
  <event_type>POSNG_RECEIPT_CLOSE</event_type>
  <operation_id>E44D0F4A</operation_id>
  <cashier>Ivanov I</cashier>
  <price>313.84</price>
  <date>11/01/2017</date>
  <time>16:40:20</time>
  <location>cas_1</location>
</transaction>
```

Each unit of transactions has:

- Mandatory set of transferred data:
  - **event\_type** - the event type;

- **operation\_id** - unique identifier (sequential number of document) all operations by which are combined into single receipt;
- **cashier** - user name;
- **date** - the operation's completion date (MM/dd/yyyy);
- **time** - the operation's completion time (hh:mm:ss).
- Set of parameters describing the operation:
  - **position** - number of item in receipt;
  - **quantity** - parameter containing quantitative characteristic of operation expressed in whole number;
  - **weight** - parameter containing fractional quantitative characteristic of operation;
  - **volume** - a parameter containing a fractional quantitative characteristic of the volume of the goods;
  - **price** - parameter containing information of the price or cost of operation being conducted;
  - **price\_per\_unit** - price per unit of goods;
  - **barcode** - item bar code;
  - **article** - item number;
  - **location** - parameter connecting operation being conducted with video channel (see section [Configuring POS terminals](#));
  - **text** - parameter is intended for the transfer of text data concerning operation (for example, item name, error code, etc.).

List of events and parameters describing given event can differ depending on videosurveillance object:

- [DSSL XML for trade objects](#);
- [DSSL XML for hotel business and public catering objects](#);
- [DSSL XML for banknote counters and sorters](#).
- [DSSL XML for warehouses](#).
- [DSSL XML for gas stations](#).



The list of event types is continuously added to. You can get an up-to-date list by contacting DSSL technical support.

A frequently-used option is to have a [script](#) send messages to 127.0.0.1 using UDP. The port number must match the terminal created in the ActivePOS settings dialog.

```
t = "<?xml version= ... <transaction> ... </transaction>"
import socket
try:
    s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    s.connect(("127.0.0.1", port))
    s.send(t)
    s.close()
except socket.error, msg:
    error("can't forward to port %i: %s" % (port, msg))
    s.close()
```



- *ActivePOS - Point-of-sale operations monitoring*
- *ActivePOS features*
- *Trading systems and equipment compatible with ActivePOS*
- *ActivePOS incidents and detectors*
- *Configuring POS terminals*
- *Configuring R-Keeper POS terminals*
- *Using ActivePOS in scripts*

## DSSL XML for trade objects

### Shift events

Event type ( <i>event_type</i> )	Description
<i>POSNG_SHIFT_START</i>	The start of a shift
<i>POSNG_SHIFT_END</i>	The end of a shift
<i>POSNG_SHIFT_RESTORE</i>	The restoration of a shift
<i>POSNG_SHIFT_OVER_24H</i>	The shift has exceeded 24 hours

### User registration

Event type ( <i>event_type</i> )	Description
<i>POSNG_CASHIER_LOGIN_BEGIN</i>	Cashier sign-in started
<i>POSNG_CASHIER_LOGIN_FAIL</i>	Cashier sign-in failed
<i>POSNG_CASHIER_LOGIN</i>	Cashier sign-in succeeded
<i>POSNG_CASHIER_LOGOUT</i>	Cashier sign-out
<i>POSNG_ADMIN_LOGIN_BEGIN</i>	Administrator sign-in started
<i>POSNG_ADMIN_LOGIN_FAIL</i>	Administrator sign-in failed
<i>POSNG_ADMIN_LOGIN_FAIL</i>	Administrator sign-in succeeded
<i>POSNG_ADMIN_LOGOUT</i>	Administrator sign-out
<i>POSNG_TAX_OFFICER_LOGIN_BEGIN</i>	Tax officer sign-in started
<i>POSNG_TAX_OFFICER_LOGIN_FAIL</i>	Tax officer sign-in failed
<i>POSNG_TAX_OFFICER_LOGIN</i>	Tax officer sign-in succeeded
<i>POSNG_TAX_OFFICER_LOGOUT</i>	Tax officer sign-out

### Creating a receipt

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_OPEN</i>	Sales receipt opened
<i>POSNG_RECEIPT_SELL_CLOSE</i>	Sales receipt closed
<i>POSNG_RECEIPT_RETURN</i>	Return receipt opened
<i>POSNG_RECEIPT_RETURN_CLOSE</i>	Return receipt closed
<i>POSNG_RECEIPT_ANNULMENT</i>	New cancellation receipt
<i>POSNG_RECEIPT_EXCHANGE</i>	New exchange receipt
<i>POSNG_RECEIPT_EXCHANGE_CLOSE</i>	Exchange receipt closed
<i>POSNG_RECEIPT_PAYOUT</i>	New payout receipt
<i>POSNG_RECEIPT_PAYOUT_CLOSE</i>	Payout receipt closed
<i>POSNG_RECEIPT_REPAYMENT</i>	New repayment receipt
<i>POSNG_RECEIPT_CLOSE</i>	Receipt closed
<i>POSNG_RECEIPT_CANCEL_BEGIN</i>	Receipt cancellation started
<i>POSNG_RECEIPT_CANCEL_FAIL</i>	Receipt cancellation failed
<i>POSNG_RECEIPT_CANCEL</i>	Receipt canceled
<i>POSNG_RECEIPT_CANCEL_WITH_WRITE_OFF</i>	Cancellation of a check with withdrawal
<i>POSNG_RECEIPT_DELAY</i>	Delayed receipt recorded
<i>POSNG_RECEIPT_DELAYED_RESTORE</i>	Delayed receipt requested

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_SOFT_REQUEST</i>	Soft receipt requested
<i>POSNG_RECEIPT_RECOVERY</i>	Receipt restored
<i>POSNG_RECEIPT_COPY</i>	Receipt copied

#### Calculation of receipt amount

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_PRELIMINARY_RESULT</i>	Cash payment subtotaled
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_CASHLESS</i>	Cashless payment subtotaled
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_SLIP_BEGIN</i>	Slip subtotal started
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_SLIP_FAIL</i>	Slip subtotal failed
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_SLIP</i>	Slip subtotaled
<i>POSNG_RECEIPT_FINAL_RESULT</i>	Receipt amount
<i>POSNG_RECEIPT_FINAL_RESULT_IS_UNKNOWN</i>	Receipt amount unknown
<i>POSNG_RECEIPT_FINAL_RESULT_IS_NULL</i>	Zero receipt
<i>POSNG_RECEIPT_CHANGE</i>	Change
<i>POSNG_RECEIPT_DISCOUNT_PROMO</i>	Discount application for the promo result
<i>POSNG_RECEIPT_DISCOUNT_ROUNDING</i>	Discount application for coin rounding result
<i>POSNG_RECEIPT_DISCOUNT_LOYALTY</i>	Discount application for loyalty result
<i>POSNG_RECEIPT_DISCOUNT</i>	Discount
<i>POSNG_DISCOUNT</i>	Discount
<i>POSNG_RECEIPT_DISCOUNT</i>	Discount canceled
<i>POSNG_RECEIPT_NUMBER</i>	Receipt number

#### Adding positions

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_ADD</i>	Position added to a receipt
<i>POSNG_POSITION_ADD_BY_ARTICLE</i>	Position added using stock number
<i>POSNG_POSITION_ADD_BY_BARCODE_MANUALLY</i>	Position added manually using barcode
<i>POSNG_POSITION_ADD_BY_SCANNER</i>	Position added using scanner
<i>POSNG_POSITION_ADD_BY_LIST</i>	Position added from a list
<i>POSNG_POSITION_ADD_BY_PRICE</i>	Position added based on price
<i>POSNG_ERROR_POSITION_NOT_FOUND_BY_ARTICLE</i>	Position not found using stock number
<i>POSNG_ERROR_POSITION_NOT_FOUND_BY_BARCODE</i>	Position not found using barcode
<i>POSNG_ERROR_POSITION_NOT_FOUND_BY_PRICE</i>	Position not found based on price
<i>POSNG_POSITION_SCAN_OUT_OF_RECEIPT</i>	Position not on receipt was scanned
<i>POSNG_POSITION_ADD_FORBIDDEN_GOODS</i>	Sale of prohibited position attempted
<i>POSNG_POSITION_ADD_PRESENT</i>	Gift added to receipt
<i>POSNG_POSITION_ENTER_AMOUNT_OF_GOODS_MANUALLY</i>	Cashier entered position quantity manually

#### Changing added positions

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_CHANGE</i>	Position changed somehow

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_AMOUNT_DECREASE_BEGIN</i>	Reduction of position quantity started
<i>POSNG_POSITION_AMOUNT_DECREASE_FAIL</i>	Reduction of position quantity failed
<i>POSNG_POSITION_AMOUNT_DECREASE</i>	Position quantity reduced
<i>POSNG_POSITION_AMOUNT_INCREASE_BEGIN</i>	Increase of position quantity started
<i>POSNG_POSITION_AMOUNT_INCREASE_FAIL</i>	Increase of position quantity failed
<i>POSNG_POSITION_AMOUNT_INCREASE</i>	Position quantity increased
<i>POSNG_POSITION_COST_DECREASE_BEGIN</i>	Position price reduction started
<i>POSNG_POSITION_COST_DECREASE_FAIL</i>	Position price reduction failed
<i>POSNG_POSITION_COST_DECREASE</i>	Position price reduced
<i>POSNG_POSITION_COST_INCREASE_BEGIN</i>	Position price increase started
<i>POSNG_POSITION_COST_INCREASE_FAIL</i>	Position price increase failed
<i>POSNG_POSITION_COST_INCREASE</i>	Position price increased

#### Deleting positions from a receipt

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_CANCEL_BEGIN</i>	Position cancellation started
<i>POSNG_POSITION_CANCEL_FAIL</i>	Position cancellation failed
<i>POSNG_POSITION_CANCEL</i>	Position canceled
<i>POSNG_POSITION_REMOVE_BEGIN</i>	Position deletion started
<i>POSNG_POSITION_REMOVE_FAIL</i>	Position deletion failed
<i>POSNG_POSITION_REMOVE</i>	Position deleted

#### Adding a discount to positions

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_DISCOUNT_BEGIN</i>	Attempt to assign discount to a good
<i>POSNG_POSITION_DISCOUNT_FAIL</i>	Position discount failed
<i>POSNG_POSITION_DISCOUNT_SELECT</i>	Position discount selected
<i>POSNG_POSITION_DISCOUNT</i>	Position discount assigned
<i>POSNG_POSITION_DISCOUNT_CANCEL</i>	Position discount canceled

#### Payment type

Event type ( <i>event_type</i> )	Description
<i>POSNG_PAYMENT_CREDIT_CARD</i>	Credit card payment
<i>POSNG_PAYMENT_CREDIT_CARD_FAIL</i>	Credit card payment failed
<i>POSNG_PAYMENT_INSIDER_CARD</i>	In-house credit card payment
<i>POSNG_PAYMENT_INSIDER_CARD</i>	In-house credit card payment
<i>POSNG_PAYMENT_INSIDER_CARD_FAIL</i>	In-house credit card payment failed
<i>POSNG_PAYMENT_DISCOUNT_CARD</i>	Loyalty card payment
<i>POSNG_PAYMENT_DISCOUNT_CARD_FAIL</i>	Loyalty card payment failed
<i>POSNG_PAYMENT_DISCOUNT_CARD_NOT_FOUND</i>	Loyalty card not found
<i>POSNG_PAYMENT_COUPON</i>	Coupon payment
<i>POSNG_PAYMENT_COUPON_FAIL</i>	Coupon payment failed



Event type ( <i>event_type</i> )	Description
<i>POSNG_PAYMENT_DOCUMENT</i>	Document payment
<i>POSNG_PAYMENT_BONUS_CARD_BEGIN</i>	Rewards card payment started
<i>POSNG_PAYMENT_BONUS_CARD_FAIL</i>	Rewards card payment failed
<i>POSNG_PAYMENT_BONUS_CARD</i>	Rewards card payment
<i>POSNG_PAYMENT_CERTIFICATE</i>	Payment certificate payment
<i>POSNG_PAYMENT_CASH</i>	Cash payment
<i>POSNG_PAYMENT_CASHLESS</i>	Cashless payment
<i>POSNG_PAYMENT_CANCEL</i>	Payment canceled
<i>POSNG_CARD_WAITING</i>	Waiting for card
<i>POSNG_CARD_NUMBER</i>	Card number received

### Modes

Event type ( <i>event_type</i> )	Description
<i>POSNG_MODE_RECEIPT_PRINT</i>	Receipt printing mode started
<i>POSNG_MODE_RECEIPT_PRINT_EXIT</i>	Receipt printing mode ended
<i>POSNG_MODE_RECEIPT_PRINT_EXIT</i>	Sales receipt printing mode
<i>POSNG_MODE_CASH_MEMO_PRINT_EXIT</i>	Sales receipt printing mode ended
<i>POSNG_MODE_SELL</i>	"Sales" mode started
<i>POSNG_MODE_SELL_EXIT</i>	"Sales" mode ended
<i>POSNG_MODE_SELL_EXIT</i>	"Return" mode started
<i>POSNG_MODE_RETURN_EXIT</i>	"Return" mode ended
<i>POSNG_MODE_SERVICE_PAYMENT</i>	"Service fee" mode started
<i>POSNG_MODE_SERVICE_PAYMENT_EXIT</i>	"Service fee" mode ended
<i>POSNG_MODE_CALCULATOR</i>	"Calculator" mode started
<i>POSNG_MODE_CALCULATOR_EXIT</i>	"Calculator" mode ended
<i>POSNG_MODE_PRODUCT_INFO</i>	"Product information" mode started
<i>POSNG_MODE_PRODUCT_INFO</i>	"Product information" mode ended

### Printing

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_PRINT</i>	Receipt printed
<i>POSNG_RECEIPT_PRINT_CASH_MEMO</i>	Sales receipt printed from "Cashier" mode
<i>POSNG_RECEIPT_PRINT_COPY</i>	Copy of receipt printed
<i>POSNG_RECEIPT_PRINT_COPY_ADMIN_MODE</i>	Copy of receipt printed from "Administrator" mode
<i>POSNG_SLIP_PRINT</i>	Slip printed
<i>POSNG_SLIP_PRINT_COPY</i>	Copy of slip printed

### Cash drawer

Event type ( <i>event_type</i> )	Description
<i>POSNG_MONEYBOX_OPEN</i>	Cash drawer opened during payment
<i>POSNG_MONEYBOX_OPEN_FORCED</i>	Cash drawer opened using button
<i>POSNG_MONEYBOX_DEPOSITION</i>	Cashier deposited cash in the register

Event type ( <i>event_type</i> )	Description
<i>POSNG_MONEYBOX_DEPOSITION_FINISHED</i>	Deposit finished
<i>POSNG_MONEYBOX_WITHDRAWAL</i>	Cash withdrawn from register
<i>POSNG_MONEYBOX_WITHDRAWAL_FINISHED</i>	Withdrawal finished
<i>POSNG_MONEYBOX_ADMIN_OPEN</i>	Cash drawer opened from "Administrator" mode
<i>POSNG_MONEYBOX_ADMIN_OPEN</i>	Administrator deposited cash in the register
<i>POSNG_MONEYBOX_ADMIN_DEPOSITION_FINISHED</i>	Administrator's deposit finished
<i>POSNG_MONEYBOX_ADMIN_WITHDRAWAL</i>	Cash withdrawn from register in Administrator mode
<i>POSNG_MONEYBOX_ADMIN_WITHDRAWAL_FINISHED</i>	Administrator's withdrawal finished
<i>POSNG_MONEYBOX_DECLARATION</i>	Cash drawer statement

#### Rewards cards

Event type ( <i>event_type</i> )	Description
<i>POSNG_BONUS_CARD_BALANCE_REQUEST</i>	Card balance requested
<i>POSNG_BONUS_CARD_ACTIVATE</i>	Card activated
<i>POSNG_BONUS_CARD_DEPOSITION</i>	Card deposit
<i>POSNG_BONUS_CARD_BONUS_DEPOSITION</i>	Rewards credited to card
<i>POSNG_BONUS_CARD_UNREGISTER</i>	Card unregistered
<i>POSNG_BONUS_CARD_BALANCE_DETAILED_REQUEST</i>	Detailed card balance requested

#### Payment certificates

Event type ( <i>event_type</i> )	Description
<i>POSNG_PAYMENT_CERTIFICATE_SELL</i>	Retail payment certificate sold

#### Cash-register system events

Event type ( <i>event_type</i> )	Description
<i>POSNG_SYSTEM_START</i>	Cash register started
<i>POSNG_SYSTEM_SHUTDOWN</i>	Cash register shut down
<i>POSNG_SYSTEM_REBOOT</i>	Cash register rebooted
<i>POSNG_SYSTEM_FMD_CREATE</i>	FMD created
<i>POSNG_SYSTEM_FMD_WRITE</i>	FMD recorded
<i>POSNG_SYSTEM_FMD_VIEW</i>	Control tape viewed
<i>POSNG_SYSTEM_FMD_PRINT</i>	Control tape from FMD printed
<i>POSNG_SYSTEM_SETUP_VIEW</i>	Cash register settings viewed
<i>POSNG_SYSTEM_SETUP_COLORS</i>	Colors configured
<i>POSNG_SYSTEM_CHECK_SALES_DATA</i>	Sales data checked
<i>POSNG_SYSTEM_DEVICE_KEEPLIVE</i>	Cash control
<i>POSNG_SYSTEM_DATABASE_CLEANUP</i>	Database cleaned up
<i>POSNG_SYSTEM_INFO</i>	System information

## Reports

Event type ( <i>event_type</i> )	Description
<i>POSNG_REPORT_DAILY</i>	Daily report printed
<i>POSNG_REPORT_BY_SECTIONS</i>	Section report printed
<i>POSNG_REPORT_X</i>	X Report printed
<i>POSNG_REPORT_Z</i>	Z Report printed
<i>POSNG_REPORT_Z_COPY</i>	Copy of Z Report printed
<i>POSNG_REPORT_FR</i>	FR report printed
<i>POSNG_REPORT_BY_CASHIERS</i>	Cashier report printed
<i>POSNG_REPORT_BY_GOODS</i>	Product report printed
<i>POSNG_REPORT_BY_TIME</i>	Time-based report printed
<i>POSNG_REPORT_BY_HOURS</i>	Hourly report printed
<i>POSNG_REPORT_BY_CASHLESS_OPERATIONS</i>	Cashless payment report printed
<i>POSNG_REPORT_BY_GROWING_RESULTS</i>	Cumulative totals report printed
<i>POSNG_REPORT_BY_BANK_OPERATIONS</i>	Bank operations report printed
<i>POSNG_REPORT_BY_SHIFT</i>	Shift report printed
<i>POSNG_REPORT_WRITE_OFF_ACT</i>	Write-off report printed

## Service events

Event type ( <i>event_type</i> )	Description
<i>POSNG_COMMENT</i>	Comments
<i>POSNG_ACTIVITY</i>	Operator activity
<i>POSNG_ACTION</i>	Action taken
<i>POSNG_FRAUD</i>	Incident event generated from a script
<i>POSNG_ERROR</i>	Error
<i>POSNG_ERROR_PRINTER</i>	Printer error
<i>POSNG_ERROR_BANK_PAYMENT</i>	Bank (payment) error
<i>POSNG_ERROR_NOT_A_NUMBER</i>	Non-numeric value entered
<i>POSNG_ERROR_NUMBER_TOO_LARGE</i>	Number entered is too large
<i>POSNG_BANK_CHECK_RESULTS</i>	Bank reconciliation
<i>POSNG_BANK_DAY_FINAL_RESULT_REQUEST</i>	Daily bank totals requested
<i>POSNG_BANK_DAY_CLOSE</i>	Bank day closed



- [DSSL XML for ActivePOS](#)
- [DSSL XML for hospitality business and public catering objects](#)
- [DSSL XML for warehouses](#)

## DSSL XML for hospitality business and public catering objects

### Shift events

Event type ( <i>event_type</i> )	Description
<i>POSNG_SHIFT_START</i>	The start of a shift
<i>POSNG_SHIFT_END</i>	The end of a shift
<i>POSNG_SHIFT_RESTORE</i>	The restoration of a shift
<i>POSNG_SHIFT_OVER_24H</i>	The shift has exceeded 24 hours

### User registration

Event type ( <i>event_type</i> )	Description
<i>POSNG_CASHIER_LOGIN_BEGIN</i>	Cashier sign-in started
<i>POSNG_CASHIER_LOGIN_FAIL</i>	Cashier sign-in failed
<i>POSNG_CASHIER_LOGIN</i>	Cashier sign-in succeeded
<i>POSNG_CASHIER_LOGOUT</i>	Cashier sign-out
<i>POSNG_ADMIN_LOGIN_BEGIN</i>	Administrator sign-in started
<i>POSNG_ADMIN_LOGIN_FAIL</i>	Administrator sign-in failed
<i>POSNG_ADMIN_LOGIN_FAIL</i>	Administrator sign-in succeeded
<i>POSNG_ADMIN_LOGOUT</i>	Administrator sign-out
<i>POSNG_TAX_OFFICER_LOGIN_BEGIN</i>	Tax officer sign-in started
<i>POSNG_TAX_OFFICER_LOGIN_FAIL</i>	Tax officer sign-in failed
<i>POSNG_TAX_OFFICER_LOGIN</i>	Tax officer sign-in succeeded
<i>POSNG_TAX_OFFICER_LOGOUT</i>	Tax officer sign-out

### Creating a receipt

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_OPEN</i>	Order is opened
<i>POSNG_RECEIPT_SELL_CLOSE</i>	Order is closed
<i>POSNG_RECEIPT_RETURN</i>	Redemption check beginning
<i>POSNG_RECEIPT_RETURN_CLOSE</i>	Redemption check end
<i>POSNG_RECEIPT_CANCEL_BEGIN</i>	Receipt cancellation started
<i>POSNG_RECEIPT_CANCEL_FAIL</i>	Receipt cancellation failed
<i>POSNG_RECEIPT_CANCEL</i>	Receipt canceled
<i>POSNG_RECEIPT_CANCEL_WITH_WRITE_OFF</i>	Cancellation of a check with withdrawal
<i>POSNG_RECEIPT_DELAY</i>	Delayed receipt recorded
<i>POSNG_RECEIPT_DELAYED_RESTORE</i>	Delayed receipt requested
<i>POSNG_RECEIPT_SOFT_REQUEST</i>	Soft receipt requested
<i>POSNG_RECEIPT_RECOVERY</i>	Receipt restored
<i>POSNG_RECEIPT_COPY</i>	Receipt copied

### Calculation of receipt amount

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_PRELIMINARY_RESULT</i>	Cash payment subtotaled

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_CASHLESS</i>	Cashless payment subtotaled
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_SLIP_BEGIN</i>	Slip subtotal started
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_SLIP_FAIL</i>	Slip subtotal failed
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_SLIP</i>	Slip subtotaled
<i>POSNG_RECEIPT_FINAL_RESULT</i>	Receipt amount
<i>POSNG_RECEIPT_FINAL_RESULT_IS_UNKNOWN</i>	Receipt amount unknown
<i>POSNG_RECEIPT_FINAL_RESULT_IS_NULL</i>	Zero receipt
<i>POSNG_RECEIPT_CHANGE</i>	Change
<i>POSNG_RECEIPT_DISCOUNT_PROMO</i>	Discount application to the promo result
<i>POSNG_RECEIPT_DISCOUNT_ROUNDING</i>	Discount application to the coin rounding result
<i>POSNG_RECEIPT_DISCOUNT_LOYALTY</i>	Discount application to the loyalty result
<i>POSNG_RECEIPT_DISCOUNT</i>	Discount
<i>POSNG_DISCOUNT</i>	Discount
<i>POSNG_RECEIPT_DISCOUNT</i>	Discount canceled
<i>POSNG_RECEIPT_NUMBER</i>	Receipt number

#### Adding positions

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_ADD</i>	Position added to a receipt
<i>POSNG_POSITION_ADD_BY_ARTICLE</i>	Position added using stock number
<i>POSNG_POSITION_ADD_BY_BARCODE_MANUALLY</i>	Position added manually using barcode
<i>POSNG_POSITION_ADD_BY_SCANNER</i>	Position added using scanner
<i>POSNG_POSITION_ADD_BY_LIST</i>	Position added from a list
<i>POSNG_POSITION_ADD_BY_PRICE</i>	Position added based on price
<i>POSNG_ERROR_POSITION_NOT_FOUND_BY_ARTICLE</i>	Position not found using stock number
<i>POSNG_ERROR_POSITION_NOT_FOUND_BY_BARCODE</i>	Position not found using barcode
<i>POSNG_ERROR_POSITION_NOT_FOUND_BY_PRICE</i>	Position not found based on price
<i>POSNG_POSITION_SCAN_OUT_OF_RECEIPT</i>	Position not on receipt was scanned
<i>POSNG_POSITION_ADD_FORBIDDEN_GOODS</i>	Sale of prohibited position attempted
<i>POSNG_POSITION_ADD_PRESENT</i>	Gift added to receipt

#### Changing added positions

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_CHANGE</i>	Position changed somehow
<i>POSNG_POSITION_AMOUNT_DECREASE_BEGIN</i>	Reduction of position quantity started
<i>POSNG_POSITION_AMOUNT_DECREASE_FAIL</i>	Reduction of position quantity failed
<i>POSNG_POSITION_AMOUNT_DECREASE</i>	Position quantity reduced
<i>POSNG_POSITION_AMOUNT_INCREASE_BEGIN</i>	Increase of position quantity started
<i>POSNG_POSITION_AMOUNT_INCREASE_FAIL</i>	Increase of position quantity failed
<i>POSNG_POSITION_AMOUNT_INCREASE</i>	Position quantity increased
<i>POSNG_POSITION_COST_DECREASE_BEGIN</i>	Position price reduction started

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_COST_DECREASE_FAIL</i>	Position price reduction failed
<i>POSNG_POSITION_COST_DECREASE</i>	Position price reduced
<i>POSNG_POSITION_COST_INCREASE_BEGIN</i>	Position price increase started
<i>POSNG_POSITION_COST_INCREASE_FAIL</i>	Position price increase failed
<i>POSNG_POSITION_COST_INCREASE</i>	Position price increased

#### Deleting positions from a receipt

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_CANCEL_BEGIN</i>	Position cancellation started
<i>POSNG_POSITION_CANCEL_FAIL</i>	Position cancellation failed
<i>POSNG_POSITION_CANCEL</i>	Position canceled
<i>POSNG_POSITION_REMOVE_BEGIN</i>	Position deletion started
<i>POSNG_POSITION_REMOVE_FAIL</i>	Position deletion failed
<i>POSNG_POSITION_REMOVE</i>	Position deleted

#### Adding a discount to positions

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_DISCOUNT_BEGIN</i>	Attempt to assign discount to a good
<i>POSNG_POSITION_DISCOUNT_FAIL</i>	Position discount failed
<i>POSNG_POSITION_DISCOUNT_SELECT</i>	Position discount selected
<i>POSNG_POSITION_DISCOUNT</i>	Position discount assigned
<i>POSNG_POSITION_DISCOUNT_CANCEL</i>	Position discount canceled

#### Payment type

Event type ( <i>event_type</i> )	Description
<i>POSNG_PAYMENT_CREDIT_CARD</i>	Credit card payment
<i>POSNG_PAYMENT_CREDIT_CARD_FAIL</i>	Credit card payment failed
<i>POSNG_PAYMENT_INSIDER_CARD</i>	In-house credit card payment
<i>POSNG_PAYMENT_INSIDER_CARD</i>	In-house credit card payment
<i>POSNG_PAYMENT_INSIDER_CARD_FAIL</i>	In-house credit card payment failed
<i>POSNG_PAYMENT_DISCOUNT_CARD</i>	Loyalty card payment
<i>POSNG_PAYMENT_DISCOUNT_CARD_FAIL</i>	Loyalty card payment failed
<i>POSNG_PAYMENT_DISCOUNT_CARD_NOT_FOUND</i>	Loyalty card not found
<i>POSNG_PAYMENT_COUPON</i>	Coupon payment
<i>POSNG_PAYMENT_COUPON_FAIL</i>	Coupon payment failed
<i>POSNG_PAYMENT_DOCUMENT</i>	Document payment
<i>POSNG_PAYMENT_BONUS_CARD_BEGIN</i>	Rewards card payment started
<i>POSNG_PAYMENT_BONUS_CARD_FAIL</i>	Rewards card payment failed
<i>POSNG_PAYMENT_BONUS_CARD</i>	Rewards card payment
<i>POSNG_PAYMENT_CERTIFICATE</i>	Payment certificate payment
<i>POSNG_PAYMENT_CASH</i>	Cash payment
<i>POSNG_PAYMENT_CASHLESS</i>	Cashless payment



Event type ( <i>event_type</i> )	Description
<i>POSNG_PAYMENT_CANCEL</i>	Payment canceled
<i>POSNG_CARD_WAITING</i>	Waiting for card
<i>POSNG_CARD_NUMBER</i>	Card number received

## Modes

Event type ( <i>event_type</i> )	Description
<i>POSNG_MODE_RECEIPT_PRINT</i>	Receipt printing mode started
<i>POSNG_MODE_RECEIPT_PRINT_EXIT</i>	Receipt printing mode ended
<i>POSNG_MODE_RECEIPT_PRINT_EXIT</i>	Sales receipt printing mode
<i>POSNG_MODE_CASH_MEMO_PRINT_EXIT</i>	Sales receipt printing mode ended
<i>POSNG_MODE_SELL</i>	"Sales" mode started
<i>POSNG_MODE_SELL_EXIT</i>	"Sales" mode ended
<i>POSNG_MODE_SELL_EXIT</i>	"Return" mode started
<i>POSNG_MODE_RETURN_EXIT</i>	"Return" mode ended
<i>POSNG_MODE_SERVICE_PAYMENT</i>	"Service fee" mode started
<i>POSNG_MODE_SERVICE_PAYMENT_EXIT</i>	"Service fee" mode ended
<i>POSNG_MODE_CALCULATOR</i>	"Calculator" mode started
<i>POSNG_MODE_CALCULATOR_EXIT</i>	"Calculator" mode ended
<i>POSNG_MODE_PRODUCT_INFO</i>	"Product information" mode started
<i>POSNG_MODE_PRODUCT_INFO</i>	"Product information" mode ended

## Printing

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_PRINT</i>	Receipt printed
<i>POSNG_RECEIPT_PRINT_CASH_MEMO</i>	Sales receipt printed from "Cashier" mode
<i>POSNG_RECEIPT_PRINT_COPY</i>	Copy of receipt printed
<i>POSNG_RECEIPT_PRINT_COPY_ADMIN_MODE</i>	Copy of receipt printed from "Administrator" mode
<i>POSNG_SLIP_PRINT</i>	Slip printed
<i>POSNG_SLIP_PRINT_COPY</i>	Copy of slip printed

## Cash drawer

Event type ( <i>event_type</i> )	Description
<i>POSNG_MONEYBOX_OPEN</i>	Cash drawer opened during payment
<i>POSNG_MONEYBOX_OPEN_FORCED</i>	Cash drawer opened using button
<i>POSNG_MONEYBOX_DEPOSITION</i>	Cashier deposited cash in the register
<i>POSNG_MONEYBOX_DEPOSITION_FINISHED</i>	Deposit finished
<i>POSNG_MONEYBOX_WITHDRAWAL</i>	Cash withdrawn from register
<i>POSNG_MONEYBOX_WITHDRAWAL_FINISHED</i>	Withdrawal finished
<i>POSNG_MONEYBOX_ADMIN_OPEN</i>	Cash drawer opened from "Administrator" mode
<i>POSNG_MONEYBOX_ADMIN_OPEN</i>	Administrator deposited cash in the register
<i>POSNG_MONEYBOX_ADMIN_DEPOSITION_FINISHED</i>	Administrator's deposit finished

Event type ( <i>event_type</i> )	Description
<i>POSNG_MONEYBOX_ADMIN_WITHDRAWAL</i>	Cash withdrawn from register in Administrator mode
<i>POSNG_MONEYBOX_ADMIN_WITHDRAWAL_FINISHED</i>	Administrator's withdrawal finished
<i>POSNG_MONEYBOX_DECLARATION</i>	Cash drawer statement

#### Rewards cards

Event type ( <i>event_type</i> )	Description
<i>POSNG_BONUS_CARD_BALANCE_REQUEST</i>	Card balance requested
<i>POSNG_BONUS_CARD_ACTIVATE</i>	Card activated
<i>POSNG_BONUS_CARD_DEPOSITION</i>	Card deposit
<i>POSNG_BONUS_CARD_BONUS_DEPOSITION</i>	Rewards credited to card
<i>POSNG_BONUS_CARD_UNREGISTER</i>	Card unregistered
<i>POSNG_BONUS_CARD_BALANCE_DETAILED_REQUEST</i>	Detailed card balance requested

#### Payment certificates

Event type ( <i>event_type</i> )	Description
<i>POSNG_PAYMENT_CERTIFICATE_SELL</i>	Retail payment certificate sold

#### Cash-register system events

Event type ( <i>event_type</i> )	Description
<i>POSNG_SYSTEM_START</i>	Cash register started
<i>POSNG_SYSTEM_SHUTDOWN</i>	Cash register shut down
<i>POSNG_SYSTEM_REBOOT</i>	Cash register rebooted
<i>POSNG_SYSTEM_FMD_CREATE</i>	FMD created
<i>POSNG_SYSTEM_FMD_WRITE</i>	FMD recorded
<i>POSNG_SYSTEM_FMD_VIEW</i>	Control tape viewed
<i>POSNG_SYSTEM_FMD_PRINT</i>	Control tape from FMD printed
<i>POSNG_SYSTEM_SETUP_VIEW</i>	Cash register settings viewed
<i>POSNG_SYSTEM_SETUP_COLORS</i>	Colors configured
<i>POSNG_SYSTEM_CHECK_SALES_DATA</i>	Sales data checked
<i>POSNG_SYSTEM_DEVICE_KEEPLIVE</i>	Cash control
<i>POSNG_SYSTEM_DATABASE_CLEANUP</i>	Database cleaned up
<i>POSNG_SYSTEM_INFO</i>	System information

#### Reports

Event type ( <i>event_type</i> )	Description
<i>POSNG_REPORT_DAILY</i>	Daily report printed
<i>POSNG_REPORT_BY_SECTIONS</i>	Section report printed
<i>POSNG_REPORT_X</i>	X Report printed
<i>POSNG_REPORT_Z</i>	Z Report printed
<i>POSNG_REPORT_Z_COPY</i>	Copy of Z Report printed
<i>POSNG_REPORT_FR</i>	FR report printed
<i>POSNG_REPORT_BY_CASHIERS</i>	Cashier report printed



Event type ( <i>event_type</i> )	Description
<i>POSNG_REPORT_BY_GOODS</i>	Product report printed
<i>POSNG_REPORT_BY_TIME</i>	Time-based report printed
<i>POSNG_REPORT_BY_HOURS</i>	Hourly report printed
<i>POSNG_REPORT_BY_CASHLESS_OPERATIONS</i>	Cashless payment report printed
<i>POSNG_REPORT_BY_GROWING_RESULTS</i>	Cumulative totals report printed
<i>POSNG_REPORT_BY_BANK_OPERATIONS</i>	Bank operations report printed
<i>POSNG_REPORT_BY_SHIFT</i>	Shift report printed
<i>POSNG_REPORT_WRITE_OFF_ACT</i>	Write-off report printed

#### Service events

Event type ( <i>event_type</i> )	Description
<i>POSNG_COMMENT</i>	Comments
<i>POSNG_ACTIVITY</i>	Operator activity
<i>POSNG_ACTION</i>	Action taken
<i>POSNG_FRAUD</i>	Incident event generated from a script
<i>POSNG_ERROR</i>	Error
<i>POSNG_ERROR_PRINTER</i>	Printer error
<i>POSNG_ERROR_BANK_PAYMENT</i>	Bank (payment) error
<i>POSNG_ERROR_NOT_A_NUMBER</i>	Non-numeric value entered
<i>POSNG_ERROR_NUMBER_TOO_LARGE</i>	Number entered is too large
<i>POSNG_BANK_CHECK_RESULTS</i>	Bank reconciliation
<i>POSNG_BANK_DAY_FINAL_RESULT_REQUEST</i>	Daily bank totals requested
<i>POSNG_BANK_DAY_CLOSE</i>	Bank day closed



- [DSSL XML for ActivePOS](#)
- [DSSL XML for trade objects](#)
- [DSSL XML for warehouses](#)

## DSSL XML for banknote counters and sorters

### Creating a receipt

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_OPEN</i>	New document "Banknote counting"
<i>POSNG_RECEIPT_CLOSE</i>	End of "Banknote counting" document

### Adding positions

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_ADD</i>	Adding banknotes/coins

### Calculation of receipt amount

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_FINAL_RESULT</i>	Receipt amount

### Reports

Event type ( <i>event_type</i> )	Description
<i>POSNG_REPORT_X</i>	X Report printed

### Service events

Event type ( <i>event_type</i> )	Description
<i>POSNG_COMMENT</i>	Comments
<i>POSNG_ERROR</i>	Error

### Banknote counters' events

Event type ( <i>event_type</i> )	Description
<i>POSNG_CASHCOUNTING_NUMBER_OF_REJECTS</i>	Rejects number
<i>POSNG_CASHCOUNTING_NUMBER_OF_BANKNOTES</i>	Banknotes number
<i>POSNG_CASHCOUNTING_NUMBER_OF_COINS</i>	Coins number
<i>POSNG_CASHCOUNTING_NUMBER_OF_COINS_NEEDED</i>	Number of coins required to complete packing procedure in all the bags
<i>POSNG_CASHCOUNTING_NUMBER_OF_BAGS</i>	Total number of finished bags packing
<i>POSNG_CASHCOUNTING_MODE_BATCHES</i>	Operation mode - packing
<i>POSNG_CASHCOUNTING_MODE_COUNT</i>	Operation mode - recounting/sorting
<i>POSNG_CASHCOUNTING_MODE_FINAL_SETTLEMENT</i>	Operation mode - total amount
<i>POSNG_CASHCOUNTING_BATCH_RESULT</i>	Packing result



- [DSSL XML for ActivePOS](#)
- [DSSL XML for trade objects](#)
- [DSSL XML for warehouses](#)

## DSSL XML for warehouses

## Receipt generation

Type of event ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_OPEN</i>	"Receipt" opening
<i>POSNG_RECEIPT_CLOSE</i>	"Receipt" closing
<i>POSNG_STOREHOUSE_CLIENT</i>	Client/supplier code (KLIENT)
<i>POSNG_STOREHOUSE_SSCC</i>	Pallet number (SSCC)
<i>POSNG_STOREHOUSE_TOLOCATION</i>	To the cell
<i>POSNG_STOREHOUSE_FROMLOCATION</i>	From the cell
<i>POSNG_STOREHOUSE_RETURN</i>	Return
<i>POSNG_STOREHOUSE_ISSUE</i>	Issue
<i>POSNG_STOREHOUSE_CHANGE_VALUE_FOR_QUALITY_CONTROL</i>	Blocking scope change for quality control
<i>POSNG_STOREHOUSE_CHANGE_INCOME</i>	Change of inflow
<i>POSNG_STOREHOUSE_CHANGE</i>	Change of storehouse
<i>POSNG_STOREHOUSE_CHANGE_WRAPPING</i>	Change of packing/repacking
<i>POSNG_STOREHOUSE_NVENTORY</i>	Inventory
<i>POSNG_STOREHOUSE_CORRECTION</i>	Correction
<i>POSNG_STOREHOUSE_UNLOADED</i>	Unloaded
<i>POSNG_STOREHOUSE_UNWRAPPED</i>	Unpacked
<i>POSNG_STOREHOUSE_SELECTION</i>	Selection
<i>POSNG_STOREHOUSE_SHIPMENT</i>	Shipment
<i>POSNG_STOREHOUSE_RESERVATION_CANCEL</i>	Customized reservation cancellation
<i>POSNG_STOREHOUSE_MOVING</i>	Moving
<i>POSNG_STOREHOUSE_MOVING_TO_PRODUCTION</i>	moving to production
<i>POSNG_STOREHOUSE_MOVING_BETWEEN_STOREHOUSES</i>	Moving between storehouses
<i>POSNG_STOREHOUSE_ADDITION</i>	Addition
<i>POSNG_STOREHOUSE_ACCEPTING</i>	Acceptance
<i>POSNG_STOREHOUSE_INCOME</i>	Inflow
<i>POSNG_STOREHOUSE_CHECK_SELECTED</i>	Selection check
<i>POSNG_STOREHOUSE_PRODUCTION</i>	Production
<i>POSNG_STOREHOUSE_PLACING</i>	Placement
<i>POSNG_STOREHOUSE_RESERVATION</i>	Customized reservation
<i>POSNG_STOREHOUSE_CHANGE_OWNER</i>	Change of ownership
<i>POSNG_STOREHOUSE_MIX_GOODS</i>	Mix lots
<i>POSNG_STOREHOUSE_SORTING</i>	Sorting
<i>POSNG_STOREHOUSE_WRITE_OFF</i>	Writing off
<i>POSNG_STOREHOUSE_DELETE_GOODS</i>	Remove storehouse commodity stock
<i>POSNG_STOREHOUSE_WRAPPING</i>	Packing



- *DSSL XML for ActivePOS*
- *DSSL XML for trade objects*
- *DSSL XML for hospitality business and public catering objects*
- *DSSL XML for banknote counters and sorters*

## DSSL XML for gas stations

### Shift events

Event type ( <i>event_type</i> )	Description
<i>POSNG_SHIFT_START</i>	The start of a shift
<i>POSNG_SHIFT_END</i>	The end of a shift
<i>POSNG_SHIFT_RESTORE</i>	The restoration of a shift
<i>POSNG_SHIFT_OVER_24H</i>	The shift has exceeded 24 hours

### User registration

Event type ( <i>event_type</i> )	Description
<i>POSNG_CASHIER_LOGIN_BEGIN</i>	Cashier sign-in started
<i>POSNG_CASHIER_LOGIN_FAIL</i>	Cashier sign-in failed
<i>POSNG_CASHIER_LOGIN</i>	Cashier sign-in succeeded
<i>POSNG_CASHIER_LOGOUT</i>	Cashier sign-out
<i>POSNG_ADMIN_LOGIN_BEGIN</i>	Administrator sign-in started
<i>POSNG_ADMIN_LOGIN_FAIL</i>	Administrator sign-in failed
<i>POSNG_ADMIN_LOGIN_FAIL</i>	Administrator sign-in succeeded
<i>POSNG_ADMIN_LOGOUT</i>	Administrator sign-out
<i>POSNG_TAX_OFFICER_LOGIN_BEGIN</i>	Tax officer sign-in started
<i>POSNG_TAX_OFFICER_LOGIN_FAIL</i>	Tax officer sign-in failed
<i>POSNG_TAX_OFFICER_LOGIN</i>	Tax officer sign-in succeeded
<i>POSNG_TAX_OFFICER_LOGOUT</i>	Tax officer sign-out

### Creating a receipt

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_OPEN</i>	Sales receipt opened
<i>POSNG_RECEIPT_SELL_CLOSE</i>	Sales receipt closed
<i>POSNG_RECEIPT_RETURN</i>	Return receipt opened
<i>POSNG_RECEIPT_RETURN_CLOSE</i>	Return receipt closed
<i>POSNG_RECEIPT_ANNULMENT</i>	New cancellation receipt
<i>POSNG_RECEIPT_EXCHANGE</i>	New exchange receipt
<i>POSNG_RECEIPT_EXCHANGE_CLOSE</i>	Exchange receipt closed
<i>POSNG_RECEIPT_PAYOUT</i>	New payout receipt
<i>POSNG_RECEIPT_PAYOUT_CLOSE</i>	Payout receipt closed
<i>POSNG_RECEIPT_REPAYMENT</i>	New repayment receipt
<i>POSNG_RECEIPT_CLOSE</i>	Receipt closed
<i>POSNG_RECEIPT_CANCEL_BEGIN</i>	Receipt cancellation started
<i>POSNG_RECEIPT_CANCEL_FAIL</i>	Receipt cancellation failed
<i>POSNG_RECEIPT_CANCEL</i>	Receipt canceled
<i>POSNG_RECEIPT_CANCEL_WITH_WRITE_OFF</i>	Cancellation of a check with withdrawal
<i>POSNG_RECEIPT_DELAY</i>	Delayed receipt recorded
<i>POSNG_RECEIPT_DELAYED_RESTORE</i>	Delayed receipt requested

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_SOFT_REQUEST</i>	Soft receipt requested
<i>POSNG_RECEIPT_RECOVERY</i>	Receipt restored
<i>POSNG_RECEIPT_COPY</i>	Receipt copied

#### Calculation of receipt amount

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_PRELIMINARY_RESULT</i>	Cash payment subtotaled
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_CASHLESS</i>	Cashless payment subtotaled
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_SLIP_BEGIN</i>	Slip subtotal started
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_SLIP_FAIL</i>	Slip subtotal failed
<i>POSNG_RECEIPT_PRELIMINARY_RESULT_SLIP</i>	Slip subtotaled
<i>POSNG_RECEIPT_FINAL_RESULT</i>	Receipt amount
<i>POSNG_RECEIPT_FINAL_RESULT_IS_UNKNOWN</i>	Receipt amount unknown
<i>POSNG_RECEIPT_FINAL_RESULT_IS_NULL</i>	Zero receipt
<i>POSNG_RECEIPT_CHANGE</i>	Change
<i>POSNG_RECEIPT_DISCOUNT_PROMO</i>	Discount application to the promo result
<i>POSNG_RECEIPT_DISCOUNT_ROUNDING</i>	Discount application for coin rounding result
<i>POSNG_RECEIPT_DISCOUNT_LOYALTY</i>	Discount application for loyalty result
<i>POSNG_RECEIPT_DISCOUNT</i>	Discount
<i>POSNG_DISCOUNT</i>	Discount
<i>POSNG_RECEIPT_DISCOUNT</i>	Discount canceled
<i>POSNG_RECEIPT_NUMBER</i>	Receipt number

#### Adding positions

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_ADD</i>	Position added to a receipt
<i>POSNG_POSITION_ADD_BY_ARTICLE</i>	Position added using stock number
<i>POSNG_POSITION_ADD_BY_BARCODE_MANUALLY</i>	Position added manually using barcode
<i>POSNG_POSITION_ADD_BY_SCANNER</i>	Position added using scanner
<i>POSNG_POSITION_ADD_BY_LIST</i>	Position added from a list
<i>POSNG_POSITION_ADD_BY_PRICE</i>	Position added based on price
<i>POSNG_ERROR_POSITION_NOT_FOUND_BY_ARTICLE</i>	Position not found using stock number
<i>POSNG_ERROR_POSITION_NOT_FOUND_BY_BARCODE</i>	Position not found using barcode
<i>POSNG_ERROR_POSITION_NOT_FOUND_BY_PRICE</i>	Position not found based on price
<i>POSNG_POSITION_SCAN_OUT_OF_RECEIPT</i>	Position not on receipt was scanned
<i>POSNG_POSITION_ADD_FORBIDDEN_GOODS</i>	Sale of prohibited position attempted
<i>POSNG_POSITION_ADD_PRESENT</i>	Gift added to receipt
<i>POSNG_POSITION_ENTER_AMOUNT_OF_GOODS_MANUALLY</i>	Cashier entered position quantity manually

#### Changing added positions

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_CHANGE</i>	Position changed somehow

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_AMOUNT_DECREASE_BEGIN</i>	Reduction of position quantity started
<i>POSNG_POSITION_AMOUNT_DECREASE_FAIL</i>	Reduction of position quantity failed
<i>POSNG_POSITION_AMOUNT_DECREASE</i>	Position quantity reduced
<i>POSNG_POSITION_AMOUNT_INCREASE_BEGIN</i>	Increase of position quantity started
<i>POSNG_POSITION_AMOUNT_INCREASE_FAIL</i>	Increase of position quantity failed
<i>POSNG_POSITION_AMOUNT_INCREASE</i>	Position quantity increased
<i>POSNG_POSITION_COST_DECREASE_BEGIN</i>	Position price reduction started
<i>POSNG_POSITION_COST_DECREASE_FAIL</i>	Position price reduction failed
<i>POSNG_POSITION_COST_DECREASE</i>	Position price reduced
<i>POSNG_POSITION_COST_INCREASE_BEGIN</i>	Position price increase started
<i>POSNG_POSITION_COST_INCREASE_FAIL</i>	Position price increase failed
<i>POSNG_POSITION_COST_INCREASE</i>	Position price increased

#### Deleting positions from a receipt

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_CANCEL_BEGIN</i>	Position cancellation started
<i>POSNG_POSITION_CANCEL_FAIL</i>	Position cancellation failed
<i>POSNG_POSITION_CANCEL</i>	Position canceled
<i>POSNG_POSITION_REMOVE_BEGIN</i>	Position deletion started
<i>POSNG_POSITION_REMOVE_FAIL</i>	Position deletion failed
<i>POSNG_POSITION_REMOVE</i>	Position deleted

#### Adding a discount to positions

Event type ( <i>event_type</i> )	Description
<i>POSNG_POSITION_DISCOUNT_BEGIN</i>	Attempt to assign discount to a good
<i>POSNG_POSITION_DISCOUNT_FAIL</i>	Position discount failed
<i>POSNG_POSITION_DISCOUNT_SELECT</i>	Position discount selected
<i>POSNG_POSITION_DISCOUNT</i>	Position discount assigned
<i>POSNG_POSITION_DISCOUNT_CANCEL</i>	Position discount canceled

#### Payment type

Event type ( <i>event_type</i> )	Description
<i>POSNG_PAYMENT_CREDIT_CARD</i>	Credit card payment
<i>POSNG_PAYMENT_CREDIT_CARD_FAIL</i>	Credit card payment failed
<i>POSNG_PAYMENT_INSIDER_CARD</i>	In-house credit card payment
<i>POSNG_PAYMENT_INSIDER_CARD</i>	In-house credit card payment
<i>POSNG_PAYMENT_INSIDER_CARD_FAIL</i>	In-house credit card payment failed
<i>POSNG_PAYMENT_DISCOUNT_CARD</i>	Loyalty card payment
<i>POSNG_PAYMENT_DISCOUNT_CARD_FAIL</i>	Loyalty card payment failed
<i>POSNG_PAYMENT_DISCOUNT_CARD_NOT_FOUND</i>	Loyalty card not found
<i>POSNG_PAYMENT_COUPON</i>	Coupon payment
<i>POSNG_PAYMENT_COUPON_FAIL</i>	Coupon payment failed



Event type ( <i>event_type</i> )	Description
<i>POSNG_PAYMENT_DOCUMENT</i>	Document payment
<i>POSNG_PAYMENT_BONUS_CARD_BEGIN</i>	Rewards card payment started
<i>POSNG_PAYMENT_BONUS_CARD_FAIL</i>	Rewards card payment failed
<i>POSNG_PAYMENT_BONUS_CARD</i>	Rewards card payment
<i>POSNG_PAYMENT_CERTIFICATE</i>	Payment certificate payment
<i>POSNG_PAYMENT_CASH</i>	Cash payment
<i>POSNG_PAYMENT_CASHLESS</i>	Cashless payment
<i>POSNG_PAYMENT_CANCEL</i>	Payment canceled
<i>POSNG_CARD_WAITING</i>	Waiting for card
<i>POSNG_CARD_NUMBER</i>	Card number received
<i>POSNG_PAYMENT_FUEL_CARD</i>	Payment by fuel card
<i>POSNG_PAYMENT_FUEL_CARD_FAIL</i>	Refusal for fuel card payment

### Modes

Event type ( <i>event_type</i> )	Description
<i>POSNG_MODE_RECEIPT_PRINT</i>	Receipt printing mode started
<i>POSNG_MODE_RECEIPT_PRINT_EXIT</i>	Receipt printing mode ended
<i>POSNG_MODE_RECEIPT_PRINT_EXIT</i>	Sales receipt printing mode
<i>POSNG_MODE_CASH_MEMO_PRINT_EXIT</i>	Sales receipt printing mode ended
<i>POSNG_MODE_SELL</i>	"Sales" mode started
<i>POSNG_MODE_SELL_EXIT</i>	"Sales" mode ended
<i>POSNG_MODE_SELL_EXIT</i>	"Return" mode started
<i>POSNG_MODE_RETURN_EXIT</i>	"Return" mode ended
<i>POSNG_MODE_SERVICE_PAYMENT</i>	"Service fee" mode started
<i>POSNG_MODE_SERVICE_PAYMENT_EXIT</i>	"Service fee" mode ended
<i>POSNG_MODE_CALCULATOR</i>	"Calculator" mode started
<i>POSNG_MODE_CALCULATOR_EXIT</i>	"Calculator" mode ended
<i>POSNG_MODE_PRODUCT_INFO</i>	"Product information" mode started
<i>POSNG_MODE_PRODUCT_INFO</i>	"Product information" mode ended
<i>POSNG_MODE_ENTER</i>	Entering mode, or window
<i>POSNG_MODE_EXIT</i>	Exiting mode, or window

### Printing

Event type ( <i>event_type</i> )	Description
<i>POSNG_RECEIPT_PRINT</i>	Receipt printed
<i>POSNG_RECEIPT_PRINT_CASH_MEMO</i>	Sales receipt printed from "Cashier" mode
<i>POSNG_RECEIPT_PRINT_COPY</i>	Copy of receipt printed
<i>POSNG_RECEIPT_PRINT_COPY_ADMIN_MODE</i>	Copy of receipt printed from "Administrator" mode
<i>POSNG_SLIP_PRINT</i>	Slip printed
<i>POSNG_SLIP_PRINT_COPY</i>	Copy of slip printed



## Cash drawer

Event type ( <i>event_type</i> )	Description
<i>POSNG_MONEYBOX_OPEN</i>	Cash drawer opened during payment
<i>POSNG_MONEYBOX_OPEN_FORCED</i>	Cash drawer opened using button
<i>POSNG_MONEYBOX_DEPOSITION</i>	Cashier deposited cash in the register
<i>POSNG_MONEYBOX_DEPOSITION_FINISHED</i>	Deposit finished
<i>POSNG_MONEYBOX_WITHDRAWAL</i>	Cash withdrawn from register
<i>POSNG_MONEYBOX_WITHDRAWAL_FINISHED</i>	Withdrawal finished
<i>POSNG_MONEYBOX_ADMIN_OPEN</i>	Cash drawer opened from "Administrator" mode
<i>POSNG_MONEYBOX_ADMIN_OPEN</i>	Administrator deposited cash in the register
<i>POSNG_MONEYBOX_ADMIN_DEPOSITION_FINISHED</i>	Administrator's deposit finished
<i>POSNG_MONEYBOX_ADMIN_WITHDRAWAL</i>	Cash withdrawn from register in Administrator mode
<i>POSNG_MONEYBOX_ADMIN_WITHDRAWAL_FINISHED</i>	Administrator's withdrawal finished
<i>POSNG_MONEYBOX_DECLARATION</i>	Cash drawer statement

## Cards

Event type ( <i>event_type</i> )	Description
<i>POSNG_BONUS_CARD_BALANCE_REQUEST</i>	Card balance requested
<i>POSNG_BONUS_CARD_ACTIVATE</i>	Card activated
<i>POSNG_BONUS_CARD_DEPOSITION</i>	Card deposit
<i>POSNG_BONUS_CARD_BONUS_DEPOSITION</i>	Rewards credited to card
<i>POSNG_BONUS_CARD_UNREGISTER</i>	Card unregistered
<i>POSNG_BONUS_CARD_BALANCE_DETAILED_REQUEST</i>	Detailed card balance requested
<i>POSNG_CREDIT_CARD</i>	Random credit card event
<i>POSNG_DISCOUNT_CARD</i>	Random discount card event
<i>POSNG_BONUS_CARD</i>	Random bonus card event
<i>POSNG_FUEL_CARD</i>	Random fuel card event
<i>POSNG_FUEL_CARD_BALANCE</i>	Fuel card balance

## Payment certificates

Event type ( <i>event_type</i> )	Description
<i>POSNG_PAYMENT_CERTIFICATE_SELL</i>	Retail payment certificate sold

## Cash-register system events

Event type ( <i>event_type</i> )	Description
<i>POSNG_SYSTEM_START</i>	Cash register started
<i>POSNG_SYSTEM_SHUTDOWN</i>	Cash register shut down
<i>POSNG_SYSTEM_REBOOT</i>	Cash register rebooted
<i>POSNG_SYSTEM_FMD_CREATE</i>	FMD created
<i>POSNG_SYSTEM_FMD_WRITE</i>	FMD recorded
<i>POSNG_SYSTEM_FMD_VIEW</i>	Control tape viewed

Event type ( <i>event_type</i> )	Description
<i>POSNG_SYSTEM_FMD_PRINT</i>	Control tape from FMD printed
<i>POSNG_SYSTEM_SETUP_VIEW</i>	Cash register settings viewed
<i>POSNG_SYSTEM_SETUP_COLORS</i>	Colors configured
<i>POSNG_SYSTEM_CHECK_SALES_DATA</i>	Sales data checked
<i>POSNG_SYSTEM_DEVICE_KEEPLIVE</i>	Cash control
<i>POSNG_SYSTEM_DATABASE_CLEANUP</i>	Database cleaned up
<i>POSNG_SYSTEM_INFO</i>	System information

## Reports

Event type ( <i>event_type</i> )	Description
<i>POSNG_REPORT_DAILY</i>	Daily report printed
<i>POSNG_REPORT_BY_SECTIONS</i>	Section report printed
<i>POSNG_REPORT_X</i>	X Report printed
<i>POSNG_REPORT_Z</i>	Z Report printed
<i>POSNG_REPORT_Z_COPY</i>	Copy of Z Report printed
<i>POSNG_REPORT_FR</i>	FR report printed
<i>POSNG_REPORT_BY_CASHIERS</i>	Cashier report printed
<i>POSNG_REPORT_BY_GOODS</i>	Product report printed
<i>POSNG_REPORT_BY_TIME</i>	Time-based report printed
<i>POSNG_REPORT_BY_HOURS</i>	Hourly report printed
<i>POSNG_REPORT_BY_CASHLESS_OPERATIONS</i>	Cashless payment report printed
<i>POSNG_REPORT_BY_GROWING_RESULTS</i>	Cumulative totals report printed
<i>POSNG_REPORT_BY_BANK_OPERATIONS</i>	Bank operations report printed
<i>POSNG_REPORT_BY_SHIFT</i>	Shift report printed
<i>POSNG_REPORT_WRITE_OFF_ACT</i>	Write-off report printed

## Service events

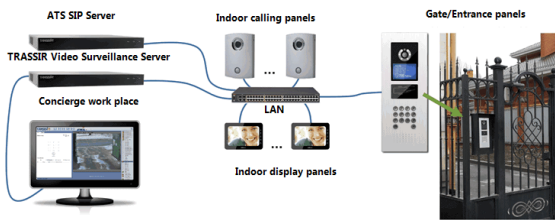
Event type ( <i>event_type</i> )	Description
<i>POSNG_COMMENT</i>	Comments
<i>POSNG_ACTIVITY</i>	Operator activity
<i>POSNG_ACTION</i>	Action taken
<i>POSNG_FRAUD</i>	Incident event generated from a script
<i>POSNG_ERROR</i>	Error
<i>POSNG_ERROR_PRINTER</i>	Printer error
<i>POSNG_ERROR_BANK_PAYMENT</i>	Bank (payment) error
<i>POSNG_ERROR_NOT_A_NUMBER</i>	Non-numeric value entered
<i>POSNG_ERROR_NUMBER_TOO_LARGE</i>	Number entered is too large
<i>POSNG_BANK_CHECK_RESULTS</i>	Bank reconciliation
<i>POSNG_BANK_DAY_FINAL_RESULT_REQUEST</i>	Daily bank totals requested
<i>POSNG_BANK_DAY_CLOSE</i>	Bank day closed
<i>POSNG_ERROR_SYSTEM</i>	System error



- *DSSL XML for ActivePOS*
- *DSSL XML for hospitality business and public catering objects*
- *DSSL XML for warehouses*

## IP-video intercom

TRASSIR can combine your video surveillance system and IP-video home entry system into a unified complex.



The list of available TRASSIR features depends on module which is determined by license.

Feature	TRASSIR Video Intercom	TRASSIR Intercom	TRASSIR Intercom Concierge
Video record from IP-videophone entry system	+		
Video/audio data synchronization from control panels and videosurveillance system devices	+	+	
Call recording and the archive maintenance	+	+	
Search for video/audio connection in the archive by the subscriber's number, date and time, call duration, outgoing, incoming and missed calls	+	+	
IP-videophone device status monitoring	+	+	
Full scale SipPhone in TRASSIR interface			+
Keeping the call log			+

All of that is possible due to the to dial exchange IP integration to TRASSIR [Asterisk](#).



TRASSIR software works with Asterisk 11.13.1 version and FreePBX 12.0.33 version  
Upgrade Asterisk software in case you use earlier versions.

See below module settings procedure. The module operation principles are described in "Operator's Guide" (???)



- [Connection to Asterisk server](#)
- [SipPhone server settings](#)
- [SipPhone on the client settings](#)

## Connection to Asterisk server

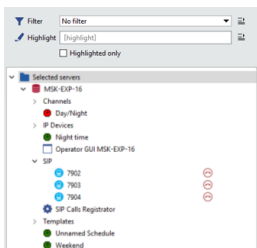
**AMI (Asterisk Management Interface)** is Asterisk(API) server control interface. Due to it TRASSIR makes connection to Asterisk server via TCP, initiate instructions execution, receives the result of their execution and receives current status of SIP-phones.

Enter the following parameters to connect to Asterisk:

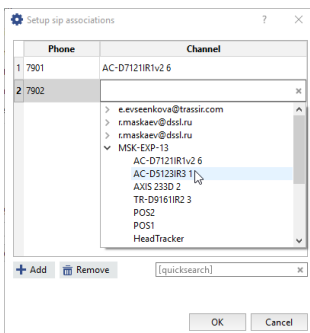
- **AMI server** - server ip-address or DNS-name.
- **AMI port** - network port of server (by default: 5038).
- **AMI user** and **AMI password** - server account name and password.

The status of connection to dial office IP is displayed in **Status** field. In case all parameters are specified correctly, **Connected** line will appear. Otherwise you'll see error message.

Specify SIP-phone numbers in **Monitoring phones** field and you will be able to trace their status in the object tree(CMS).



When calling to phone, TRASSIR can output video from camera to operator's display. It requires **Set up associations...**, that is indicate SIP-phone number and video channel corresponding to it.



This function can be used, for example, in IP-video home entry system. When visitor presses video home entry device, the call is effected to corresponding number and video transmitted by video home entry device is displayed on the security post display.



Devices status from the field **Monitoring phones** and **Setup associations** will be sent to all SIP-phones with this server **defined as Master Trassir**.

**Call archive** is used to store audio data and complete information about the calls going via telephone exchange IP. Server with archive shall have installed data base and FTP-server. Enter the following parameters for connection:

- **Driver** - data base type: **MySQL** or **PostgreSQL**.

- **Server** - server with database IP-address or DNS-name.
- **Port** - server with database network port.
- **Data base name** - the name of the data base.
- **User** and **Password** - user account and password on database server
- **Audio files URL** - address of FTP-server and folder where calls audio records will be stored.  
Server address should be specified as `ftp://[ip-address]:[port]/[folder]`.  
For example, `ftp://192.168.5.77:21/var/spool/asterisk/monitor`.
- **FTP user** and **FTP password** - user name and password to access to FTP-server.
- **Maximum depth** - depth of audio records storage. On default Asterisk uses 3-level system of audio records storage - /year/month/day. Modify parameter value in case you have other settings.

Status of connection to database and FTP server is displayed in the **Status** field. In case all parameters are specified correctly, **Connected** line will appear. Otherwise you'll see the error message.



- [IP-video intercom](#)
- [SipPhone server settings](#)

## SipPhone server settings

To start using SipPhone plugin in TRASSIR, the below described settings should be configured. After that, TRASSIR server operator will be able to call Asterisk subscribers, receive calls and send service instructions.

The screenshot shows a 'Setup' window with a 'Help' tab. The 'Current state' is 'Connected'. Under 'Connection Options', there are fields for 'Asterisk host' (localhost), 'Asterisk port' (5060), 'User' (7908), 'Password' (masked with dots), 'DND on' (\*78), 'DND off' (\*79), and 'Code'. At the bottom, there is a 'Master Trassir' dropdown menu with 'MSK-EXP-16' selected.



First of all, for each TRASSIR server, an account on Asterisk server should be created. TRASSIR server operator will use it to receive and make calls.

Set up **Connection parameters**:

- **Asterisk server** - Asterisk server IP-address or DNS-name.
- **Asterisk port** - Asterisk server network port (by default: 5060).
- **User** and **Password** - account name (phone number) and password on Asterisk server.
- **Activate DND** and **Deactivate DND** are commands sent to server to activate and deactivate DND ("Do Not Disturb") mode
- **Key** - a command to open the door sent to home entry system device from operator's interface.

The status of connection to dial office IP is displayed in the **Status** field. In case all parameters are specified correctly, **Connected** line will appear. Otherwise you'll see error message.

In case you would like the current server operator to have access to the calls history, phone talk records and set associations of channels, select in **Master TRASSIR** field name of server on which [connection to AMI server](#) is set.



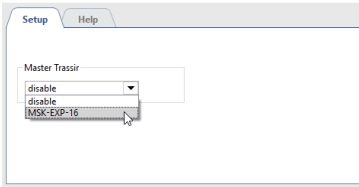
Selecting a server as **Master Trassir** will be possible only after the connection to it. See detailed description of connection to server procedure in the section [Connecting to a new server](#).



- [IP-video intercom](#)
- [Connection to Asterisk server](#)

## SipPhone on the client settings

To start using SipPhone plugin in TRASSIR Client, the below described settings should be configured.



In order to provide server operator with access to the calls history, phone talk records and set associations of channels, select in **Master Trassir** field name of server on which [connection to AMI server](#) is set.



Server selection as **Master Trassir** will be possible only after connection to it. See detailed description of connection to server procedure in the section [Connecting to a new server](#).



- [IP-video intercom](#)



## AutoTRASSIR - Automated license plate recognition

AutoTRASSIR is designed for automatic recognition of license plates caught in video camera field of view. It can be used in video surveillance system to monitor vehicles entry/exit from the territory of industrial areas, parking lots, checkpoints, etc.

In addition, the TRASSIR means can provide interaction with other systems (for example, access control systems, video and audio control) and equipment (barriers, actuators, etc.).



AutoTRASSIR is available in 2 variants: "fast" (up to 200 km/h), and "slow" (up to 30 km/h). This parameter is determined by the license, adjustment of both types in TRASSIR is identical. TRASSIR has several versions of AutoTRASSIR mode included, which have a number of specific features:

The **AutoTRASSIR (LPR1)** and **AutoTRASSIR (LPR3)** plugins run **locally** on all TRASSIR servers.

The **AutoTRASSIR (LPR5)** plugin runs:

- **local** for **NeuroStation** and **QuattroStation** server with TRASSIR OS;
- **remotely** on all TRASSIR servers.



**AutoTRASSIR (LPR5)** settings peculiarities in remote working mode:

- The server with license plate recognizing cameras should be connected to TRASSIR OS server, which will be used as **Analytics server**.  
**AutoTRASSIR (LPR5)** can use TRASSIR OS server **NeuroStation** version as analytics server. Read more about server connection in [Connecting to a new server](#).
- [Enable network analytics](#) in the settings of the user that should be connected to analytics server.
- [General AutoTRASSIR module setup](#) is performed on the server, to which the cameras are connected. Analytics server only allows to choose **LPR version**.
- AutoTRASSIR module type ("quick" or "slow") **is defined by the analytics server license**.

AutoTRASSIR features:

- **License plate reading by templates and without them**

AutoTRASSIR can recognize license plates of the following countries: Russia, Ukraine, Turkey, Taiwan, Moldova, Kyrgyzstan, Qazaqstan, Spain, Georgia, Belorussia, China, etc. The operation of the recognition templates depends on the selected AutoTRASSIR plugin version:

**LPR5** - with TRASSIR neural network solutions on several templates simultaneously and without if the countries are not in the list of AutoTRASSIR templates.

**LPR3** - simultaneously with several templates or without template if the country is not in AutoTRASSIR template list.

**LPR1** - with single template, which is defined by TRASSIR license.



Chinese license plate number recognition is not supported by AutoTRASSIR (LPR5).

- **Working with internal and external databases**

Live search of recognized license plates. Use of databases as white ("friend"), black ("foe") and/or information lists. Saving of the recognized license plate numbers in the internal database with time and date of passage, links to video information, etc. Advanced search and editing of license plate numbers in the internal database.

- **Operator's interface**

Displaying video information about a vehicle and its license plate number, simultaneously from several cameras. Searchable recognized license plate numbers register.



- *AutoTRASSIR general settings*

## Selecting, installing, and configuring cameras to work with the AutoTRASSIR module

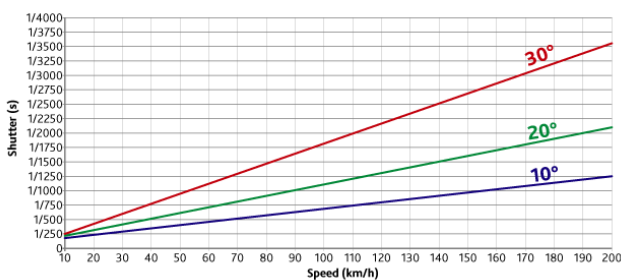
The correct selection of a video surveillance camera and its proper installation and configuration are among the key requirements for the correct operation of the AutoTRASSIR module. We recommend that you read the Administrator's Guide very carefully.

Both analogue and IP cameras can be used for state license plate number recognition.

The AutoTRASSIR (LPR5) plugin can use image from any video surveillance camera. When using AutoTRASSIR (LPR1/LPR3) plugins, it is recommended to use black and white camera image since it features greater (comparing to the color) resolution capability and sensitivity. (The color image camera will be converted to black and white by recognition). The analogue video surveillance camera, used for AutoTRASSIR plugin must have resolution starting from 500 TVL (Television vertical Lines, picture definition).

The primary problem affecting image quality during license plate recognition is motion blur. To avoid motion blur, the shutter speed (the time each frame is exposed) must be very small.

The maximum shutter speed depends on the vehicle speed and the camera's installation angle (see the figure). The camera installation angle is the angle between the optical axis of the camera and the direction of vehicle motion.



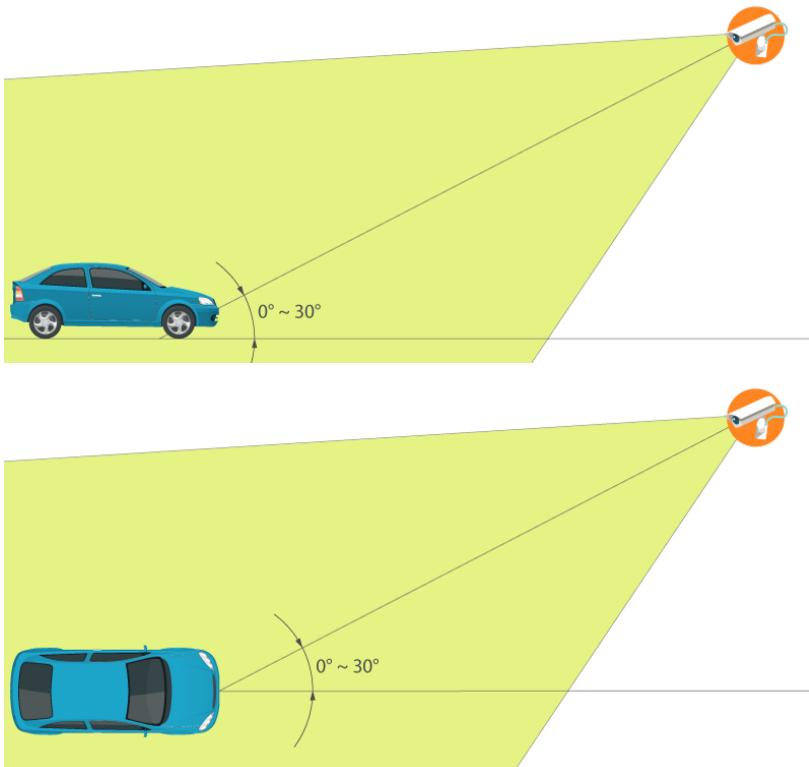
The shutter speed must be fixed or, if the camera supports it, a maximum shutter speed must be set.



The camera must support setting the shutter speed manually!

For example, given a camera installation angle of 20° and a speed of 80 km/h, the shutter speed must be set at 1/1000 of a second (see the figure).

In order to avoid number recognition errors when using the AutoTRASSIR module (LPR1 / LPR3), the camera should be installed so that the vehicle number is perpendicular to the camera. For AutoTRASSIR (LPR5) module, the camera can be installed at the angle to the direction of the vehicle movement. The angle should not be more than 30°. The higher the angle is, the lower is the license plate recognition quality.



Given large camera installation angles, the time of vehicle passes through the camera's field of view must also be considered. For good recognition results, the camera should capture at least 10 frames of the license plate number being recognized.

It is necessary to watch the license plate number was located horizontally on the image. The AutoTRASSIR (LPR5) module allows the license plate number deviation up to  $5^\circ$  from the horizontal, without the loss of recognition quality. If the number deviates to  $5^\circ$  -  $10^\circ$  from the horizontal, errors in recognition of some characters may occur.

If swing barriers are used to control entrances/exits, we recommend installing the camera in such a way that the swing barrier does not reach the bottom of the screen. Otherwise, the swing barrier may cause false positives.

Verify that there is sufficient brightness during nighttime conditions. To do this, record a small section of video. License plate numbers should be easily recognized during playback. If the license plate images to noisy or dark, the rightness must be increased or the lens must be replaced with a higher-aperture lens. Also be sure that the lens diaphragm is fully open. We do not recommend installing the camera at a low height, because it night the camera will be overexposed by the headlights of passing vehicles.

Other camera settings include:

- Autofocus must be disabled.
- The superposition of any information onto the image (date, camera name, etc.) must be disabled.
- The focal length must be set such that the license plate is approximately 120-140 pixels along the horizontal in the analyzed video. Learn more in the [AutoTRASSIR settings](#) section.



- [AutoTRASSIR - Automated license plate recognition](#)
- [AutoTRASSIR settings](#)

## AutoTRASSIR general settings



Before the AutoTRASSIR configuration, we strongly recommend you to read the section [AutoTRASSIR - Automated license plate recognition](#).

Before using the AutoTRASSIR module, be sure you have correctly configured your [database connection](#).

Main parameters of the AutoTRASSIR module are displayed on the **Plugins** -> **AutoTRASSIR** tab of the **Settings** window.

- In the **LPR core** configuration, select the version of AutoTRASSIR.



After changing the version of the module, the server must be rebooted.

- In the **Country preset** you can select the country in which license plate recognition will take place. Furthermore, the templates of the selected country and of the neighboring ones will be displayed in **Visualization templates** list. You can also select **custom** item and enable the required templates manually.



AutoTRASSIR recognizes license plates regardless of the selected country visualization template. The display of the visualization templates is required only in the operator's interface. Thus, if the recognized license plate corresponds to the selected country template, it will be displayed in that country format in operator's interface.

or

Otherwise, the recognized license plate will be displayed as a set of recognized characters.



Select **Chinese** in **OCR type** setting in order to increase the quality of Chinese license plate recognition in AutoTRASSIR (LPR3). Use **standard** OCR type in any other cases.

- The **Licenses usage** field shows the number of currently connected channels out of the maximum allowed (which is limited by your license).
- The **Channels** section displays the list of channels for which AutoTRASSIR has been activated.
- The **Mismatch with list record** setting lets you set up mismatch which can be used for the recognized numbers search in the [internal lists](#), from **0** to **5** symbols.



E.g. the **Mismatch with list record threshold** value is set to **1** and the license plate number **m221co177** is in the whitelist.

In case AutoTRASSIR makes a mistake in 1 symbol when recognizing a license plate and recognizes **a221co177** or **m221co77** instead of **m221co177** number, due to 1 symbol mismatch, the mistakenly recognized number with match with the number from the whitelist.

- The **External lists** area displays a list of all of the **external lists connected to AutoTRASSIR**.

Configuring AutoTRASSIR typically includes several stages:

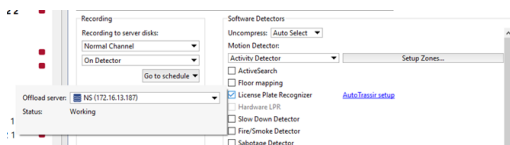
1. Install and configure in TRASSIR the cameras that will be used for license plate number recognition.



In order for the license plate number recognition system to work properly, the camera must have a number of technical characteristics and be correctly installed and configured. Be sure to review **Selecting, installing, and configuring cameras to work with the AutoTRASSIR module**.

2. Go to the **Channels** node of the settings tree, select the desired channel from the list, and enable **License plate recognition** on the channel in the **Software-based detectors** area.

To activate the plugin, go to the **Channel settings** to the **Software detectors** area, select **License plate recognizer** and then select the **Server** which will calculate the analytics.



Analytics server is not selected in LPR1 and LPR3.

3. Follow **AutoTRASSIR setup** link and configure module operation on the selected channel.



AutoTRASSIR channel configuration depends on the version of the module. For a configuration description, see the corresponding section of the manual:

- **AutoTRASSIR (LPR5) setup**
- **AutoTRASSIR settings (LPR3)**
- **AutoTRASSIR settings (LPR1)**



Be sure that the **Recording to server disks** parameter in the **Archive recording** area is set to **Permanent** or **On Detector**.

4. Verify that the AutoTRASSIR module is properly functioning by **creating a simple template**.
5. Configure "black", "white" or "info" plate lists:

- Using **internal lists**.
- You can also connect external lists, stored in external text files or databases.



The settings for connecting external lists of license plate numbers differs for *Windows* and *TRASSIR OS*.



- *AutoTRASSIR settings*
- *Creating an AutoTRASSIR template*
- *Maintaining internal lists of license plate numbers*
- *Connecting external lists of license plate numbers from a text file*
- *Connecting external lists of license plate numbers in TRASSIR for Windows*
- *Connecting external lists of license plate numbers in TRASSIR OS*

## AutoTRASSIR settings



Before beginning this configuration process, be sure that the camera to work with AutoTRASSIR has been correctly *selected, installed, and configured*.

Depending on the version of AutoTRASSIR, select the appropriate configuration manual:

- *AutoTRASSIR (LPR5) setup*
- *AutoTRASSIR settings (LPR3)*
- *AutoTRASSIR settings (LPR1)*



The module version is selected on the tab **Settings** -> **Plugins** -> **AutoTRASSIR**. For a detailed description, see section *AutoTRASSIR general settings*.

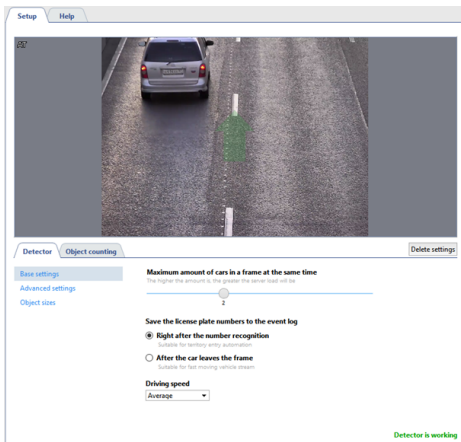


- *AutoTRASSIR - Automated license plate recognition*
- *Maintaining internal lists of license plate numbers*
- *Connecting external lists of license plate numbers from a text file*
- *Connecting external lists of license plate numbers in TRASSIR for Windows*
- *Connecting external lists of license plate numbers in TRASSIR OS*



## AutoTRASSIR (LPR5) setup

AutoTRASSIR setting aims to selecting the detector's working mode and defining the size of objects and recognition borders. All other parameters are integrated into the neural network, which detects license plates and recognizes test on them.



### Detector

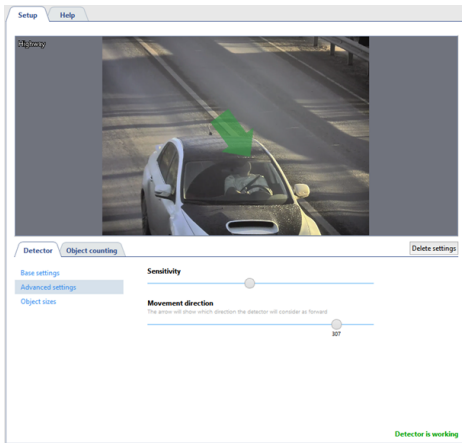
Set up the following parameters in the **Base settings** on the **Detector** tab:

- **Maximum amount of cars in a frame at the same time** - the maximum amount of cars, which can be detected by the detector at the same time in a frame. As a rule this value is set depending on the amount of the lanes in a frame. The higher the value is, the greater is the server load.
- **Save the license plate numbers to the event log** - sets the saving mode of the recognized license plate numbers to the log. It is selected depending on the required detection:
  - Right after the number recognition** - In this case AutoTRASSIR fixes the license plate number right after the vehicle appears in a frame and saves it to the log when it is recognized with the greatest extent of confidence. It suits for slowly moving or standing vehicles.
  - After the car leaves the frame** - in this mode AutoTRASSIR tries to recognize the license plate number when the vehicle is in a frame and fixes the number when the car leaves the frame. It will suit if the maximum precision of license plate number detection in the fast moving traffic flow is required.
- In the **Driving speed** dropdown list select the traffic speed in a frame. The higher the selected speed is, the more often the detector triggers and the greater is the server load:
  - **Stationary** - standing or very slow moving vehicle, such as a car approaching an auto barrier.
  - **Very slow** - up to 10 km/h.
  - **Slow** - up to 20 km/h.
  - **Average** - up to 30 km/h.
  - **Fast** - up to 200 km/h.
  - **Highest possible** - detector will trigger at each frame.

The **Advanced settings** area lets you set the following parameters:

- The **Sensitivity** parameter sets the level of confidence which is used during the license plate recognition and is defined depending on the detection requirements. The lesser the value is, the lesser is the probability of the detector false triggerings.
- The **Movement direction** parameter sets the direction of the traffic flow, which the detector will take as the direct movement. The direction is indicated by the green arrow on video and the slider shows the value.

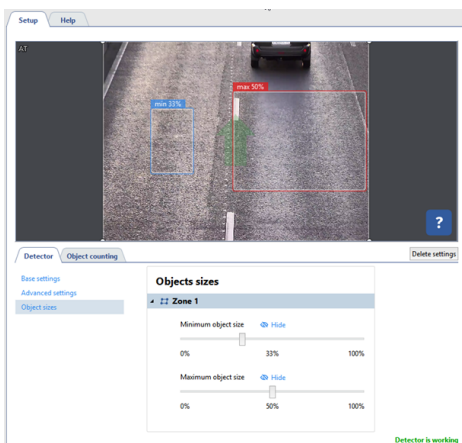
- The **Duplicate detection filter** parameter lets you eliminate repeated detections of the same license number if it has been previously recognized. The repeated detections may occur when the recognized license plate number disappears and then reappears in the frame, e.g. when it is hidden by another car. Select the time interval during which the recognized license plate number will not be detected repeatedly by the module.
- The **Analyze the lower part of the vehicle** parameter lets you prevent the detector triggering on the inscriptions located on the body of the shell. This setting allows you to set the license plate area more accurately.



**i** In the AutoTRASSIR log the movement in the direction of the green arrow is indicated by up arrow and the oncoming direction - by the down arrow. You can read more about recognized license plate number review in the [License plate recognition](#) and [Filtering current license plates](#) sections of the Operator's Guide.

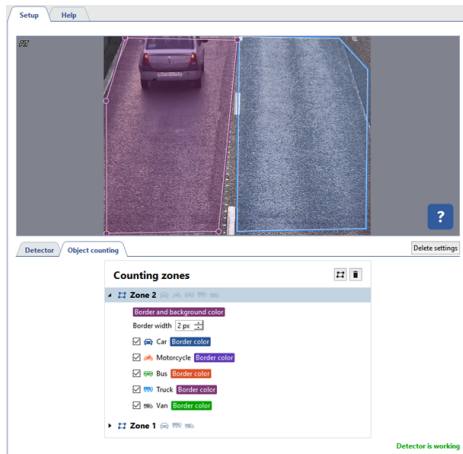
Plate	Time	Channel
15 19 100	11:51:05	AT
15 19 100	11:51:04	Highway
15 19 100	11:51:04	AT
NO PLATE	11:51:04	AT
15 19 100	11:51:03	Highway
15 19 100	11:51:03	AT
NO PLATE	11:51:02	AT
15 19 100	11:51:02	LPR test
15 19 100	11:51:02	AT
15 19 100	11:51:01	AT
15 19 100	11:51:01	Highway

The **Object sizes** area lets you create a zone in which the vehicles will be detected. With the help of **Minimum object size** and **Maximum object size** parameters set the minimal and maximal sizes of the detected objects.



## Object counting

The **Object counting** tab lets you set the zones, in which the vehicles will be detected and specify their borders. In order to create a new **counting zone** press **+** and set its vertices. Left click on the zone starting point or press **CTRL + ENTER** to finish the zone drawing.



Both traffic lanes and the adjacent territories can be taken as counting zones. You can create a zone of any form to avoid objects causing the false triggerings, such as parked cars.

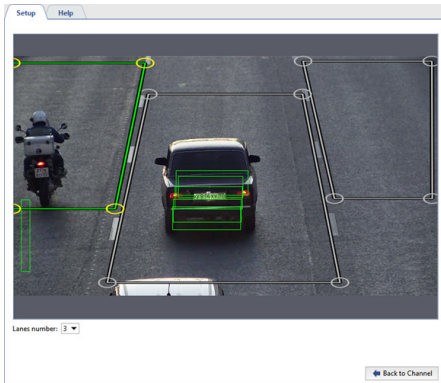
You can check the setting correctness in the *operator's interface*.



- [AutoTRASSIR general settings](#)
- [AutoTRASSIR settings \(LPR1\)](#)
- [AutoTRASSIR settings \(LPR3\)](#)

## AutoTRASSIR settings (LPR3)

AutoTRASSIR configuration comes to selection of the number of detection zones and determination of their boundaries.



Use the following guidelines during setup:

- **Number of lanes.** Choose the number of lanes based on the actual width of the carriageway, indicating the nearest possible value.



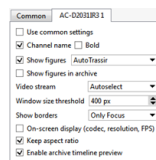
The standard commonly accepted lane width of a roadway is 3,5 meters. If the camera captures the roadway width which is 8 meters (that is not only the roadway, but the entire actual width of the image in meters). In this case you should select the closest to 8 meters value, which is 2 lanes.

- **Defining identification area boundaries.** Select isolated zones to obtain information about the passage of a car with a link to a particular lane (control of bus lanes, detection of car passage along the sidewalk, etc.). In addition, this will reduce the number of false alarms of the detector and will save the resources of the server, analyzing only targeted and suitable area of the image.

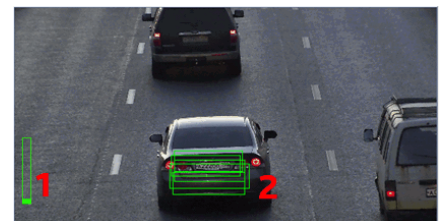


It is necessary to take into account depth of field and number of frames shot by the camera during the passage of the car inside the zone when selecting areas of recognition. Number of frames shot by the camera will directly depend on the speed of the car. It must be remembered as well that not all frames will be suitable for recognition, the image of the license plate number should be clear and easily recognizable. In most cases, it's enough to get 4-5 frames suitable for recognition.

You can verify the settings by **showing AutoTRASSIR figures**. To do this, right-click on the frame and select **View Options...** in the context menu. Set the **Show figures** checkbox and select **AutoTRASSIR Detector** in the dropdown list.



The **AutoTRASSIR figures** will be displayed on the screen:



1. **Processing queue** - This indicator reflects the state of the queue for processing license plate numbers. If the vertical bar fills up and turns red, then AutoTRASSIR begins to drop frames. The processing queue will fill if the server's CPU is heavily loaded and unable to process the frames.

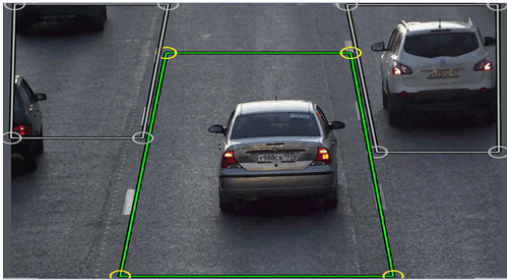
2. **Frame recognition quality** - is a rectangular indicator that displays recognition quality. Each rectangle is a separate frame used for license plate number recognition. Depending on whether or not the frame was suitable for recognition, the color of the rectangle will change from green (a "good" frame) to red (a "bad" frame).

Examples of module configuration:

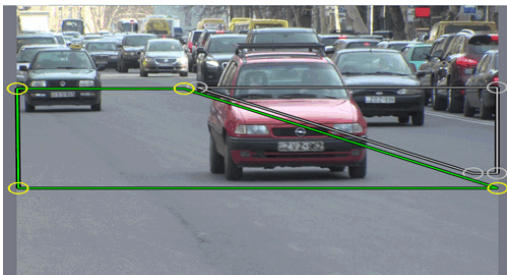
- To recognize license plate numbers of entering and leaving through the gate cars, you can select only the gate area. Cars passing on the road will be ignored in this case.



- You should draw a separate zone on each lane of the multilane roadways.



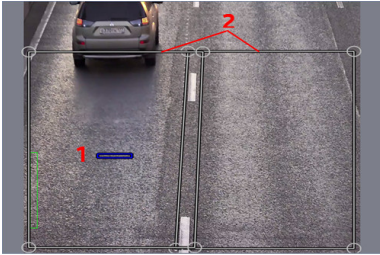
- In this example the camera has been installed so that the depth of field (the area of the image with the best image quality) covers only a small area in the middle of the frame. This is the same area that is relevant and useful for license plate recognition. There is no point in performing license plate recognition where the license plate is blurry or isn't visible. Limit the recognition zone to the area where the license plate is clear and of the required size.



- [AutoTRASSIR general settings](#)
- [AutoTRASSIR settings \(LPR1\)](#)
- [AutoTRASSIR \(LPR5\) setup](#)

## AutoTRASSIR settings (LPR1)

You can use the following tools during AutoTRASSIR configuration:



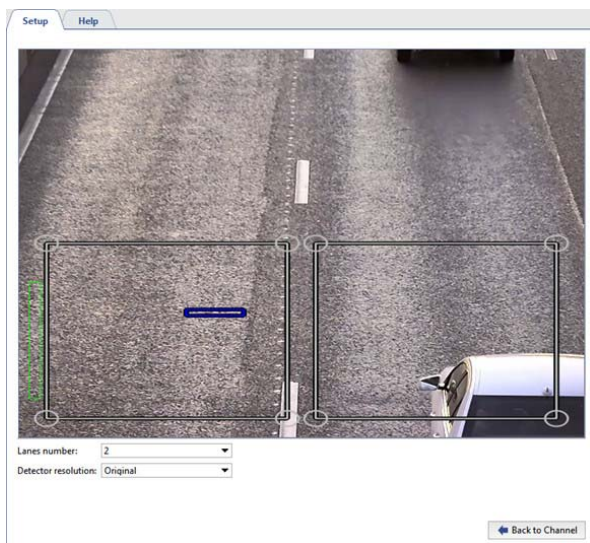
1. **Expected license plate size** - The estimated area of the image that will be used to determine the license plate size for license plate detection.
2. **Detection zones** - the areas on the image where the license plates will be detected.

To configure AutoTRASSIR, follow these steps:

1. Depending on the scene, select the desired value in the **Lanes number** dropdown list. The corresponding number of **Lane zones** will appear on the screen.



Select the number of the lanes based upon the actual roadway width, picking out the closest available value. The standard commonly accepted lane width is 3,5 meters. If the camera captures the roadway width which is 8 meters (that is not only the roadway width, but also the actual image width in meters). The closest to 8 meters should be selected in this case, which is "2 lanes".



In the **Detector resolution**, leave the default value - **Original**!

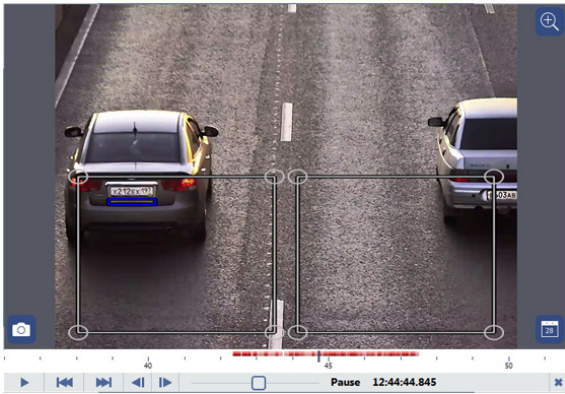


At this stage of the configuration it is not necessary to precisely determine the dimensions of the recognition zones. The recognition zones will be configured in step 6.

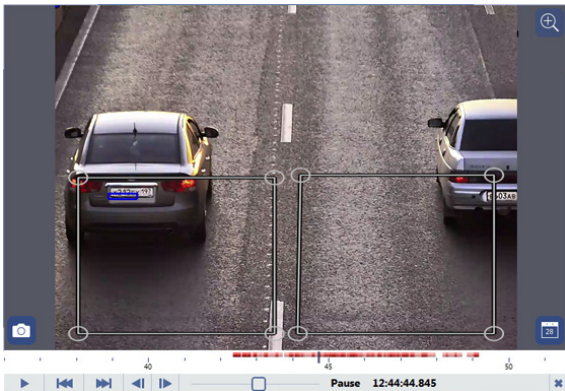
2. Compare the **expected license plate size** (you can freely move the icon around the screen) with the actual image of a license plate in the frame. For convenience, the comparison may be made in archive viewing mode after selecting the best frame of a passing vehicle.

If the actual size of the license plate on the image does not significantly differ from the **expected license plate size**, then the focal distance of the camera's lens must be changed. In this manner you can increase or decrease the size of the vehicle in the frame. If adjusting the focal distance is insufficient, then try changing the camera's angle or its installation height \ location.






3. If the actual license plate size in the image is much larger than the **expected license plate size**, then use the **Detector resolution** settings.



In the **Detector resolution** dropdown list, select **Preset**. The picture's resolution will be reduced in the best way possible, with minimal loss of quality and minimal additional load on the server's CPU.

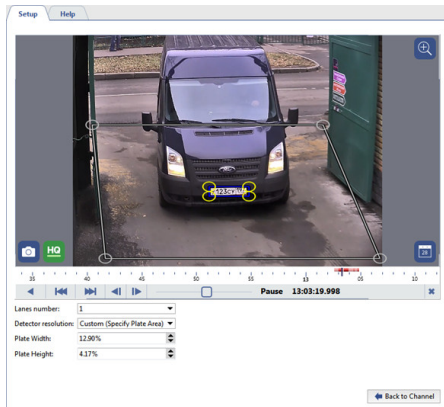


This situation may occur if a high-resolution camera is used to monitor a very narrow section of road. For example, if a 3-MP camera is used to monitor a single lane. Note that in this case the **expected license plate size** depends on the value of the **Lanes number** parameter.

4. During the comparison, if the actual size of the license plate on the image is much smaller than the **expected license plate size** and adjusting the focal distance and changing the camera's angle and/or installation location does not fix this, the resolution of the camera used for license plate recognition may be insufficient for the given scene.



5. If a complete match between the actual license plate size and the **expected license plate size** could not be achieved in the previous configuration steps, you can specify the **expected license plate size** manually. To do this, in the **Detector resolution** setting, select **Custom (Specify Plate Area)**.  
To do this, on the selected archive frame change the **expected license plate size** so that it precisely matches the license plate's actual image.



Using the **Custom (Specify Plate Area)** parameter increases the load on the server's CPU. Moreover, reducing the image to an arbitrary size may introduce compression artifacts, which negatively affect license plate number recognition quality. Use this setting only if the other options did not help.

6. The final stage of configuring AutoTRASSIR requires defining the recognition zones' precise boundaries. Assigning distinct zones makes it possible to:

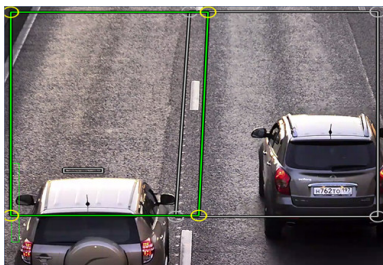
- associate a vehicle's passing with a specific lane (monitoring selected lanes for fixed-route vehicles, detecting vehicles passing on a walkway, etc.);
- save server resources by analyzing only the truly interesting and relevant areas of the image, minimizing the number of false activations of the detector.

For example:

- To recognize the license plates of vehicles entering and exiting through a gate, you can assign only the area with the gate. In doing so, vehicles passing by on the road will be ignored.

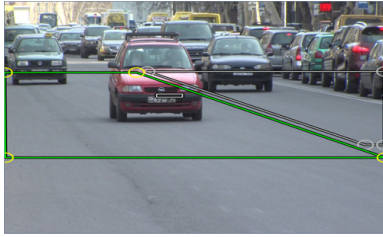


- You should draw a separate zone on each lane of the multilane roadways.



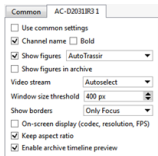
- In this example the camera has been installed so that the depth of field (the area of the image with the best image quality) covers only a small area in the middle of the frame. This is the same area that is relevant and useful for license plate recognition. There is no point in performing license plate recognition where the license plate is blurry or isn't visible. Limit the recognition zone to the area where the license plate is clear and of the required size.



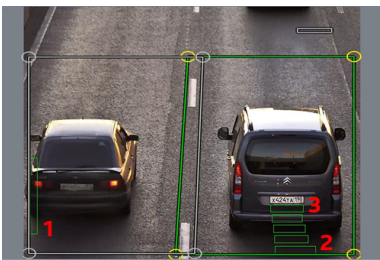


Upon setting the depth of field and assigning recognition zones, it should be born in mind how many frames the camera will be able to capture in the time period the vehicle passes through the zone. The number of frames the camera takes depends directly on the vehicle's speed. Additionally, note that not all frames are recognizable. The license plate image must be clear and distinguish. In most cases, capturing 4-5 viable frames is sufficient.

You can verify the settings by **showing AutoTRASSIR figures**. To do this, right-click on the frame and select **View Options...** in the context menu. Set the **Show figures** checkbox and select **AutoTRASSIR Detector** in the dropdown list.



The **AutoTRASSIR figures** will be displayed on the screen:



1. **Processing queue** - This indicator reflects the state of the queue for processing license plate numbers. If the vertical bar fills up and turns red, then AutoTRASSIR begins to drop frames. The processing queue will fill if the server's CPU is heavily loaded and unable to process the frames.
2. **Frame recognition quality** - This indicator, in the form of a stripe, displays the actual size of the license plate and its recognition quality. Each stripe pertains to a separate frame used for license plate number recognition. Depending on whether or not the frame was suitable for recognition, the color of the stripe will change from green (a "good" frame) to red (a "bad" frame).
3. **Expected license plate size** - This blue indicator represents the expected size of a license plate. The vertical green stripes show the actual size of the license plate in the frame.



- [AutoTRASSIR general settings](#)
- [AutoTRASSIR settings \(LPR3\)](#)
- [AutoTRASSIR \(LPR5\) setup](#)

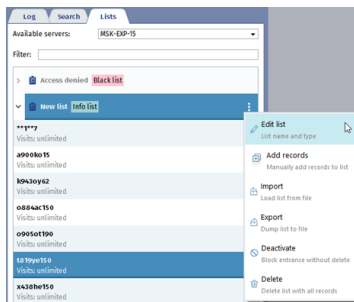
## Maintaining internal lists of license plate numbers

The AutoTRASSIR plugin can use the internal license plate lists, which are stored in its own database. If the number stored in the internal list is recognized, AutoTRASSIR will build up the message in accordance with the settings, specified for this license plate number.



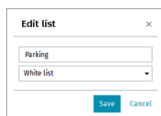
In order to start working with AutoTRASSIR internal license plate number lists, you should create [a simple AutoTRASSIR template](#)

An operator can create and edit license plate number lists in the **Lists** tab in the **AutoTRASSIR log** area. You can create an unlimited number of lists. Press **Add list** to create a list and select the reaction type: **info list**, **white list** or **black list**.

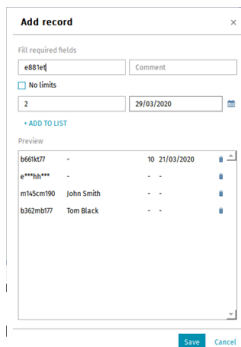


The list editing menu lets you:

- **Edit list** - change the list name or type.



- **Add records** - add one or several numbers to the list.



Enter all the required number information in the opened window and press **+Add to list**:

**License plate** is a vehicle number. Both Latin and Russian letters can be used. You can also use a "mask" in which "\*" and "?" symbols are used instead of unknown symbols.



"?" stands for a single unknown symbol, while "\*" stands for one or several unknown symbols. I.e. in case the plate number is known, but the region number is unknown, you can use the following types of masks:

**b663kt??** - for plate numbers with double region number: **b663kt77** or **b663kt95**.

**b663kt???** - for plate numbers with triple region number: **b663kt777** or **b663kt190**.

**b663kt\*** - for double as well as triple region numbers: **b663kt77** or **b663kt190**.

**Comment** - the description of the number, displayed at the operator's monitor.

Uncheck **No limits** field and specify the **Visits count** or set the **Date** till which the entrance is allowed to create a record with visits time or count limit. Upon of the conditions' completion (the number of visits or the entrance allowance period expired), the record will be removed.

Upon completion press **Save**.

- **Import** - import a list of numbers from any spreadsheet editor (Microsoft Office Excel or Apache OpenOffice Calc) saved in \*.csv. The data in the imported file should be in the following format:

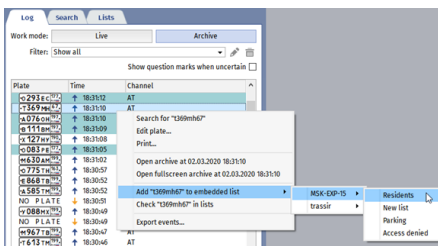
```
"License plate";"Comment";"Visits count";"Expiration date"
"b663kt777";"John Smith";;
"m145cm190";"Peter Still";;
"o362tk197";"Ian Johns";10;29/02/2020
```

- **Export** - save the license plate number list to a file (\*.csv). The saved list can be used for import.
- **Deactivate** or **Activate** - deactivate or activate the license plate number list. The numbers from the deactivated list won't be highlighted when recognized.
- **Delete** - delete the number list.

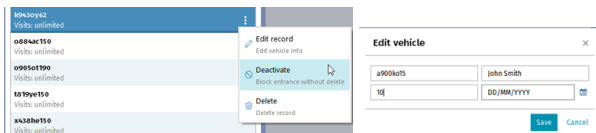


The **Audit** plugin lets following the editing history of the embedded license plate lists. Read more about it in the **Audit** section.

Besides manual addition or import from the file, the numbers can be added to the list with the help of scripts or from AutoTRASSIR log.



You can deactivate the number in the list or edit it. The list remains activated when a number is deactivated.



When a license plate number is recognized, it is highlighted in the event log by the light, corresponding to the list type to which it is added. If a number is added to several lists, all of them will be displayed near the recognized number in the operator's interface.





You can also connect lists of license plate numbers obtained from [external sources](#):

1. [From a text file](#) - each line must contain a license plate number and comments delimited by a space or special character.
2. [From a database](#). A database connection is made using the ODBC software interface; a previously created ODBC data sources required to make a connection. For a description of database connection settings in TRASSIR OS, see [Connecting external lists of license plate numbers in TRASSIR OS](#).



- [AutoTRASSIR general settings](#)
- [AutoTRASSIR - Automated license plate recognition](#)
- [Selecting, installing, and configuring cameras to work with the AutoTRASSIR module](#)
- [AutoTRASSIR settings](#)
- [Creating an AutoTRASSIR template](#)

## Connecting external lists of license plate numbers from a text file

To connect an external list from a text file:

1. In the **Settings** window on the **Server settings** -> **AutoTRASSIR** tab, click the **Add text file** button.
2. In the window that opens, specify the connection settings for the external list:

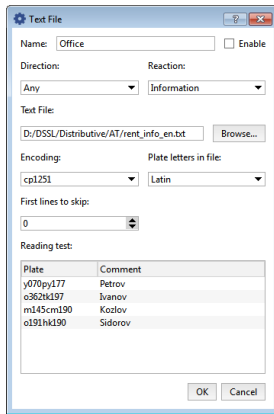
- **Name** - The name for the list of license plate numbers in TRASSIR.
- **Enable** - This checkbox determines if this source of license plate numbers should be processed by the AutoTRASSIR module. If the checkbox is cleared, then license plate numbers from this list will be ignored and messages will not be issued to the operator.
- **Direction** - Your choice of a value from the dropdown list: "Down" or "Up". This parameter is set based on the direction in which vehicles move relative to the camera. If license plate numbers should be processed for vehicles traveling in both directions, select "Any".
- **Reaction** - The type of message issued to the operator: "Blacklist", "Whitelist" or "Informational". Note that this determines the response type for all license plate numbers in the list.
- **Text file** - The path to a text file that contains the list of license plate numbers.



Text format is a list of strings, each containing the number and the comment, separated by backspace or TAB symbol. I.e.:

```
y070pyl77 John Rain
o362tk197 Peter Steel
m145cm190 Tony Shot
o191hk190 Ian West
```

- **Encoding** - The text file's encoding.
  - **Plate letters in file** - A value from the dropdown list. Choose "Latin" or "Russian", depending on the type of characters used in the license plate numbers in the file.
  - **First lines to skip** - The number of lines that should not be processed (for example, if the file contains some textual information other than license plate numbers). If the file only contains license plate numbers, then leave the value "0".
3. After specifying the settings, be sure that the file's data has been read correctly in the **Preview** pane.



If the **Reading test** pane displays unreadable symbols, be sure that you have correctly indicated the type of characters used in the file and the correct encoding.

4. Click **OK**. The connection to the external list will be saved in TRASSIR.

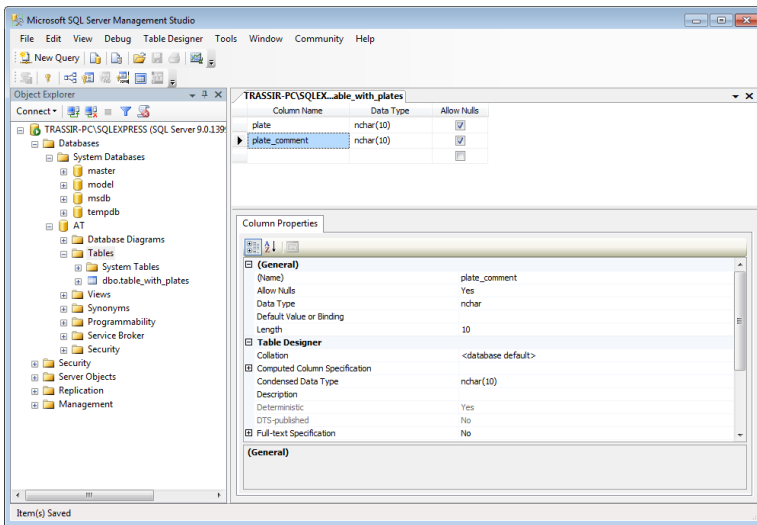


- [AutoTRASSIR general settings](#)
- [AutoTRASSIR - Automated license plate recognition](#)
- [Selecting, installing, and configuring cameras to work with the AutoTRASSIR module](#)
- [AutoTRASSIR settings](#)
- [Creating an AutoTRASSIR template](#)
- [Maintaining internal lists of license plate numbers](#)

## Creating an external ODBC data source for AutoTRASSIR

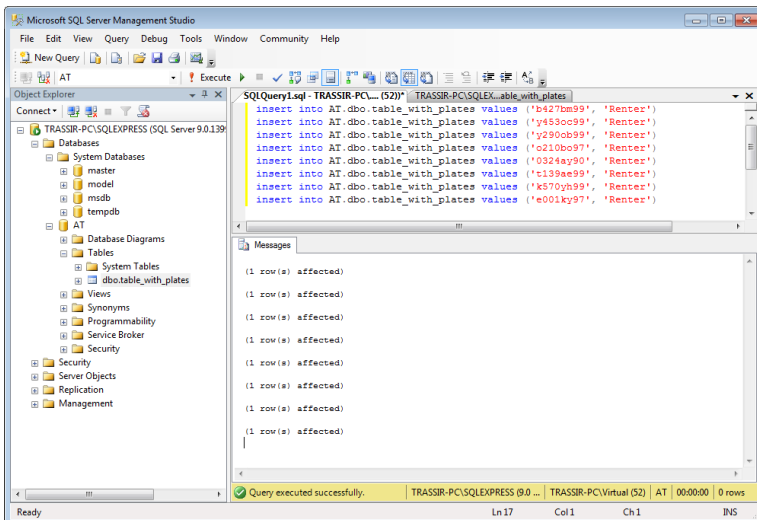
Let us consider the creation of an external ODBC data source using an MSSQL database.

To begin, first use Microsoft SQL Server Management Studio to create an **AT** database with a **table\_with\_plates** table, which contains **plate** and **plate\_comment** columns:

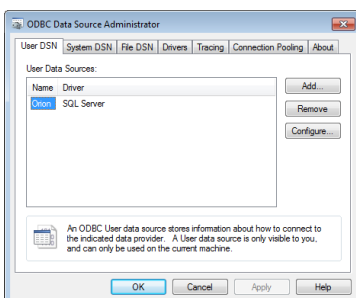


In our example we are only using two columns that contain the license plate number and a description of its owner. You can create tables with any number of columns and amounts of information. For example, you might include the vehicle's time of passage or its color.

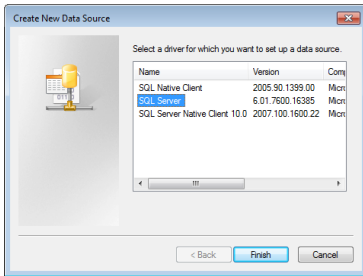
Next, use an SQL query to fill the table:



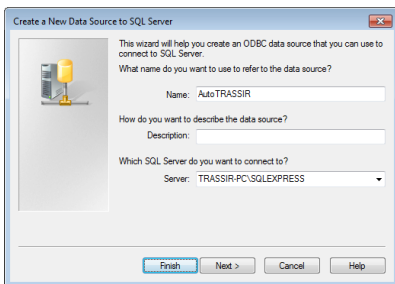
Now let's create the ODBC data source. To do this, launch the **ODBC Data Source Administrator** (**Start -> Control Panel -> Administrative Tools -> Data Sources (ODBC)**)



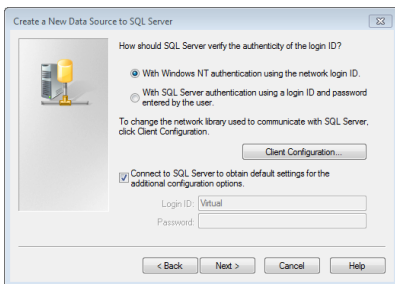
Click the **Add** button and select a driver in the window that opens. In our case, we will use **SQL Server**. To begin the configuration, click **Finish**



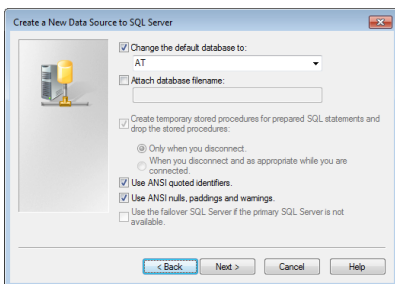
After that, the wizard will prompt you to enter the name of the data source, which will subsequently be used to configure the connection in TRASSIR, and the path to the SQL server. Enter the required information and click **Next >** to continue.



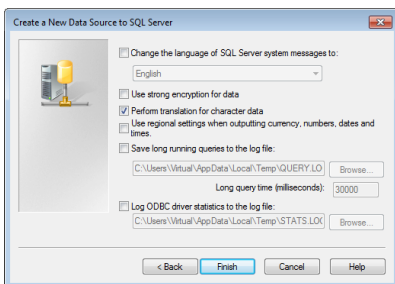
In the next step, the wizard will prompt you to select a user authentication option. In our case, we will leave the settings unchanged and click **Next >** to continue.



In the next step of the configuration, set the **Use database by default** checkbox and select the previously created **AT** database. Leave the remaining settings unchanged. To continue the configuration, click **Next >**.

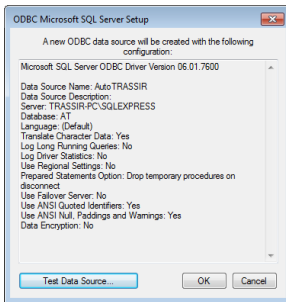


Similarly, leave the ODBC data source's other parameters unchanged.

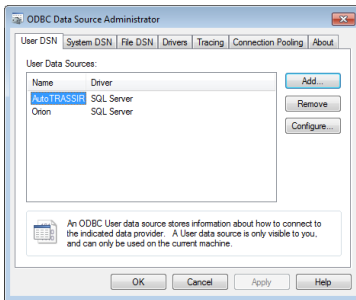


At the end of the configuration of the ODBC data source, click **Finish**. A window will open showing all of the ODBC data source's settings made using the wizard. To finish the configuration, click **OK**.





The ODBC data source is ready for AutoTRASSIR.



- *Connecting external lists of license plate numbers in TRASSIR for Windows*
- *Connecting external lists of license plate numbers in TRASSIR OS*

## Connecting external lists of license plate numbers in TRASSIR for Windows



The creation and initial configuration of an ODBC data source are described in [Creating an external ODBC data source for AutoTRASSIR](#).

To connect an external list from an ODBC data source:

1. In the **Settings** window on the **Server settings** -> **AutoTRASSIR** tab, click the **Add ODBC source** button.
2. In the window that opens, specify the connection settings for the ODBC data source:

- **Name** - The name used to identify the data source in TRASSIR.
- **Enable** - This checkbox determines if the source should be used by the AutoTRASSIR module. If the checkbox is cleared, then license plate numbers from this source will not be processed.
- **Direction** - Your choice of a value from the dropdown list: "Down" or "Up". This parameter is set based on the direction in which vehicles move relative to the camera. If license plate numbers should be processed for vehicles traveling in both directions, select "Any".
- **Reaction** - The type of message issued to the operator: "Blacklist", "Whitelist" or "Informational". Note that this determines the response type for all license plate numbers in the list.
- **ODBC data source** - A value from the list of ODBC data sources registered on the computer.
- **Username** and **Password** - Credentials for connecting to the data source.
- **Plate letters in database** - A value from the dropdown list. Choose "Latin" or "Russian", depending on the type of characters used in the license plate numbers in the database.
- **Letter case in database** - A value from the dropdown list. Choose "Upper" or "Lower", depending on the case of the characters used in the license plate numbers in the database.
- **SQL query** - The database query to check for the presence of a recognized number in the database. The query looks like this:

```
SELECT plate_comment FROM table_with_plates WHERE plate = ?
```

where:

plate\_comment - The name of the column containing the comments;

table\_with\_plates - The name of the database table containing the license plate numbers;

plate - The name of the column containing the license plate numbers.



Note that the names of tables and columns will be specific to your database.

The specified SQL query will be run on the data source for every instance of a recognized license plate number. In doing so, the recognized license plate number will replace the "?" in the query. If a given number exists in the database, then the corresponding comments ( `comment` column) will be returned in the results.

3. After specifying the settings, be sure that the data from the database has been read correctly in the **Test** pane. To do this:

- Enter a license plate number that exists in the database.
- Click **Test**;
- Verify the value in the **Result** field; if the SQL query is incorrect, it will contain an error message.

4. Click **OK**. The connection to the external list will be saved in TRASSIR.



- [AutoTRASSIR general settings](#)
- [Creating an external ODBC data source for AutoTRASSIR](#)

## Connecting external lists of license plate numbers in TRASSIR OS



The description of this setting is applicable when using TRASSIR OS. When using the Windows version, use the [next section in the guide](#).

To connect an external list from an ODBC data source:

1. In the **Settings** window on the **Server settings** -> **AutoTRASSIR** tab, click the **Add ODBC source** button.
2. In the window that opens, specify the connection settings for the ODBC data source:

- **Name** - The name used to identify the data source in TRASSIR.
- **Enable** - This checkbox determines if the source should be used by the AutoTRASSIR module. If the checkbox is cleared, then license plate numbers from this source will not be processed.
- **Direction** - Your choice of a value from the dropdown list: "Down" or "Up". This parameter is set based on the direction in which vehicles move relative to the camera. If license plate numbers should be processed for vehicles traveling in both directions, select "Any".
- **Reaction** - The type of message issued to the operator: "Blacklist", "Whitelist" or "Informational". Note that this determines the response type for all license plate numbers in the list.
- In the **Database settings** settings group, enter the ODBC data source's connection settings:
  - **DB Type** - The type of database being connected;
  - **DB Host** - The IP address or DNS name of the server where the ODBC data source is located.



If using SQL Server Express, the server's address is entered as `[server_name]\[instance_name]`.  
For example: `192.168.5.202\SQLEXPRESS` or `atserver\SQLEXPRESS`.

- **DB Name** - The name of the database.

- **DB Port** - The port to be used to connect to the server;



If using SQL Server Express, in the **DB Port** field enter the value 0.

- **Username** and **Password** - Credentials for connecting to the data source.
- **Plate letters in database** - A value from the dropdown list. Choose "Latin" or "Russian", depending on the type of characters used in the license plate numbers in the database.
- **Letter case in database** - A value from the dropdown list. Choose "Upper" or "Lower", depending on the case of the characters used in the license plate numbers in the database.

- **SQL query** - The database query to check for the presence of a recognized number in the database. The query looks like this:

```
SELECT plate_comment FROM table_with_plates WHERE plate = ?
```

where:

plate\_comment - The name of the column containing the comments;

table\_with\_plates - The name of the database table containing the license plate numbers;

plate - The name of the column containing the license plate numbers.



Note that the names of tables and columns will be specific to your database.

The specified SQL query will be run on the data source for every instance of a recognized license plate number. In doing so, the recognized license plate number will replace the "?" in the query. If a given number exists in the database, then the corresponding comments (commentcolumn) will be returned in the results.





- After specifying the settings, be sure that the data from the database has been read correctly in the **Test** pane. To do this:
  - Enter a license plate number that exists in the database.
  - Click **Test**;
  - Verify the value in the **Result** field; if the SQL query is incorrect, it will contain an error message.
- Click **OK**. The connection to the external list will be saved in TRASSIR.



- [AutoTRASSIR general settings](#)
- [Creating an external ODBC data source for AutoTRASSIR](#)

## Creating an AutoTRASSIR template

You can verify that the AutoTRASSIR module has been correctly configured and is working properly by creating a simple template. To do this:

1. Open the *Main control panel* and display a *video monitor* on one of the server's screens.
2. Click **Template editor**  and select **New** .
3. Click **+ Add AutoTrassir** .
4. Drag the camera signal being processed by the AutoTRASSIR module from the list of channels to an available space.
5. Click **Save As...** .

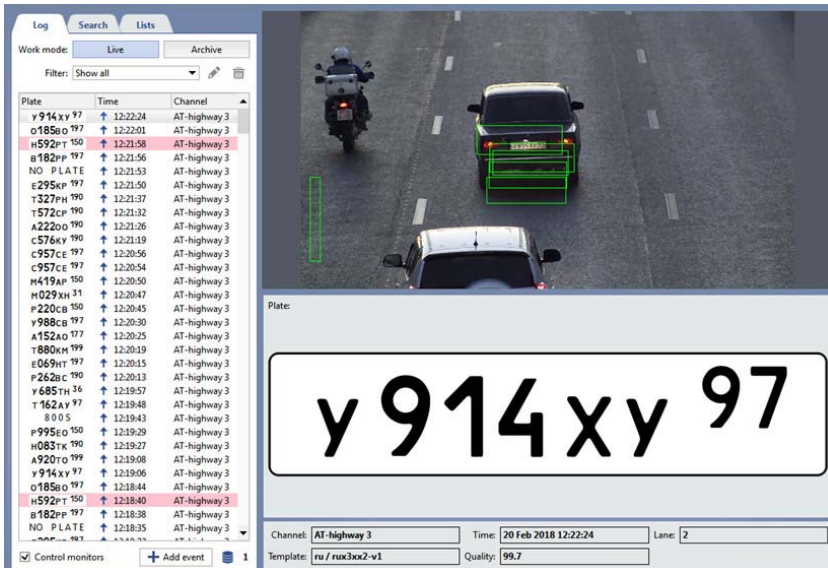
Save template under name:

AT

OK Cancel

Enter the name of the new template in the small window that opens, and click **OK**.

As a vehicle passes, the recognized license plate number will appear in the AutoTRASSIR log.



The screenshot shows the AutoTRASSIR interface. On the left is a log table with columns for Plate, Time, and Channel. The log contains several entries, with the most recent one being 'y 914 xy 97' at '12:22:24' on 'AT-highway 3'. On the right is a video monitor showing a car with a license plate 'y 914 xy 97' and a motorcycle. Below the video monitor is a large display of the license plate number 'y 914 xy 97'. At the bottom, there are fields for Channel (AT-highway 3), Time (20 Feb 2018 12:22:24), Lane (2), Template (ru / rux3xx2-v1), and Quality (99.7).

Plate	Time	Channel
y 914 xy 97	12:22:24	AT-highway 3
o185a o 197	12:22:01	AT-highway 3
h592p t 150	12:21:58	AT-highway 3
h182p p 197	12:21:56	AT-highway 3
NO PLATE	12:21:53	AT-highway 3
e295k p 197	12:21:50	AT-highway 3
t327p h 190	12:21:37	AT-highway 3
t572c p 190	12:21:32	AT-highway 3
a222o o 190	12:21:26	AT-highway 3
c576k y 190	12:21:19	AT-highway 3
c957c e 197	12:20:56	AT-highway 3
c957c e 197	12:20:54	AT-highway 3
h419a p 150	12:20:50	AT-highway 3
h029x h 11	12:20:47	AT-highway 3
p220c b 150	12:20:45	AT-highway 3
y988c b 197	12:20:30	AT-highway 3
a152a o 177	12:20:25	AT-highway 3
t800h h 199	12:20:19	AT-highway 3
o069h t 197	12:20:15	AT-highway 3
p262c c 190	12:20:13	AT-highway 3
y685t h 16	12:19:57	AT-highway 3
t162a y 197	12:19:48	AT-highway 3
800 S	12:19:43	AT-highway 3
p995i o 150	12:19:29	AT-highway 3
h083k x 190	12:19:27	AT-highway 3
a920i o 199	12:19:08	AT-highway 3
y 914 xy 97	12:19:06	AT-highway 3
o185a o 197	12:18:44	AT-highway 3
h592p t 150	12:18:40	AT-highway 3
h182p p 197	12:18:38	AT-highway 3
NO PLATE	12:18:35	AT-highway 3



If license plate numbers do not appear as vehicles pass, then verify that:

- the **License plate recognition** checkbox is set in the *Software-based detectors* area of the channel settings.
- the *database connection* has been configured.

You can read more about working with the template editor and the AutoTRASSIR module in the Operator's Guide (???)



- *AutoTRASSIR general settings*
- *AutoTRASSIR - Automated license plate recognition*
- *Selecting, installing, and configuring cameras to work with the AutoTRASSIR module*
- *AutoTRASSIR settings*
- *Maintaining internal lists of license plate numbers*
- *Connecting external lists of license plate numbers in TRASSIR for Windows*
- *Connecting external lists of license plate numbers in TRASSIR OS*

## SIMT software-based detector

The purpose of a SIMT detector (Simple Intelligent Motion TRASSIR) is to identify an object with specific parameters in a video against a background of abundant and random motion, which is noise in most instances. SIMT can filter out very powerful noises, which are beyond the capabilities of other detectors, such as: tree branches swaying in the wind, snow with rain, minor camera jitters, etc.

Out of an entire image, SIMT identifies the objects that are really moving, along with their history and the nature of their motion; it can also distinguish these objects from one another. An object that is briefly hidden from the field of view (for example, behind a tree) will not be treated as a new or different object.

SIMT's scope of application:

- guarding perimeters and open territories, parking lots and oil pipelines; appropriate in video surveillance systems where motion is an alarm event that requires attention;
- guarding subway station entrances and transportation nodes;
- any sites that require an intelligent evaluation of the situation, for example, detecting a running person in a place where running is not a normal motion.

The SIMT module provides:

- high tolerance of precipitation, interference, and noise;
- detection of the speed, direction of the motion, distance covered, and the sizes of actually moving objects;
- monitoring of intersections with object borders;
- monitoring of the presence of objects in a zone;
- automated PTZ camera control (in conjunction with the [ActiveDome](#) module);

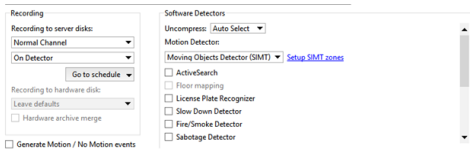


- [SIMT detector settings](#)
- [ActiveDome - Automated PTZ-camera control](#)




## SIMT detector settings

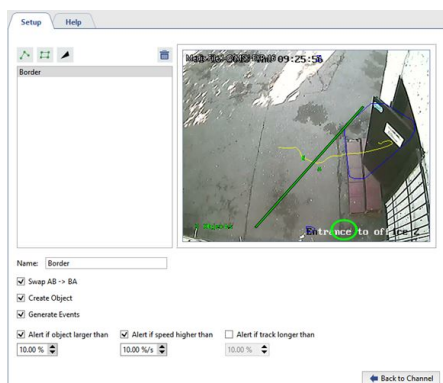
To configure the SIMT detector, in the **Motion detector** settings group in the **Software Detectors** area of the **Channel settings** window, select **Moving object detector (SIMT)** and click **Setup SIMT zones**. A window for configuring the SIMT detector's borders and zones will open.




You can create borders and zones, as well as indicate areas to ignore.

1. A border is a type of detector area specified using a polygonal line. A detector event is generated if one of the specified lines is crossed. To add a border:

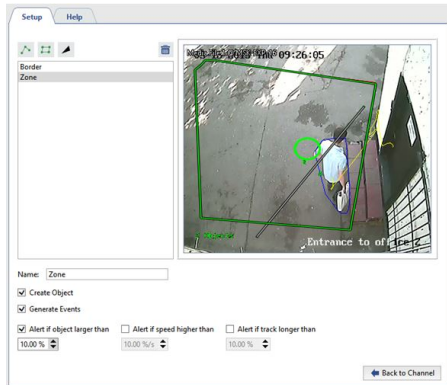
- Click the ;
- Then left-click with the mouse to specify the vertices of a polygonal line;
- Click **Finish**;
- Give the detection zone a name;
- Set the **Swap AB -> BA** checkbox in order to make zones A and B switch places;
- Set the **Create object** checkbox if you need to create an object for this border in the TRASSIR object tree. A border object may be used, for example, when setting up monitoring using the object tree (CMS) and the corresponding filters.
- Set the **Generate events** checkbox if you want an "Object intersected border" event to be generated and written to the database when the border is intersected. Moreover, the event will include the direction of motion, i.e. the side from which the object intersected the border.
- Set the **Alarm if object larger than**, **Alarm if speed greater than**, and **Alert if track longer than** checkboxes if you want additional alarm events that depend on the nature of the object's motion to be generated and written to the database.




2. A detection zone is an area that will be monitored by a detector if motion occurs in it. A detector event can be generated when motion occurs within the specified polygon. To add a detection zone:

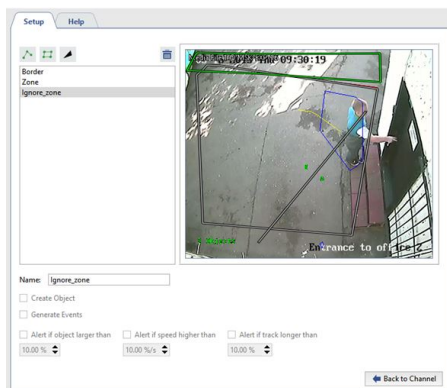
- Click the ;
- Consecutively left-click with the mouse to specify the vertices of the polygon;
- Click **Finish**;
- Give the detection zone a name;

- Set the **Create object** checkbox if you need to create an object for this zone in the TRASSIR object tree. A zone object may be used, for example, when setting up monitoring using the object tree (CMS) and the corresponding filters.
- Set the **Generate events** checkbox if you want "Object entered zone" and "Object exited zone" events to be generated and written to the database when there is motion in the zone.
- Set the **Alarm if object larger than**, **Alarm if speed greater than**, and **Alert if track longer than** checkboxes if you want additional alarm events that depend on the nature of the object's motion to be generated and written to the database.



3. An ignore zone is an area for which the detector will not take any action when motion occurs in it. The vertices of a polygon are used to specify an ignore zone. To add an ignore zone:

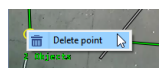
- Click the ;
- Consecutively left-click with the mouse to specify the vertices of the polygon;
- Click **Finish**;
- Give the ignore zone a name.



After defining zones and borders you can adjust the position of their vertices, delete unnecessary vertices, or add new ones.

To edit a zone (border):

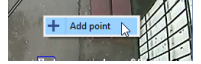
1. Select the zone (border) in the list. The currently selected zone (border) will be highlighted in green, while the remaining zones (borders) will be gray.
2. Left-click with the mouse near a vertex (marked by a green oval).
3. Without releasing the left mouse button, adjust the position of the vertex.
- 4.



If a vertex is unnecessary you can delete it. To do this:

- Point the cursor near the green oval;
- Right-click with the mouse;
- Select **Delete point** in the context menu that appears.

5.



To add a new vertex to an existing zone (border):

- Point the cursor at the desired location for the new vertex;
- Right-click with the mouse;
- In the context menu that appears, select **Add point**.



- *SIMT software-based detector*
- *Motion detector settings*
- *Channel settings*

## ActiveSearch - find motion

ActiveSearch is a archive search tool that offers:

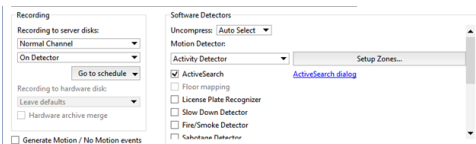
- super fast search across the entire archive;
- motion search in the specific zone with the preset parameters;
- versatility using set parameters (speed of motion, object size, duration of motion, exact time);
- archive viewing in the search window;
- easy interactive search and the possibility of the search using standard templates or a specific time interval;

To operate, the MotionSearch module uses information from software-based motion detectors (an activity detector and a software-based SIMT detector) and several hardware-based detectors.



Note that when switching from a hardware-based detector to a software-based detector or vice-versa, the information from the old detector will no longer be available. After switch detectors, you will only be able to find motion over the period of time in which the new detector has been operating.

To activate the plugin go to the [Channel settings](#) to the [Software detectors](#) settings group and select **ActiveSearch**. In case the archive search is required, open the [ActiveSearch dialog](#) link.



If the **ActiveSearch** checkbox is disabled, be sure the right detector is being used for processing on the channel.

You can read more more about working with the ActiveSearch module in the Operator's Guide (???).



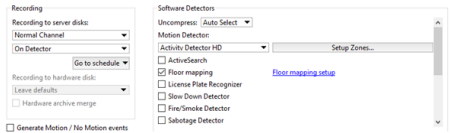
- [Motion detector settings](#)
- [Channel settings](#)

## Floor mapping settings

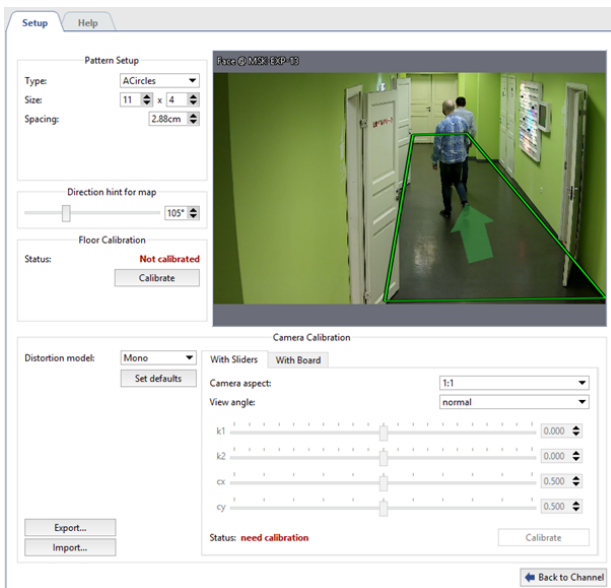


**Floor mapping** is designed for transferring image from camera to the floor surface. It is required for TRASSIR showing people movement on the *map*, detected by *Neuro detector*. It is also required for building *heatmap*.

To activate the plugin go to *Channel settings* to the *Software detectors* settings area and select **Floor mapping**. Click **Setup floor mapping** link to open the settings window.



The detector settings window will open:



The module is configured by calibration with the help of a special template. Before starting a calibration, download a template from the website [nerian.com](http://nerian.com). Print it in 1:1 scale in A2 format or bigger sheet.

**Check the scale of the received template using the ruler.**



## Settings

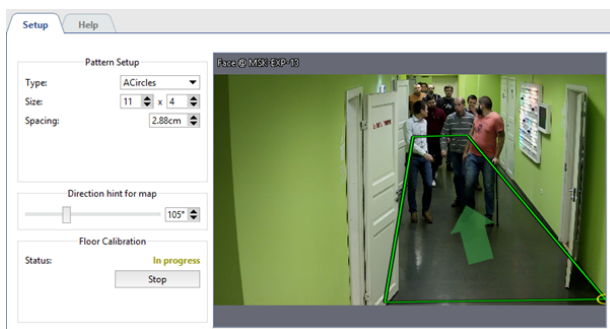
### 1. Make the module preset

In the **Pattern Setup** group of settings enter the parameters of the template to perform calibration. All required parameters are specified in the template.

- **Type** - the type of the template.
- **Size** - number of lines and rows.
- **Spacing** - the distance between the template items.

### 2. Floor calibration

Before starting the calibration, put template on the floor in such a way to ensure its coming into image coverage in full. Click **Calibrate** in **Floor calibration** settings group and wait for the calibration completion. Calibration is deemed to be completed when the value in **Status** changes to **Calibrated**.



Floor calibration is not required in case of using **Fisheye** cameras.



Floor re-calibration is required in case of the change of:

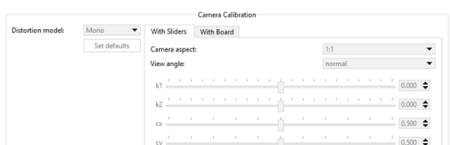
- camera installation location;
- camera tilting angle;
- focal distance of the lens.

### 3. Camera calibration

To start with select the **Distortion model** installed on the camera: **Mono** or **Fisheye**.

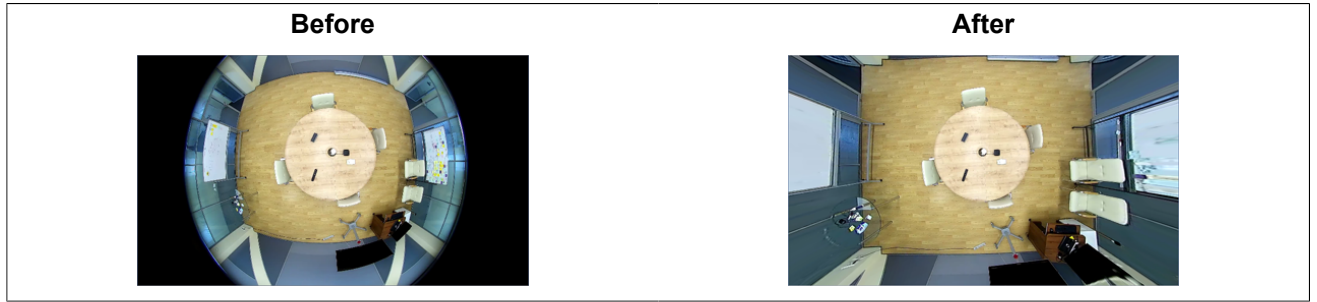
Further calibration of camera can be done in two ways:

#### • With sliders

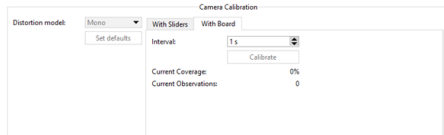


On the **"With sliders"** tab in **Camera aspect** and **View angle** fields select height-to-width aspect of maximum resolution and lens vision's horizontal angle.

Then on click **Calibrate** and changing the sliders adjust the image deterioration in such a way to make all straight lines in real life (walls and floor borders, door and window reveals, etc.) straight in the image. On completion click on **Stop**.



#### • Camera calibration with board



On the **With board** tab in **Interval** field enter the time which will pass between neighboring calibrations.

Further on calibration shall be done as follows: one person shows a template to the camera in various points of the shooting area and the other person clicks **Calibrate** and monitors the changes in the values of **Current Coverage** and **Current Observations**.



The calibration is considered to be completed when the **Current coverage** parameters will exceed 80%. Click **Stop**, to stop calibration and fix the result.



**Set defaults** resets the camera calibration settings.

The camera calibration depends on the camera model and lens installed on it. Thus making single camera calibration you can conduct **Export / Import** of settings to the other **camera of the same model** and **with the same lens**.

#### 4. Floor area marking

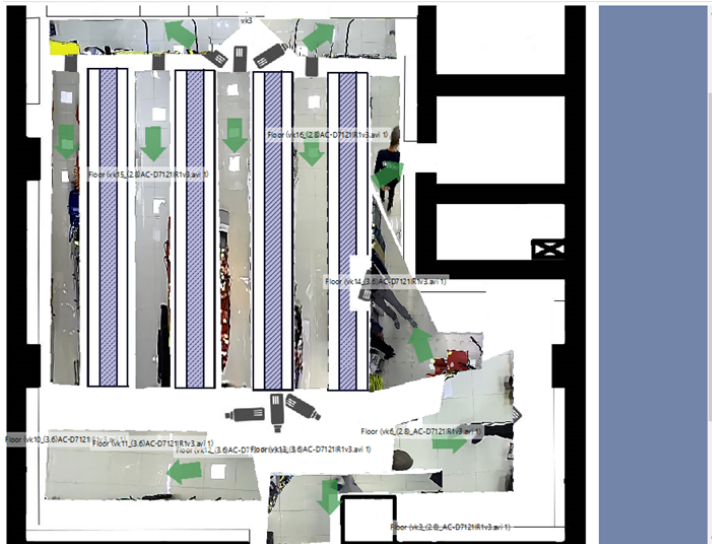
Modify the position of the rectangle points in such a way to make the marked area to enframe all visible surface of the floor. If necessary, add the desired number of points using the context menu.

Further on to ensure the correct floor area location on the map you'll need to orient it in space. To do this using **Direction hint for map** direct an arrow in such a way to direct it on the one of the walls or make parallel to the passage.



#### 5. Calibration validity check

Calibration validity test can be done *by adding floor area on the map*. Under correct settings floor area will be maximum approximated to the plan.



- *Neuro detector setup*
- *Motion detector settings*
- *Channel settings*



## Slow Down Detector

Slow Down Detector helps to detect the objects of different sizes left in the camera's field of sight. It can instantly detect unattended and forgotten objects that pose a potential threat to the object of video surveillance.

There are **Simple** and **Advanced** abandoned objects detectors built-in to TRASSIR 4. Depending on the detector, their functionality and settings procedure vary:

**Common** slow down detector:

- detects objects of a certain size;
- uses the entire filming area for analysis;
- helps determine the ignore zone;
- does not require a separate license.

**Advanced** slow down detector:

- detects objects of various sizes;
- uses specified filming areas for analysis;
- has advanced detection settings;
- uses 2 detection algorithms;
- works by schedule;
- is licensed per channel.



Setup procedure of each detector is described in their relevant sections:

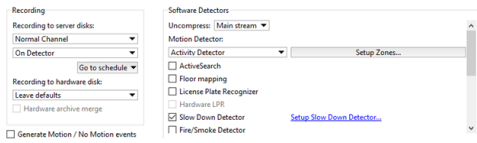
- [\*Common Slow Down detector settings\*](#)
- [\*Configuration of the Advanced Slow Down detector\*](#)



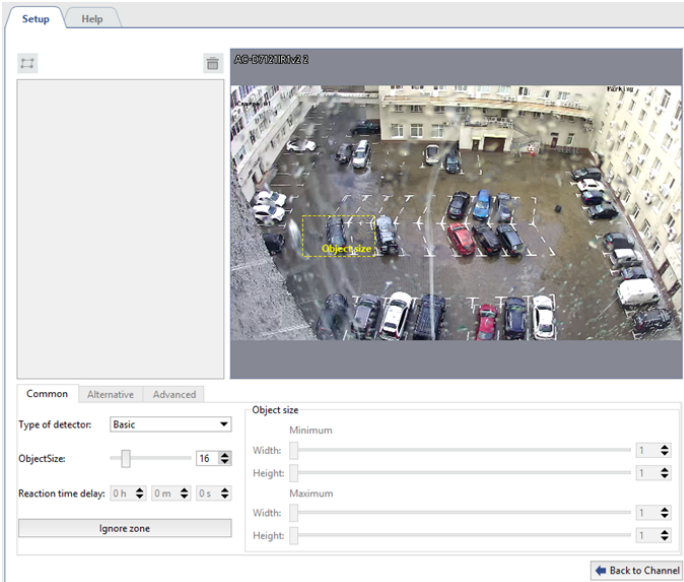
- [\*Channel settings\*](#)
- [\*Motion detector settings\*](#)

## Common Slow Down detector settings

To connect and set up the detector, in the *Channel Settings* set **Slow Down detector** checkbox and click **Setup Slow Down detector...** link



In the **Common** tab of the window that opens, select **Basic** in the **Type of detector** field.

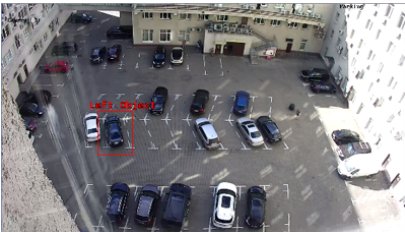


By default, the detector monitors appearance of abandoned objects across the entire image area. If necessary, you can decrease this area. To do that, click **Ignore zone** button and holding the right button select image areas the detector should ignore.

Using **Object size** settings determine an approximate size of the object, the detector will respond to.

The yellow rectangle on the image will help to evaluate the sizes of the object to be detected. Any object that significantly exceeds this size will be ignored.

In case of successful detector configuration the left objects will be highlighted with a red rectangle.



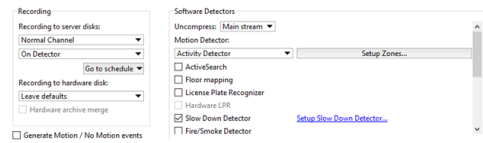
To monitor changes in the detector's operation, enable displaying of figures on the channel **Slow Down detector** (see section ???).



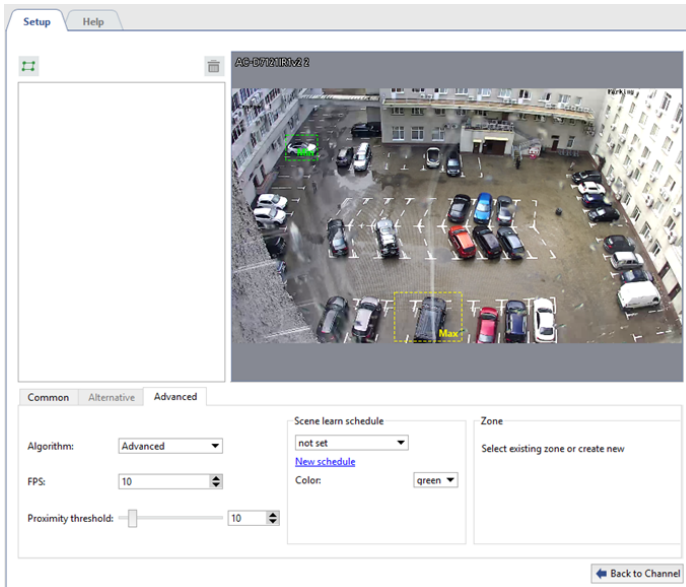
- [Channel settings](#)
- [Motion detector settings](#)
- [Slow Down Detector](#)

## Configuration of the Advanced Slow Down detector

To connect and configure the detector, select in *Channel settings* **Slow Down detector** checkbox and click **Setup Slow Down detector...** link



In **Common** tab of the window that opens, select **Advanced** in the **Detector type** field.

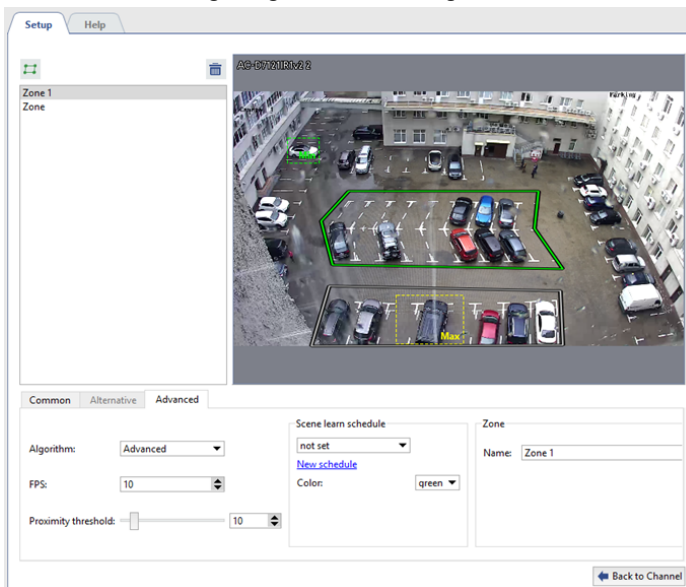


Next, using **ObjectSize** setting, you can determine a **minimum** and **maximum** size of the object, the detector will respond to. Rectangles on the image will help to evaluate its size. The detector will trigger if the abandoned object is bigger than the green box, but smaller than the yellow box.

The **Sensitivity** option determines the degree of the detector's sensitivity.

**Reaction time delay** is the time passed from detecting of an abandoned object to notifying about it.

To continue configuring the detector, go to the **Advanced** tab.



The advanced slow down detectors analyzes the video using two algorithms: **Simple** and **Advanced**. We recommend to start configuring with the simple algorithm. If the detector shows false triggering in its operation, change the algorithm for **Advanced**.

**Frames per sec** settings determines the speed, with which the detector will try to detect abandoned objects.

In the **Proximity threshold** setting, you can specify an approximate distance between a person and the object they abandoned. Should this distance be exceeded, the detector will consider the object abandoned. As the setting is changed, you can see on the video images from the camera, which you can use to evaluate the distance between the object and the person.



In the **Scene learn schedule** group of settings, you can configure the detector operation schedule. Click **New schedule** link to create a new schedule or **Settings** to change the existing one. In the **Color** box, select the area color for the schedule, during which the abandoned objects will be detected. See for details of schedule creation process in the **Schedules**.

Select the image areas, where left objects will be monitored. To do that, click  and clicking sequentially the left mouse, specify the box vertices. Once you are done, click **Finish**. If necessary, specify the area name.

In case of successful detector configuration the left objects will be highlighted with a red rectangle.



To monitor changes in the detector's operation, enable displaying of figures in the view options of the **Slow Down Detector** (see section ???).



- [Channel settings](#)
- [Motion detector settings](#)
- [Slow Down Detector](#)

## Face recognizer

The module is designed for automatic detection and recognition of faces in the camera image and can be used in video surveillance systems to control people entering the territory, analysis of large crowds, etc.



There are two versions of the module built into TRASSIR: **Face Recognizer** and **Face Recognizer 2.0**. Each version has a number of particular characteristics:

**Face recognizer** can operate:

- **locally** on all TRASSIR servers (face database can be located on any server);
- **remotely** on all TRASSIR servers (face database can be located on any server).

**Face recognizer 2.0** can operate:

- **locally** on TRASSIR OS server of **NeuroStation** versions (face database can be located on any server);
- **remotely** on all TRASSIR servers (face database should be located on analytics server).



Features of the module remote mode operation settings:

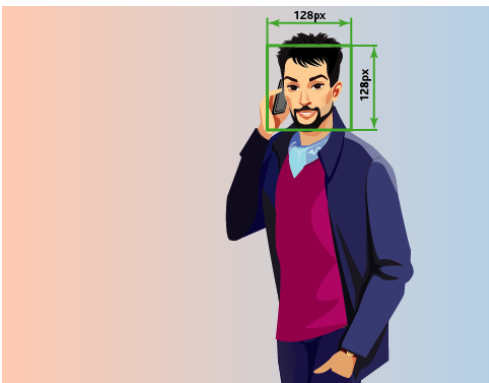
- The server with cameras that recognize faces must be connected to the server with TRASSIR OS, which will be used as **Analytics Server**.  
The TRASSIR OS server of **NeuroStation** version can be used as analytics server.  
Read more about server connection in [Connecting to a new server](#).
- Check the [Enable remote analytics](#) flag in the user's settings, which will be connected to the analytics server.
- The number of channels that can be used by the module are determined by the **by the license on the analytics server**.

## Module options

Face recognizer	
Human face detection	
Face tracking	
Face identification and quality assessment	
Identifying gender and age by face	
Recognizing specific attributes of a person's appearance	In a appea
Ability to recognize the usage of photo in frame	
Searching by face in the archive	
Using module in Access Control	

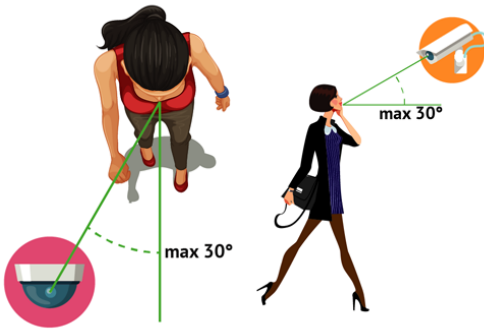
## Recommendations on choosing and setting up a camera

- The sensor size should be at least 1/3", the lens aperture should not be less than F1.4. In case there are high-contrast areas with various degrees of light in the shooting area, it is recommended to use cameras with a hardware WDR.
- To work with the plugin, it is recommended to use a camera with a varifocal lens that will allow you to zoom the shooting area in or out without changing the camera position. It is not recommended to use fish-eye lens cameras.
- The camera should be set to the minimal shutter speed and minimal GOP.
- It is recommended to disable noise reduction and other digital image transformations.
- The image should be clear and without any distortions. The faces in the image should be sufficiently contrasted, illuminated and clearly distinguishable to the naked eye.
- The distance between the pupils in the image must be at least 60px. Use a camera with any resolution, but so that the size of the face in the frame is greater than 128px.



## Recommendations on choosing angle and lighting

- The survey area where faces are detected must be well lit. The presence of shadows on the face or excessive light will significantly reduce the probability of recognition of the person.
- The installation of multiple cameras is recommended for broad areas.
- The shooting direction should be in such a way that people's faces look directly into the camera lens. It is allowed to rotate the camera horizontally or vertically, but not more than 30 degrees. The best recognition quality is achieved when the faces are tilted by no more than 15 degrees.



- [Face recognizer basic settings](#)
- [Face recognizer settings for the channel](#)
- [Face recognizer 2.0 settings for the channel](#)
- [Face database](#)



## Face recognizer basic settings

The "Face recognizer" basic settings vary depending on module version. You can find the settings on the **Modules** -> **Face recognition** tab.

- **Face recognizer**

Channel Name	Age/Gender	Attributes	Liveness	Face Analytics	Face Search	Recognize
Faces	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- **Face recognizer 2.0**



Some module settings can be changed individually for each channel, if necessary (see *Face recognizer settings for the channel* and *Face recognizer 2.0 settings for the channel*).

## General settings

The module can process images from all cameras connected to it simultaneously. The maximum number of simultaneously activated detectors is determined by the license and displayed in the **Available licenses** block in the **detectors** field.

The module uses two databases in operation:

- **Temporary Face Database** for keeping all recognized faces. Its size is defined in the **Storage depth** setting. It is used by *Face Recognizer 2.0*
- **Face database** containing information about the person and his anthropometric data, which is used for comparison with the person found on the video. The maximum size of this database is determined by the license and displayed in the **Faces DB size** field.

**Maximal thread count** is the number of "queues" in which faces are detected. In each frame received, it tries to detect a face and, by increasing the number of streams, you increase the detection rate. The maximum value of streams is limited by the number of processor cores on the server.



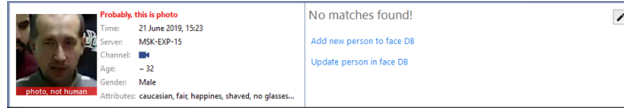
Be careful, increasing the number of streams will increase the server load.

The plugin can search for faces on all frames. However, not all frames show human faces in a good quality. In order to prevent false detections, change the following settings:

- The **Physical Access Control System mode** flag enables the detector's Physical Access Control System mode. Press the **Set default settings** to enable detector's settings optimized for Physical Access Control System operation.
- **Quality threshold** excludes poor quality faces: greased, partially hidden, etc.
- **Confidence Threshold** is the boundary that determines the degree of compliance of the detected person and a person in the faces database.

- **Minimum face size** and **Maximum face size** determine the range of sizes of the faces the module works with.
- **Detection period** is an interval between the frames that will be used to detect faces, the smaller it is, the more often faces will be searched on the video.
- **Detection algorithm** is an internal set of rules, with the help of which a face is detected on video.
- **Recognition algorithm** is another set of rules, with the help of which faces are recognized among the detected ones. The algorithm is selected depending on the required detection quality and the resources of the server which will analyze video:
  - ALG1** - average recognition quality with the moderate resource usage;
  - ALG2** - high recognition quality with average resource use;
  - ALG3** - the highest recognition quality with the use of large amount of resources.

- **Liveness threshold** - is a level of alikeness of the detected face to a human or a photo.



- **Emotion Algorithm** - is a set of rules allowing to show only happy looks from all detected faces.

Moving person can turn his head or face and can hide behind natural obstacles. Set **Merge short tracks** flag and the module will combine these movements into one, depending on the following parameters:

- **Cache lifetime** is the time during which the module stores the face of one person, found in different frames. For example, a track lifetime is 5 seconds, the module detected the face and the person turned away from the camera. If he turns back 4 seconds, then the face information will be added to the existing record. And if in 6 seconds, then a new one will be created.
- **Similarity threshold** is the boundary that determines the degree of similarity of detected and stored earlier face of a person. If the face looks alike, the information about it will added to the current database record. If not, then a new one will be created.
- **Detect More** - in *TRASSIR Face Recognizer* settings, set the **Determine gender** and **Determine age** flags, in order to display this information in the operator's interface when a person is recognized.

## Face database

Database	
Location:	Local server
Status: ready	<a href="#">view content</a>

**Face database** can be stored both locally and on any TRASSIR server with the appropriate license. In order to connect to the database, [configure the connection to the server](#) and specify it in the **Show face DB** configuration. To use a local database, select the name of the custom server. And to go to the [face database](#) click the appropriate link.



TRASSIR uses local face database cash for detection. That's why in case of the face database server connection loss, the face detection will continue. Local face database cash will be updated upon the connection recovery.

## Channel management

Channels						
Channel Name	Age/Gender	Attributes	Liveness	Face Analytics	Face Search	Recognize
<a href="#">TR-02111R3W.1</a>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

At the bottom of the window, a list of cameras with enabled **Face tracker/recognizer** module is displayed. Clicking on the link will take you to the module settings on the selected camera. By setting the appropriate flag in front of the camera, you will enable:

- **Age/Gender** - displays a person's gender and age *in operator interface*.
- **Attributes** is face search by specific human appearance attributes.
- **Liveness** is a feature distinguishing a person from photo or image on video.
- **Analytics** - sends data on the recognized face to the "Analytics" script.
- **Face Search** - *search by face and photo* functions.
- **Recognize** is a face detection feature with the help of *face database*



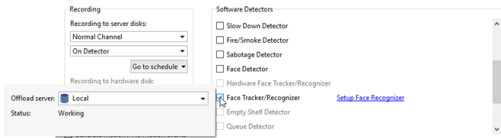
For a detailed description of the operator interface, see [Face recognizer](#) section of Operator manual.



- [Face recognizer](#)
- [Face recognizer settings for the channel](#)
- [Face recognizer 2.0 settings for the channel](#)
- [Face database](#)

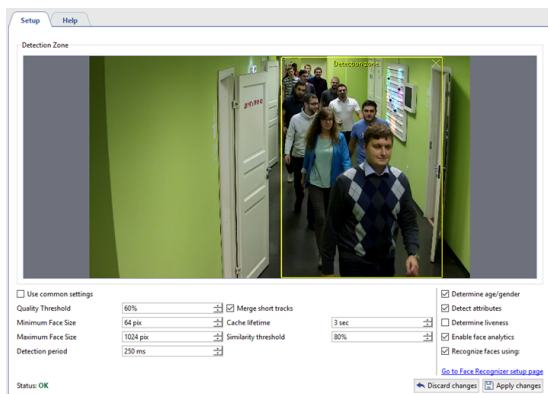
## Face recognizer settings for the channel

To activate the plugin, go to the *Channel settings* to the *Software detectors* area and select the *Face Tracker/Recognizer* and then select the *Server*, which will calculate the analytics. Click the *Setup Face Tracker/Recognizer* link to open the settings window.



In the window opened:

- Determine the *Detection Zone* size - the area of the image where faces will be recognized.

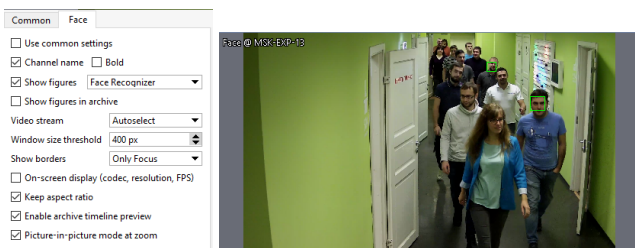


- If common detection parameters are not suitable for the detector operation on this channel, then clear the *Use common settings* checkbox and change them.

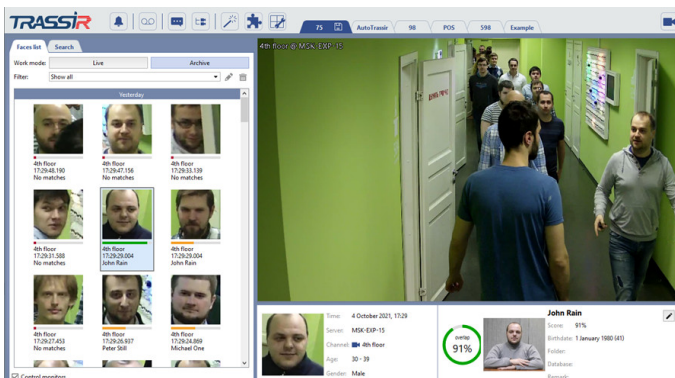


Clicking the *Go to Face Recognizer setup page* link you will go to the global settings of the detector. Description of the detection parameters can be found in the section *Face recognizer basic settings*.

You can check the correctness of the detection settings by turning on the display of the figures. To do this, right-click on the image, select *View options* from the drop-down menu, set the flag next to *Show figures* menu item and select *Face Recognizer* from the drop-down list. The recognized faces will be highlighted in the image:



The full operation of the module can be seen in the operator interface. To do this, you can *create a simple template*.

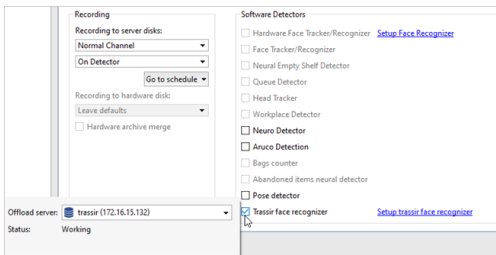




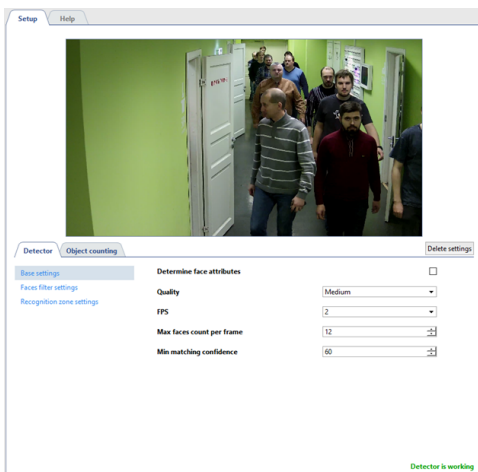
- *Face recognizer*
- *Face recognizer basic settings*
- *Channel settings*
- *Motion detector settings*

## Face recognizer 2.0 settings for the channel

In order to activate the module, go to the *Channel settings* to the *Software detectors area* and select **Face recognizer 2.0**, then select the **Server**, which will calculate the analytics.



Press the **Face recognizer 2.0 settings**. The detector settings will open.



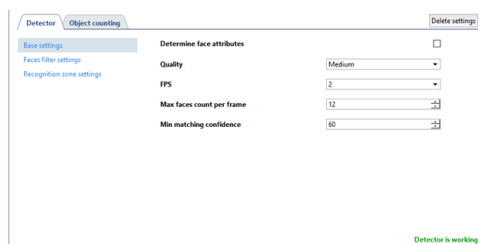
You can check the correctness of the detection settings, by enabling the figure display. To do this, right-click on the image and select the **View options...** item in the drop-down menu. Set the **Show figures** flag and select **Face recognizer** item in the drop-down menu. The recognized faces will be highlighted on the image:



You can check the full module operation in the operator interface. *Create a simple template* to do this.

You can configure the operation of the detector on the **Detector** tab.

- The **basic settings** of the detector let you configure the following parameters:



- Determine face attributes** - set the flag to display gender and age when a person is recognized.
- Quality** - select the speed and quality of the detector operation. The higher the recognition quality is, the lower is the processing speed, and vice versa.



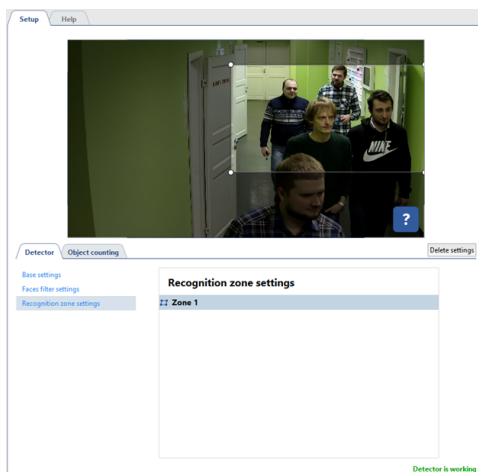


To ensure the detector correct operation, you should select the same quality in the analytics server settings as in the detector settings.

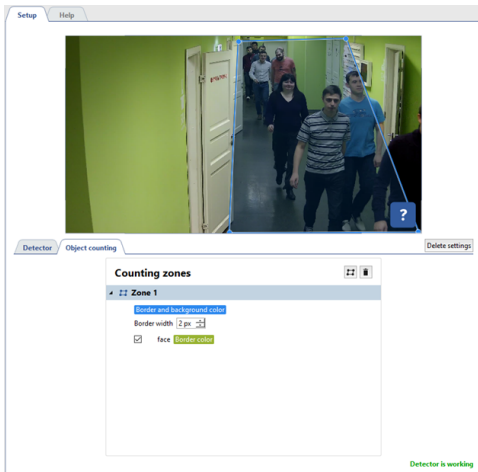
- **FPS** - frame rate.
- **Max faces count per frame** - set the maximum number of faces that the detector can recognize in one frame. If the number of faces exceeds the selected value, the detection frames around them will be gray, and such faces will be displayed as unrecognized in the operator interface.
- **Min matching confidence** - set the degree of correspondence between the detected person and the person in face database.
- The **Faces filter settings** menu lets you set up the recognized face parameters.




- **Min face image side size** and **Max face image side size** - set the range of face sizes with which the module works.
- **Allowed face angles** - the range of face tilt / rotation angles, in which the module can recognize a person: narrow axis - head tilt forward / backward, vertical axis - face turns right / left, roll axis - head tilt right / left.
- **Sensitivity** - the detector sensitivity level. The higher the value is, the higher is the probability of false alarms.
- The **Recognition zone settings** menu lets you specify the area in which faces are recognized. The neural network does not transmit the entire image from the camera, but a selected part of it, which improves the recognition quality. Unlike detection zones, the recognition zone is always rectangular. You can resize it by dragging the vertices.



The **Object counting** tab lets you create zones in which faces will be detected. By default, there is a zone created in the settings that occupies the entire image area. You can adjust its size by changing the position of the corners, if necessary.



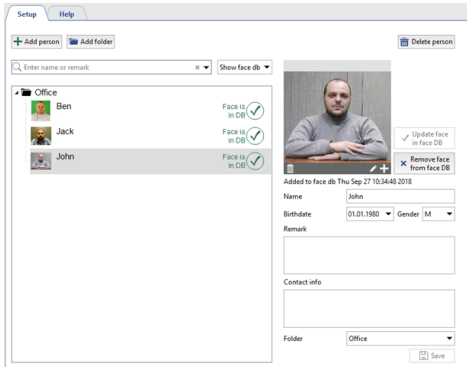
In order to create a new **counting zone**, press  and set its vertices on the image. Place the cursor to the zone starting point and left-click or press **CTRL+ENTER** to complete the zone drawing.



- *Face recognizer*
- *Face recognizer basic settings*
- *Channel settings*
- *Motion detector settings*

## Face database

**Face database** is a part of *Persons database*, which includes people and their anthropometric data. Face database is used for comparison with faces that *Face Tracker/Recognizer* module detects on camera image.



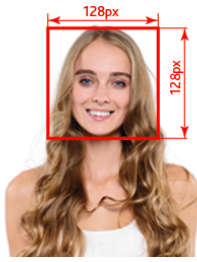
For a detailed description of the person creation process, see *Persons* section.



TRASSIR can use a unified or **central face database**. For this purpose, a number of requirements should be met:

- All face detecting servers and the server, containing the central face database, should have the relevant licenses.
- You should select the server, containing the central face database from the *Face recognizer setup* in the *Location* list.
- Face detecting servers should connect to the central face database server regularly to synchronize the data. In order to reduce the network load, a special script can be used. To receive the script and its description, please, contact technical support.

## Recommendations to the photos used for recognition



TRASSIR uses all photos in the **Face database** for recognition. The probability of recognizing a person caught in a camera depends on the quality of the photos loaded to the TRASSIR. To increase the probability of recognition, use the following guidelines:

- You can upload several photos for one person, one of which must be taken in full-face, and the rest are allowed to rotate no more than 30 degrees vertically or horizontally. Photos in which the person is depicted half-face, will significantly reduce the probability of this person recognition.
- If a person wears glasses, then upload a photo with glasses to improve recognition.
- Photos on which a person's face is blurry, lighted or in shadow will significantly reduce the probability of recognition.
- The face on the photos should not be smaller than 128x128px.

### Examples of photos that improve the quality of recognition



### Examples of photos that reduce the quality of recognition



- [Face recognizer basic settings](#)
- [Face recognizer settings for the channel](#)
- [Face recognizer 2.0 settings for the channel](#)
- [Persons](#)

## Neural Empty Shelf Detector

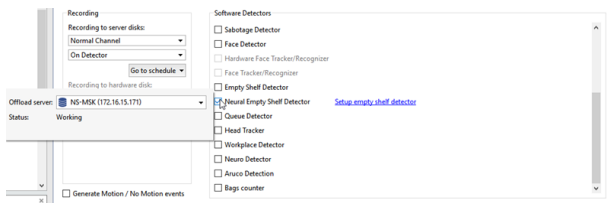
The **Neural Empty Shelf Detector** is intended to build up video surveillance systems which require the detailed analysis with the help of the neural networks. As a result, the video surveillance operator will monitor the shop shelves state in real time.



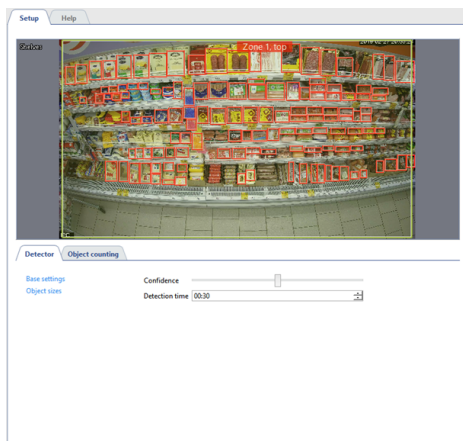
### Neural empty shelf detector features:

- This plugin operates on **NeuroStation** video recorders or on any video recorder which has TRASSIR 4 installed and is connected to **NeuroStation** server, which will be used as **Analytics server**. Read more about server connection in [Connecting to a new server](#).
- Check the [Enable remote analytics](#) flag in the user's settings, which will be connected to the analytics server.

To activate the plugin, go to the [Channel settings](#) to the [Software detectors](#) area, select the **Neural Empty Shelf Detector** and then select the **Server** which will calculate the analytics.



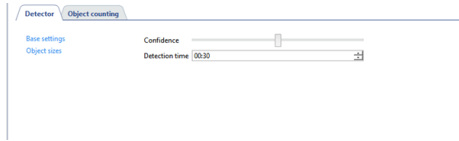
Press [Setup empty shelf detector](#) to open the settings window.



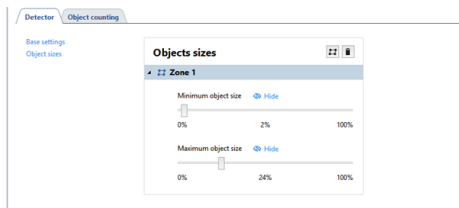
## Detector

The detector's parameters are set up on the **Detector** tab.

- Set the detector's **Sensitivity** and specify the **Detection time** in the **base settings**.

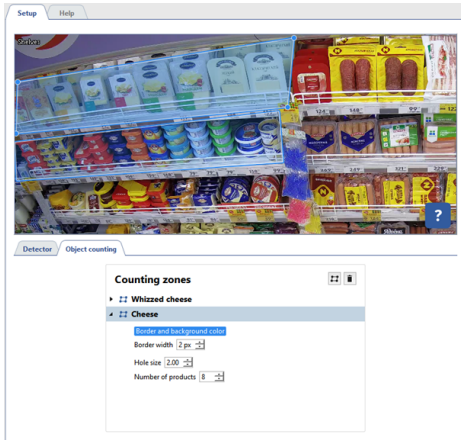


- You can create the zones in which empty space on the shelves will be swept in the **Object sizes** settings group. Set the biggest and the smallest sizes of the detected objects with the help of **Minimum object size** and **Maximum object size** settings.



## Object counting

The **Object counting** tab lets you create the zones to detect empty spaces on the shelves. There is already a default zone created, which occupies the entire image. You can correct its sizes by changing the position of the angles.



To create a new **counting zone** press **Ctrl+N** and set its vertices on the images, starting from the upper right and then in the clockwise direction. In order to finish the zone drawing, place the mouse cursor to the zone starting point and then left-click or press **CTRL+ENTER**.



Counting zones requirements:

- The zones should be four cornered.
- The zones should be drawn in such a way, so they won't capture price tags or shelves partitions.
- To detect holes in the first or the bottom row only, the zone should be drawn in such a way, so the goods from the second row stay outside this zone.



For each created zone should be setup parameters by which the detector will detect empty spaces on the shelves:

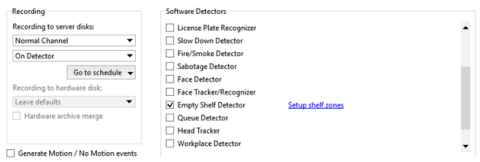
- **Number of products** - is the number of the units of goods or the piles of goods, aligned in a row by the counting zone.
- **Hole size** is the number of the units of goods or piles, the absence of which will be detected by the detector.




- [Motion detector settings](#)
- [Channel settings](#)

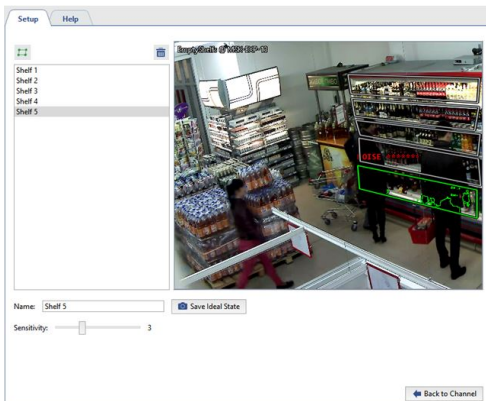
## Empty Shelf Detector







The shelf detector is intended to track the good availability on the shop shelves. With its help TRASSIR will compare the current state of the specified shooting area with the previously saved image and notify the operator of the changes. To set up the empty shelf detector zones open [Channel settings](#) in the [Software detectors](#) area and select **Empty shelf detector**. Click the **Setup empty shelf detector** link to open the setting window.

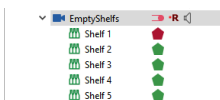


In the window that opens you can create detector zones - the areas which will be monitored by the detector:

1. Click the .
2. Consecutively left-click with the mouse to specify the vertices of a polygon. Upon completion, click **Finish**.
3. Enter the zone name.
4. To set the zone's current state as the ideal state, click the **Save Ideal State** button. When recording a shelf's ideal state, the amount of motion (noise) in the frame must be observed. The noise level is represented by stars on the video frame. The fewer the stars, the less noise in the frame and the more accurately the detection zone's ideal state will be recorded.
5. Use the **Sensitivity** slider to set a value for the zone. The higher the value, the more sensitive the detector will be to changes in the frame.



You can track the detection zones' state in real time in the object tree (CMS). When the number of items decreases, the color of the selected zone's indicator will change  →  →  →  →  → .



To track the detector's state in a timely fashion, you can create a [rule or script](#) that will activate when the state changes.



- [Channel settings](#)
- [Motion detector settings](#)



## Queue detector and workplace detector

**Queue detector** module can be used in the security systems' construction (to detect congestions in the pre-set area), as well as in business analytics, i.e. to count the number of people in the queue.

**Workplace detector** module is designed to estimate the actual employee's work time.

To ensure the correct operation of the modules the analysable image from the camera should meet a number of mandatory requirements:

- The module detects a person by head and shoulders, so the image of the person should include his/her shoulders under the head or the head over the shoulders (at plan view).



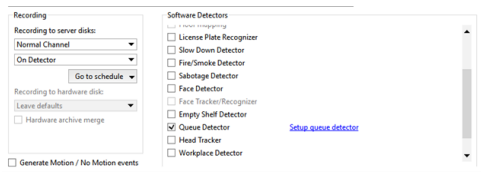
- The size of the head on the image should be of 40 pixels at least and should not exceed 25% of the entire frame size.
- The size of the head at the image limiting points should not alter more than twice.



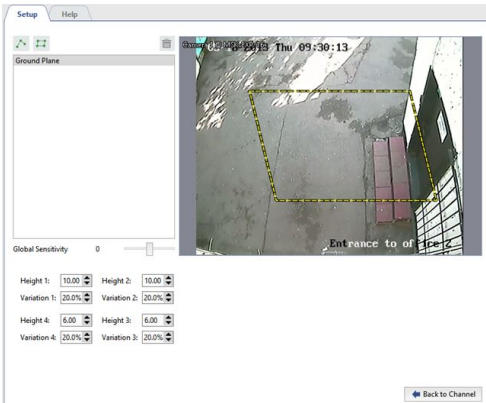
- *Channel settings*
- *Motion detector settings*
- *"Queue detector" module settings*
- *Workplace detector module settings*

## "Queue detector" module settings

To activate the plugin go to *Channel settings* to the *Software detectors* area and select *Queue Detector*. Click the *Setup queue detector* to open the settings window.



In the opened detector settings window a *Ground plane*, which should be configured, will be already created.



A camera is usually pointed at an angle relative to the surface of the floor. Accordingly, the same person will have different dimensions in various places on the frame. For the counter's proper operation, the *Ground Plane* must be configured to enable counting in the entire area. To do this, move the Ground Plane's vertices to define the area within the frame to be monitored by the counter. Then sequentially select the vertices and use the *Height* settings to define the size of a person's head at the extreme positions of the Ground Plane.

The counter can be more accurately configured with the assistance of a helper. You can verify the accuracy of the selected settings based on the size of his/her head. Ask your helper to move sequentially to each of the Ground Plane's vertices. Change the values of the *Height* parameters to specify the size of a head. So, you can verify the size of your helper's head using an indicator consisting of concentric squares. If you point it at a person's head, green squares will indicate that at that position in the frame people with heads that fit within the green squares will be detected, while people with heads the size of the gray squares will not be detected by the counter.



If you have no helper or cannot use it, you can go to an archive and configure the counter using saved video segments.

The *Variation* parameter defines the range of the *Height* parameter. For example, if it is 10%, then the counter will analyze an area 10% smaller and 10% larger than the selected area.


To prevent false triggerings, adjust the *Global Sensitivity* parameter.

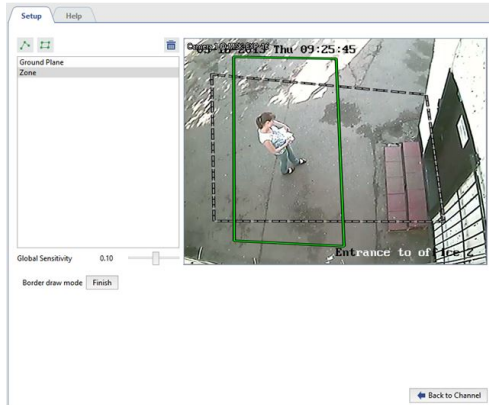
If the counter is configured correctly, the heads of people within the frame will be highlighted with a blue square.




Queue detector can be used to count the number of people:

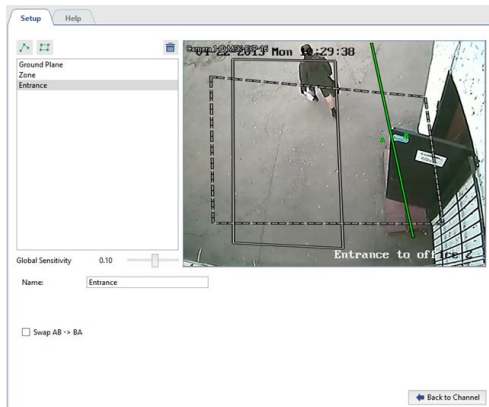
- within a selected area.







To do this, click the  button and specify an area within the Ground Plane.

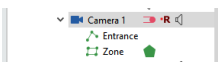


- intersecting a border line from either direction.

To do this, click the  button and add the border line. If needed, you can switch the locations of zones A and B by setting the **Swap AB -> BA**



In a real-time environment the selected area status and limits can be monitored in the object tree (CMS). When the number of people in the selected area increases the indicator will change the color  →  →  →  →  → :



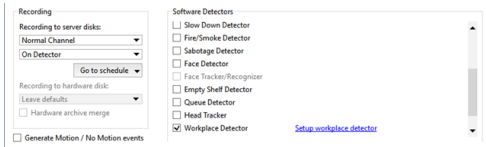
To track the detector's state in a timely fashion, you can create a *rule or script* that will activate when the state changes.



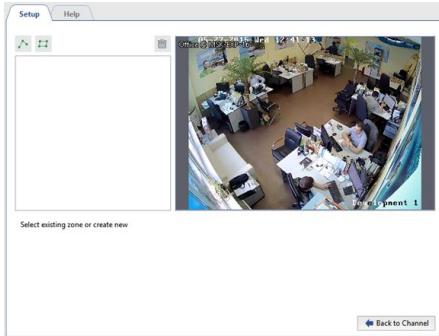
- [Channel settings](#)
- [Motion detector settings](#)

## Workplace detector module settings


To activate the plugin go to the *Channel settings* to the *Software detectors* area and select **Workplace detector**. Click the **Setup workplace detector** link to open the settings window.



Detector settings window:



Create detector's zones - the areas which will be monitored by the detector.

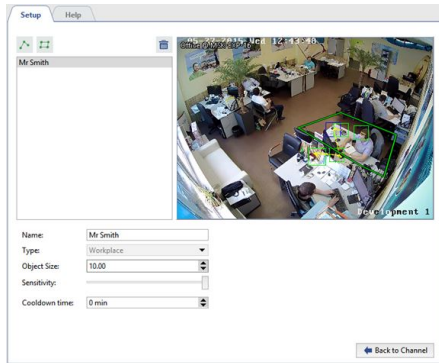
1. Press the button .
2. Set the vertex of the polygon by pressing the left mouse button sequentially. Upon completion press **Finish** button.
3. Set the zone name, i.e. employee's name or the name of the workplace.

After that the parameters where the detector will be activated should be defined for each zone:

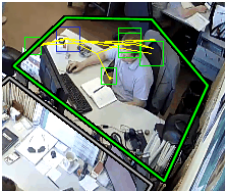
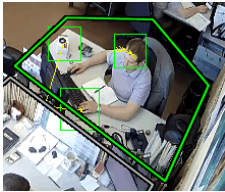
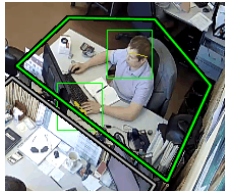
- **Object size** - the size of the head of the monitored objects.
- **Sensitivity** - the level of the detector's sensitivity.
- **Cooldown period** - the duration of motion absence in the zone.

## Setting procedure

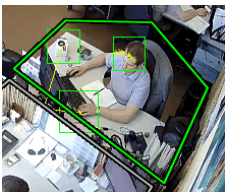
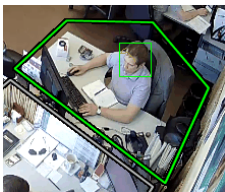
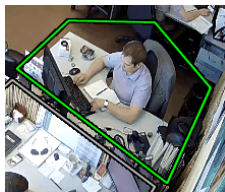
1. Move the **Sensitivity** slider right to adjust the detector's sensitivity above average. You'll see false triggerings of detector on the display in the shape of several squares.





2. Increase or decrease the value in the **Object size** field, so that a person's head would fit the green square.

Small	Optimal	Large
		

3. Move the **Sensitivity** slider left to prevent false triggerings.

High	Average	Low
Detects multiple objects.	Detects one object.	Detects nothing.
		

4. To prevent detecting a motionless person as employee's workplace absence, increase the **Cooldown period**.

You can monitor the zones' status in objects tree in real time; the indicator will change its color in case of the employee's absence at the workplace  → .



You can set up a **rule** or **script** triggering on the status change for the immediate detector's status monitoring.







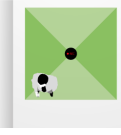
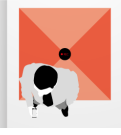
- [Channel settings](#)
- [Motion detector settings](#)

## Head Tracker





**Head Tracker** module is a light version of the [Queue detector](#) and is designed to define the number of people crossing the preset border line on the camera image in one or other way.

To ensure the stable operation of the module the survey coverage and the camera installation location should meet the following requirements.





### 1. Select the camera installation location properly

Requirements	CORRECT	INCORRECT
The camera should be installed above the people passage point.		
No camera tilt is allowed. The camera lens should be directed vertically down. In this case the image of the camera will run parallel to the floor.		
The object size on the image should be 5% at least and 25% at most of the entire frame. The range of the width of the camera image should be from 600px to 700px.		

### 2. Check the lighting conditions

Requirements	CORRECT	INCORRECT
The survey area should be moderately lightened. Insufficient or excessive lighting of the survey area negates the effectiveness of the module.		
Prevent any sharp alterations of the lighting conditions. The survey area must not have any specular surfaces. Hard shadows of moving objects interfere with the module operation.		

### 3. Disturbances in the survey coverage

Requirements	CORRECT	INCORRECT
Static background without any moving objects (moving stairways or moving walkways) ensure the stable operation of the module.		
Constantly opening doors and other objects showing in the survey area decrease the module efficiency.		



- [Channel settings](#)
- [Motion detector settings](#)



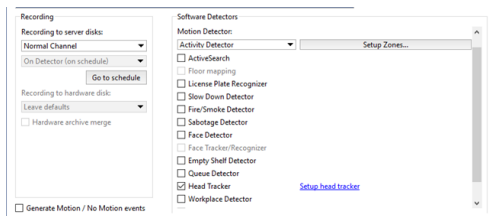
## "Head Tracker" module settings

To activate the plugin go to the *Channel settings* to the *Software detectors* area and select **Head Tracker**. Click the **Setup head tracker** link to open the settings window.




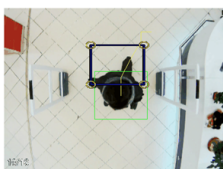
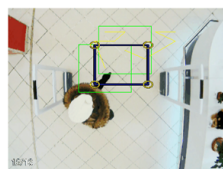
Set up the module:

1. Change the size of a rectangle so that an average sized person would fit in.



You can define the maximum size of the object by the value in the **Object size** settings. In case they exceed the allowed value you should change the settings or *camera location*.

2. Then in the **Detection algorithm** settings select **Standard** and by dragging the **Sensitivity** slider set the best settings value.


Low	Optimal	High
Object can not be detected in the frame.	Object is detected correctly.	One object is detected as 2 or more.
		



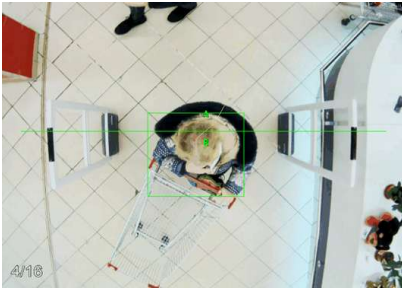
If the optimal result fails to appear under the given parameters, select **an alternative** detection method and repeat the settings.

3. Other parameters help to enhance the module operation:

- **Operation resolution** settings lets you select the size of the image which will be used to analyze the scene. **Low resolution image analysis is the most cost-effective way to use the server resources**
- **Distance to the floor** - this parameter depends on the camera height and the zoom level set on it. It can be identified by the size of the object in picture. The bigger it is the less is the distance to the floor. (less than 14,5% is **high**, from 14,5% to 18,5% is **average** and over 18,5% is **small**) Leave **Auto** box checked and it will set up with reference to the **Object size** field value.

4. Locate the border line to be crossed by people. To do this press the button  and, sequentially clicking with the left mouse button, specify the vertices. If necessary, you can enter the boundary name and set the **Swap AB -> BA** checkbox in order to switch the A and B zones.

If the module has been set up correctly, the captured in the frame people will be outlined with a green rectangle.



To track the module's state in a timely fashion, you can create a *rule or script* that will activate when the state changes.



- *Channel settings*
- *Motion detector settings*



## Neuro detector

The **Neuro Detector** can be used for building up security systems, which require in-depth image analysis. As a result, the video surveillance operator will get the information on various objects in the specified area in real time.

**Neuro detector** is intended for detecting the following object types on video:

- ordinary people or people wearing the uniform of the specific color;
- a person's head or a person not wearing the special headwear (hard hat);
- a bicycle or a person riding a bicycle;
- a car.

Besides of that, neuro detector can be used for counting objects in the specified area.



The **Neuro detector** plugin operation peculiarities:

- The plugin works with **NeuroStation** video recorders or with any dashboard cameras with TRASSIR 4, connected to **NeuroStation** server and using it as **Analytical server**. See details of a server connection in the section [Connecting to a new server](#).
- In the user settings from which connection to analytical server is established, the analytics shall be [allowed via network](#).
- The operation of the **Count objects**, **Track objects** and **Build heat map** parameters is defined by corresponding license availability on the analytics server.

Follow the below described recommendations to improve the quality of the object detection.

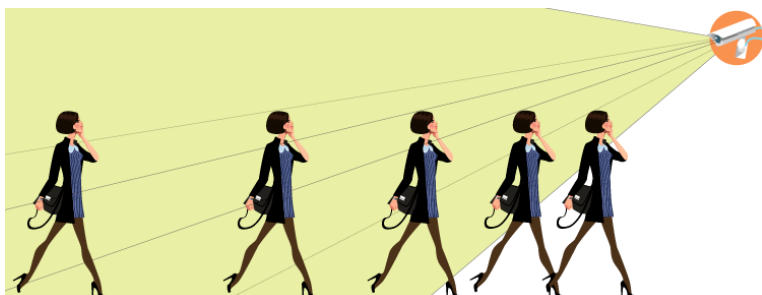
### Recommendations on the camera selection, its location and shooting area lighting:

- The shooting area where the detection will be carried out, should be sufficiently lightened. The shadows could impair the detection quality.
- Video from any camera will suit for plugin operation, including Fisheye cameras that support [software image dewarp](#).
- The camera should be installed at the 30 to 60 degree angle to the people flow or detected objects. The objects appearing in the shooting coverage should not obstruct each other.

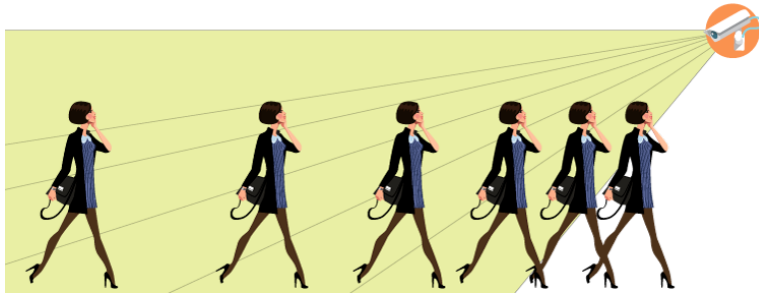


- By using the Neuro detector to detect and count heads, the angle of the camera with respect to the ground plane is selected according to the requirements and the intensity of the stream of people:

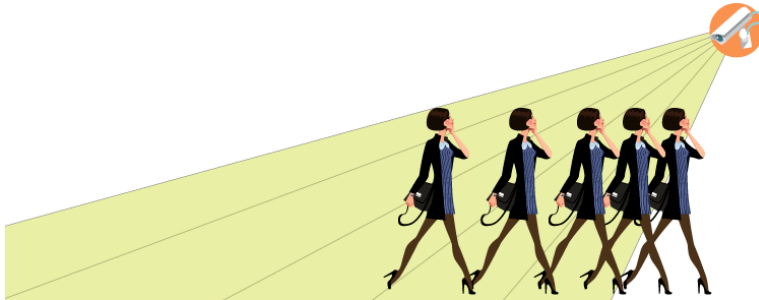
**from 15 to 25 degrees** - people are far away from each other and the exact number of people in the target area is not required.



**from 25 to 40 degrees** - the optimal tilt for the detection and count people that could be enclosed by other people and objects.



**from 40 to 75 degrees** - the flow of people is dense and the exact number of people in the target area is required.



We do not recommend installing cameras at more than 75 degrees as long as in this case a person's head will blend in with the body and become undetectable.

#### Camera settings tips:

To detect objects on video, the plugin can analyze video stream of any resolution and bitrate. TRASSIR will decode the image to the format which is required for analysis. The video recorder resources can be used for image decoding. To reduce the resource exploitation we recommend setting the following values in the [device settings](#):

- Resolution - VGA (640x480) or D1 (720x576)
- Bitrate - from 256 to 512 kB/s



Usually, the devices transmit two video streams (main and substream). The module can use any of them for video analysis. Using a substream will allow you to save the resources of the dashboard camera. At the same time, the main stream can be configured for viewing and archiving.

To use the substream, enable it in the [device settings](#) and adjust its parameters according to the above stated recommendations.



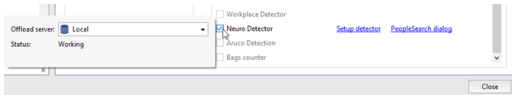
- [Channel settings](#)
- [Motion detector settings](#)
- [Neuro detector setup](#)
- [Classifier](#)

## Neuro detector setup

To activate the plugin go to the [Channel settings](#) to the [Software detectors](#) area, select **Neuro detector** and then select the **Server** which will calculate the analytics.

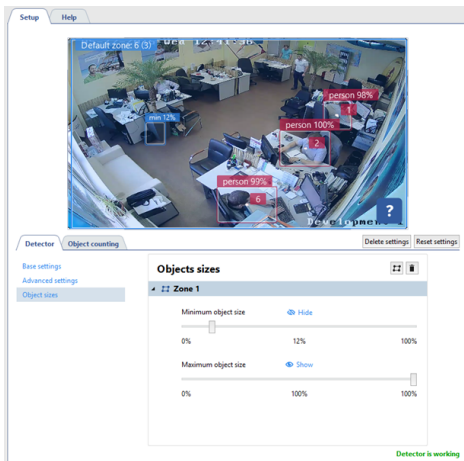


In case the module is activated on the **NeuroStation**, video recorder, in the **Server** settings select the **locally** value. Otherwise select **NeuroStation** server name.



The **Search for detections** link opens the window of object search in the archive. You can read more about this feature in the Operator's Guide (???).

Click **Setup detector** link to open the detector's settings.

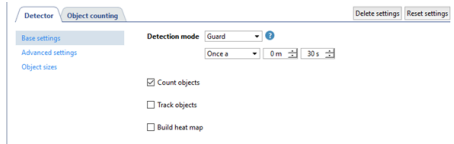


Enable showing the **People/Object detector** figure on the channel before configuring the detector settings and to track the changes in the detector's operation (read more in ???).

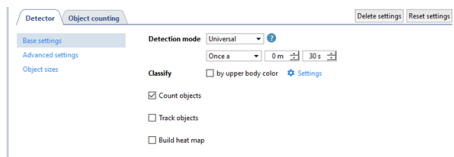
## Detector

Select **Detection mode** in the **base settings** and set up the detection period, depending on the detected objects requirements:

- **Guard**. This mode suits best for outdoor scenes with a decent amount of detected objects. It is designed for vehicle, people, animals and birds detection.



- **Universal**. This mode is designed for outdoor as well as indoor scenes. In this mode the detector detects people, vehicles and bicycles.



If you need to identify people wearing the same color of clothing among all detected objects on video, set the **by upper body color** flag and press **Settings** to choose the required classes.

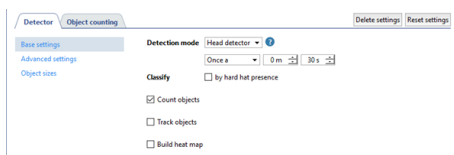
i

To create classes which will be used by the detector, go to the **Server settings** -> **Plugins** -> **Neuro detector**.

The 'T-shirt color classifier' window shows a list of classes on the left: 'employee1', 'employee2', and 'employee3', each with a checkbox. To the right is a color bar with a gradient from purple to red. Below the color bar is a red t-shirt icon labeled 'Average color'. At the bottom are 'Cancel' and 'Ok' buttons.

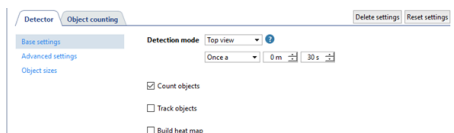
Read more about creating classes in [Classifier](#).

- **Head detector** is designed for detecting people in crowded scenes.



Set the **by hard hat presence** flag to highlight by different colors people wearing and not wearing hard hat.

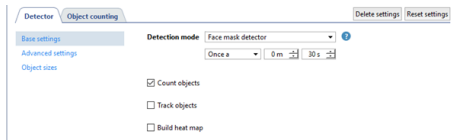
- The **Top view** detects people the same as the **Head detector**. It is designed for scenes with complex angles (i.e. when a camera shots from above or installed at the 75 degree or greater angle).



i

Use this mode only in case there is no option of installing video cameras according to **our recommendations**.

- The **Face mask detector** identifies the faces of people wearing face masks and highlights people with and without the masks by different colors on the image.



The below listed flags enable displaying of the following information on video:

- **Count objects** - the amount of objects, detected in the zone, or objects crossed the specified boundary;
- **Track objects** - the motion track of the detected objects;
- **Build heat map** enables the *heat map building*.



You need to additionally *Calibrate the floor* and *add the ground plane on map* to build the object heat map.

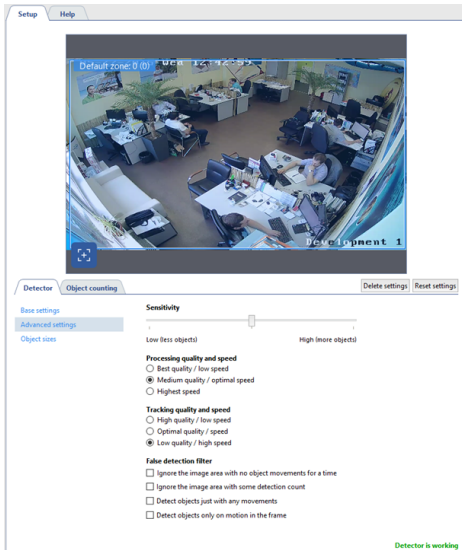


The operation of the detector depends on the **Mode** selected in the *analytics server settings*:

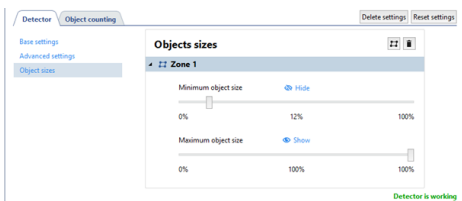
- The **Count objects** and **Track objects** features will operate when the following mode are selected **Default**, **Neuro detector** and **Classifier**.
- The **Classify by upper body color** and **Classify by hard hat presence** work only in the **Classifier** mode.

Read more about analytics server settings and its operation mode in the *Analytics*.

The **Advanced settings** are meant for determining speed and quality indicators of neuro detector operation.



The **Object sizes** option lets you create zones in which the objects will be detected. Using **Minimum object size** and **Maximum object size** settings select the largest and the smallest sizes of the detected objects. Bear in mind the sizes of the detected objects (human height, vehicle size or size of a person riding a bicycle) when choosing sizes.




If the detector is unable to detect an object in any image area, you should set another zone with the other size range for this area.



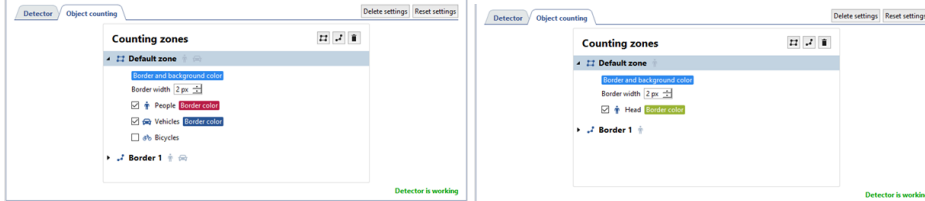
Do not create new object detection zones if it is not necessary, because each new zone increases the server load.


## Object counting

The **Object counting** tab lets you create zones and boundaries for counting the amount of the detected objects. There is already a default zone, created by the detector, which occupies the entire image area.

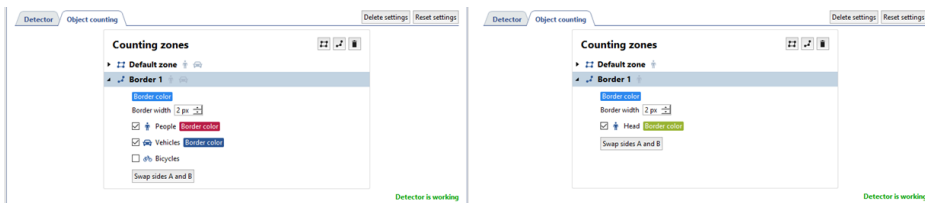
To create a new **counting zone** press  and set its vertices. To finish drawing, left click or press **CTRL+ENTER** at the zone starting point.

The counting zone setup depends on the detected object type:



To create a **border**, press  and set its location points on the image. To finish drawing the border, left-click or **CTRL+ENTER** at the zone starting point.

The counting border setup depends on the detected object:



- [Motion detector settings](#)
- [Channel settings](#)

## Classifier

The classifier lets single out people with a distinctive feature - a specific uniform color, among all the people, detect by *neuro detector*.

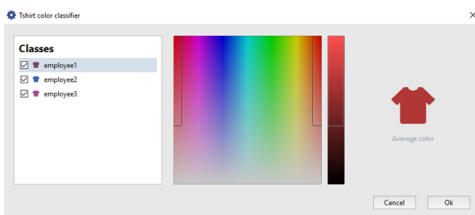
It can be used in the following situations:

- to detect and count the number of store employees in the given area;
- to subtract store employees from the whole number of detected people;
- etc.



Read more about classes for object detection in *Neuro detector setup*.

To create classes, go to **Server settings** -> **Plugins** -> **Neuro detector**.



To create a class press **+** and enter the class name.

You can select the color of the uniform which people of the given class will wear, can be selected on the color scale on the left. The color chart on the right lets you select the range of hues, which will be used by the detector to detect people in various lighting conditions.



To enhance the module operation quality, we advise to use bright and deep colors in the outfit. It will reduce the number of false activations and will allow the detector to detect the required person from the total quantity of the detected people.



- *Neuro detector setup*



## ArUco Detector

ArUco markers are 2D bar code similar to QR-code consisting of single or several segments. Single marker contains a whole number in the range 0 through 999999999999. You can find detailed information regarding ArUco markers at [docs.opencv.org](https://docs.opencv.org).



Using ArUco marker detector, TRASSIR can:

- detect ArUco markers both on static and moving objects;
- decode marker content and display it on operator's display;
- use marker content in the scripts.

### Recommendations on the camera selection and its configuration:

- Camera of any resolution can be used to work with detector however the size of single marker segment in the frame should exceed 25x25 px.
- The bitrate on the camera should be adjusted to provide transmission of video signal without artifacts.
- Marker image on video in detection zone should be distinct and contrast.

### Recommendations on the camera selection, its location and shooting area lighting:

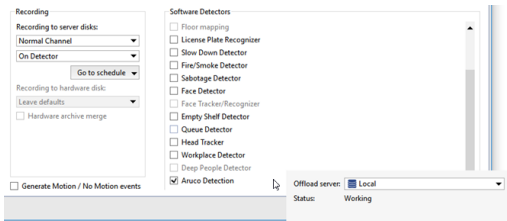
- Shooting area where markers detection takes place should be well lit. Shadows and highlights presence on the marker will reduce probability of its detection and decoding.
- The camera should be mounted in such a way to provide full view of the marker. Partially covered marker will not be detected by the detector.
- The marker should be located at the flat surface. It is allowed to position the marker at the angle not exceeding 45 degrees to the shooting area. Inclination angle increase will reduce probability of its detection and decoding.



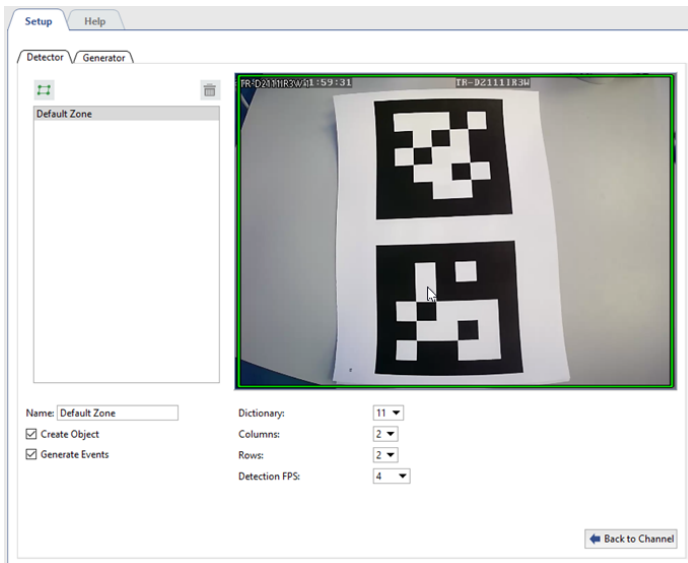
- [ArUco Detection](#)
- [ArUco Marker generator](#)

## ArUco Detection

To activate the plugin, go to the [Channel settings](#) to the [Software detectors](#) area, select **ArUco Detection** and then select the **Server**, which will calculate the analytics. Click **Setup ArUco detector**.



Detector settings window will open:

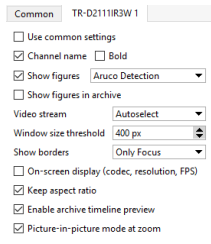


Before the detector settings decide the type of markers which will be detected by TRASSIR. In the section [ArUco Marker generator](#) types of supported markers are described along with their creation procedure. In case you are aware of the type of markers to be detected, go to the detector settings.

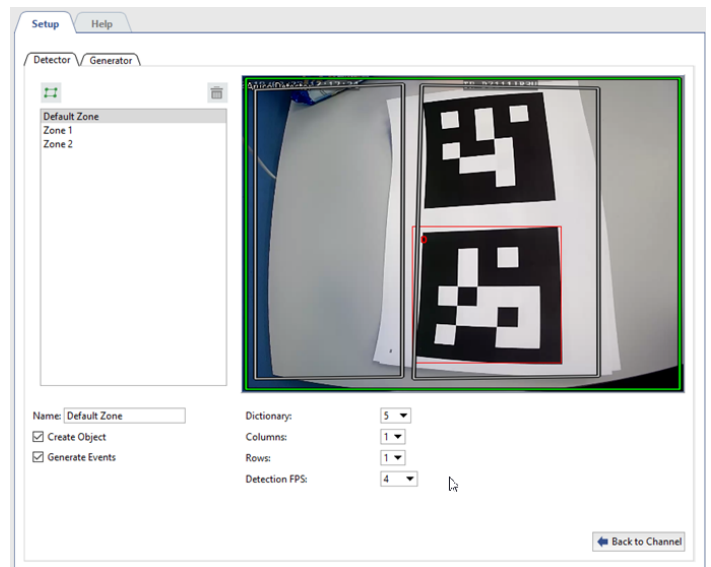
## Settings


### 1. Configure the module preset:

- To trace changes in the detector's operation, activate **ArUco detection** on figures display channel (see section ???).



### 2. General detection parameters.



In the **Detector** tab create one or several areas where markers detection will be done. To do this press the button  and specify the area borders on the image.

Next, set the detector's operation parameters:

- Dictionary** - type of markers to be detected by the detector.
- Columns** and **Rows** - format of markers or number of segments in the marker by columns and lines.



- Detection FPS** - rate of detection to be selected depending on shooting conditions and speed of movement of the object with the marker being detected.

Detector can detect markers both on static objects and on moving ones. For static objects we advise to set the rate **0.25**(1 frame in 4 seconds), and for the objects moving at low speed - **4**(4 frames per second).



Type and format of markers with which detector will operate is written on the sheet with marker. Markers type and format can also be found out at **Generator** tab (see section [ArUco Marker generator](#)).

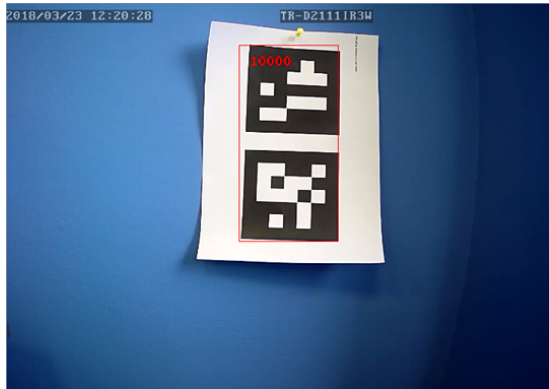


Be careful while selecting detection FPS. Do not set maximum value to detect markers on static or slowly moving objects. The higher the frequency is - the higher is the server load.

### 3. Verify settings correctness.

Put the sheet with the marker to the camera.

Under correct settings of detector, TRASSIR will mark the marker with red rectangle containing the marker value.

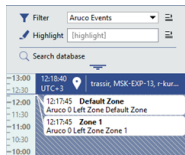


### 4. Set the detector status tracing parameters.

Detector status change can be traced using scripts and event log.

Check **Create object** box to create the object and trace change of its status using [script or rule](#).

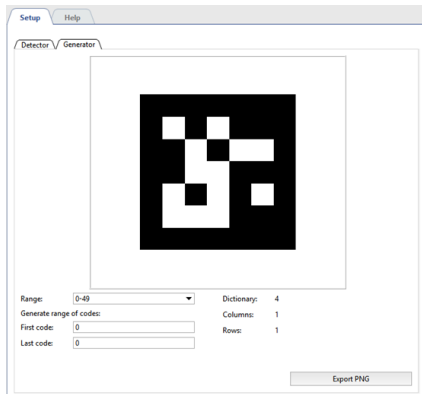
To display detector status check **Generate events** box in the log of events.



## ArUco Marker generator

In the **Generator** tab you can:

- create the required number of markers for printing and stickers for the detectable objects;
- define ArUco markers parameters which will be used for *Detector settings* .



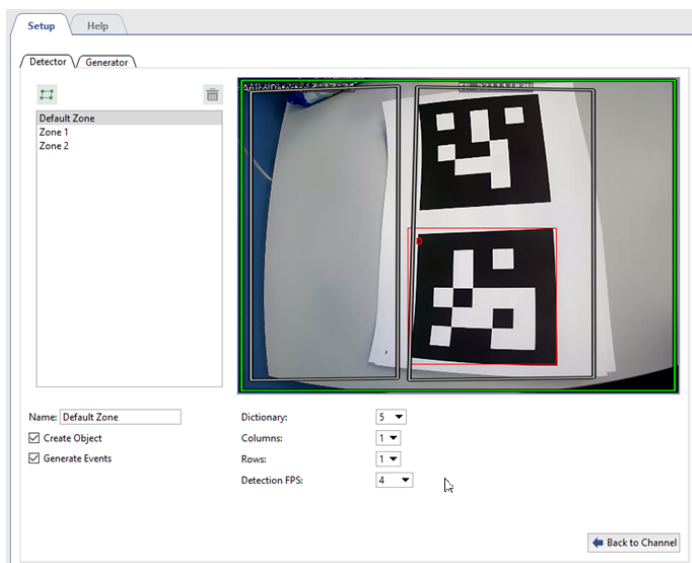
To do this:

1. Select in **Dictionary** field a range of the numbers corresponding to the number of objects which will be marked by the markers.



While setting the value in the **Dictionary** field it is necessary to take into consideration that the detector can operate with a single range of numbers only. So in case you would like to increase the range in future, you need to re-create all markers.

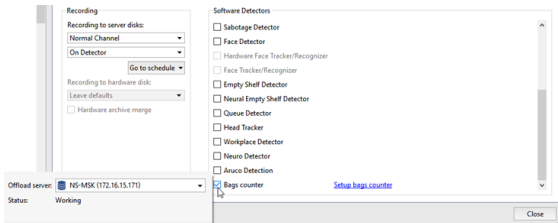
2. To create ArUco marker images, enter the range of numbers into **First code** and **Last code** fields.
3. Press **PNG export** to save the marker images for further printing.
4. The values displayed in the **Dictionary**, **Columns** and **Rows** fields will be used for *ArUco detector settings* on **Detector** tab.



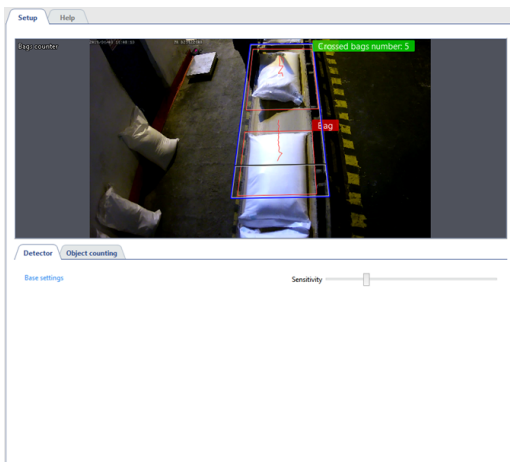
## Neural bags counter

The **Neural bags counter** is intended to build up video surveillance system which require detailed image analysis with the help of neural networks. As a result, the video surveillance operator will receive the information on the bags on the conveyor belt in real time.

To activate the plugin, go to the *Channel settings* to the *Software detectors* area, select the **Bags counter** and then select the **Server**, which will calculate the analytics.

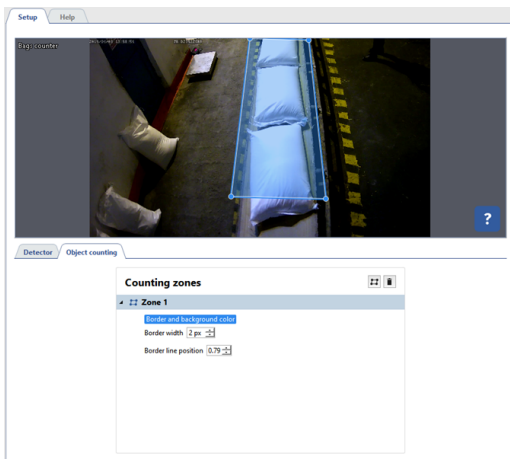


Click **Setup bags counter** to open the detector settings window.



Set the detector **Sensitivity** on the **Detector** tab in the **base settings**.

The **Counting zones** in which the detector will detect and count the bags, moving on the conveyor belt, are created on the **Object counting** tab. The counting zone position should be such so as the **Border line position** was at the end of the movement of the bags on the conveyor belt. To prevent the false detections, the counting zone width should match the conveyor belt width.



- *Motion detector settings*
- *Channel settings*

## Abandoned items neural detector

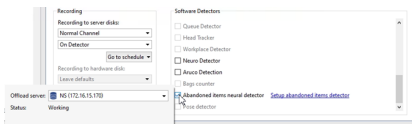
**Abandoned items neural detector** is designed for building complex video surveillance systems which require detailed image analysis with the help of neural networks. As a result of the detector's operation the video surveillance system operator will detect various objects of various sizes left in the camera coverage in realtime, as well as instantly identify left and forgotten objects which can potentially threaten the security of the video surveillance object.



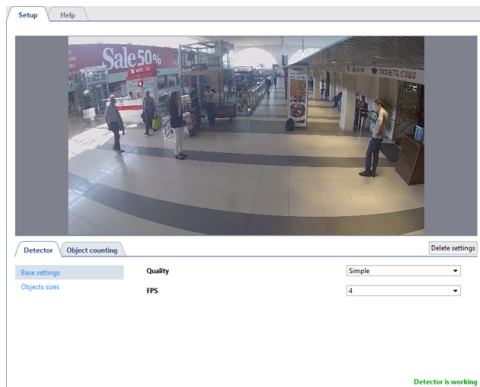
### Abandoned items neural detector specifics:

- This plugin operates on **NeuroStation** video recorders or on any video recorder which has TRASSIR 4 installed and is connected to **NeuroStation** server, which will be used as **Analytics server**. Read more about server connection in [Connecting to a new server](#).
- Check the [Enable remote analytics](#) flag in the user's settings, which will be connected to the analytics server.
- One or more GPUs should have the **Abandoned Items Detector** enabled in the analytics server settings, on the **Analytics** tab. Read more in [Analytics](#).

In order to activate the plugin, open the [Channel settings](#) and in the [software detectors](#) area select the **Abandoned items neural detector** and select the **Server** which will calculate the analytics.



Press the **Setup Abandoned items neural detector** to open the settings window.



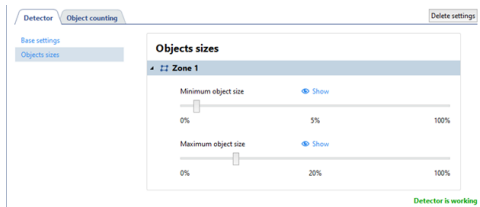
## Detector

The detector's parameters are set up on the **Detector** tab.

- Select the **Quality** of the detector operation in the **base settings**. The higher the quality is, the better the detector will find out the abandoned items. It is recommended to use the advanced quality of the detector operation for complex scenes with a great amount of moving objects. The higher the quality is, the greater is the analytics server load. Use **FPS** parameter to set the amount of frames which will be analyzed for 1 second. The higher is the parameter, the lower is the amount of false detections and the higher is the analytics server load.



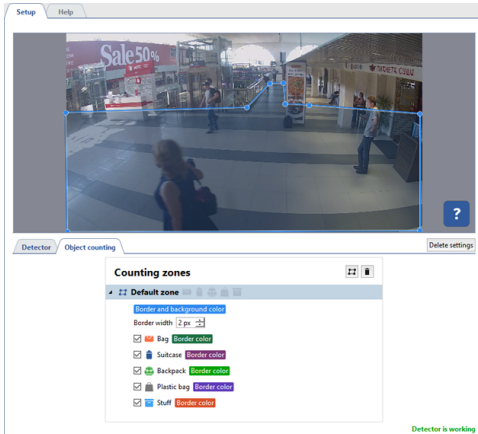
- Create the zones in the **Object size** settings menu. These zones will allow you to select the biggest and the smallest detected object sizes using **Minimal object size** and **Maximum object size** parameters. The object dimensions selection should be based on the detectable object dimensions (boxes, bags, suitcases, etc.).





## Object counting

The **Object count** tab lets you create the zones in which the abandoned objects will be detected. There is already a default zone created which contains the entire image. You can edit its sized by changing the positions of vertices.



To create a new **counting zone** press and set its vertices on the images, starting from the upper right and then in the clockwise direction. In order to finish the zone drawing, place the mouse cursor to the zone starting point and then left-click or press **CTRL+ENTER**.

For each created zone you should select the objects which will be tracked by the detector and highlighted with a frame of corresponding color. In case of the abandoned object detection the **lost owner** signature will appear near the object and the message on lost item detection will *event log*, as well.



In order to track changes in the detector's operation enable displaying **Abandoned object neural detector** figures on channel (see ???).



- [Motion detector settings](#)
- [Channel settings](#)

## Pose detector

**Pose detector** is designed for building complex video surveillance systems which require deep analysis with the help of neural systems. The detector allows to recognize a person's posture based on movement and behavior algorithms. It helps video surveillance system operator follow the nontypical or suspicious people behavior in observation zone in real time, such as falling or raising hands up when attacking. The detector can recognize the following postures of a person:

- sitting;
- in a crouching position;
- laying;
- both hands raised;
- left hand raised;
- right hand raised.

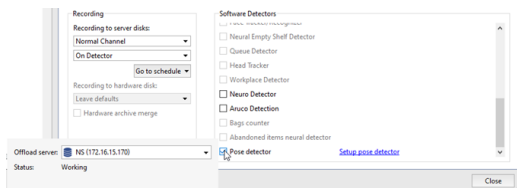
All other postures are classified by the detector as regular.



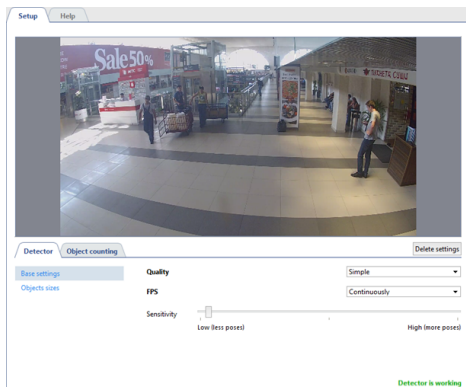
### Pose detector features:

- This plugin operates on **NeuroStation** video recorders or on any video recorder which has TRASSIR 4 installed and is connected to **NeuroStation** server, which will be used as **Analytics server**. Read more about server connection in [Connecting to a new server](#).
- Check the [Enable remote analytics](#) flag in the user's settings, which will be connected to the analytics server.
- One or several GPU should have **Pose detector** operation mode enabled on the **Analytics** tab in the analytics server settings. Read more in [Analytics](#).

In order to activate the module open the [Software detectors](#) area of the [Channel settings](#). Select **Pose detector** and then select the **Server** which will calculate analytics.



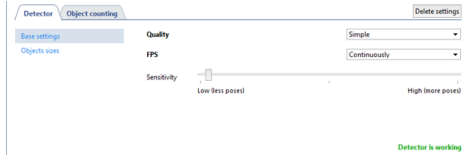
Click the [Setup pose detector](#) link. The settings window will open.



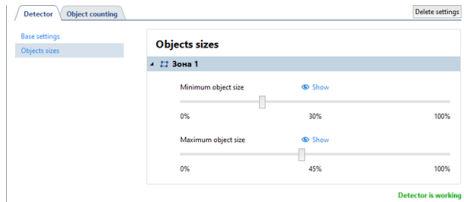
## Detector

The detector's parameters are set up on the **Detector** tab.

- Select the **Quality** of the detector's operation in **base settings**. We recommend using advanced quality for complex scenes with a great amount of moving objects. The higher the quality is the greater is the analytics server load. Use **FPS** parameter to set the amount of frames which will be analyzed for 1 second. The higher is the parameter, the lower is the amount of false detections and the higher is the analytics server load. Set up the **Sensitivity** of the detector. The higher the value is the more sensitive is the detector and there is a greater chance of false positives.

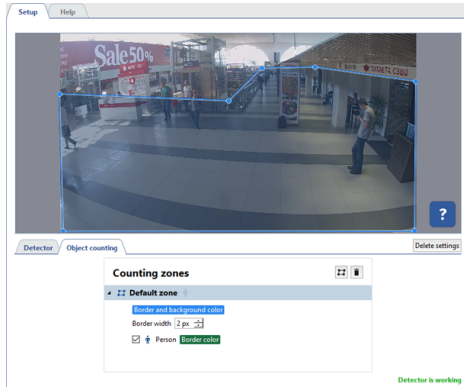


- The **Objects sizes** option lets you create zones in which you should select the biggest and the smallest sizes of a detected object with the help of **Minimal object size** and **Maximum object size** settings. Objects that are smaller than the minimum and larger than the maximum size will not be detected. When choosing sizes, it is necessary to be guided by the height of a person.



## Object counting

Open the **Object counting** tab to create zones in which areas in which people will be searched and their poses analyzed. Outside the detection zones the poses will not be detected. There is already a default zone created in the settings, which occupy the entire image area. You can customize the zone sizes by changing the angles position, if necessary.



To create a new **counting zone** press and set its vertices on the images, starting from the upper right and then in the clockwise direction. In order to finish the zone drawing, place the mouse cursor to the zone starting point and then left-click or press **CTRL+ENTER**.



In order to track changes in the detector's operations enable **Pose detector** display on channel (read more in ???).

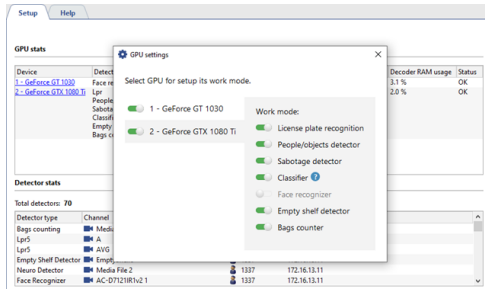


- [Motion detector settings](#)
- [Channel settings](#)

## Analytics

One of the problems experienced when building up complex video surveillance systems, where alongside with the archive record TRASSIR detects various objects (people, faces, etc.), and analyzes their behavior, is the lack of the server computing resources. TRASSIR lets move a significant part of the computing resources which are necessary for detectors and videoanalytics plugins operation to **Analytics server**.

**Analytics Server** - is a server with TRASSIR OS installed, which supports offload-analytics, based on neural networks. Servers where **NeuroStation** or **QuattroStation** version of TRASSIR OS is installed can be used as analytics servers. They use CPU and GPU resources for calculations.



You can enable or disable GPU by clicking the video card name in the **GPU Stats** table.

The **Prefer capability** list defines for which detectors and videoanalytics plugins the selected GPU will be used. The amount of the simultaneously operating detectors depends on the GPU capacity. The higher the capacity is, the more detectors can be simultaneous enabled.

In addition, on the **Analytics** tab you can find the information on the resources used by analytics server.

**GPU Stats** shows the GPU resource load.

Device	Detectors	Load	Decoder count	Decoder load	TF RAM usage	Cuda RAM usage	Decoder RAM usage	Status
1 - GeForce GTX 1080 Ti	Face recognizer	22.1 %	4	7.0 %	0.0 %	0.0 %	3.1 %	OK
2 - GeForce GTX 1080 Ti	Lpr	36.6 %	3	8.0 %	65.3 %	1.1 %	2.0 %	OK

**Detector Stats** shows the list of local and remote channels on which detectors and modules, consuming the analytics server resources, are enabled. Remote user addresses are also displayed.

Detector type	Channel	Remote user	Remote address
Bags counting	Media File 2	1337	172.16.13.11
Lpr	A	1337	172.16.13.153
Lpr	AVG	1337	172.16.13.153
Empty Shelf Detector	EmptyShelf	1337	172.16.13.11
Neuro Detector	Media File 2	1337	172.16.13.11
Face Recognizer	AC-D712181v2.1	1337	172.16.13.11



Specific features of analytics server settings:

- One can connect to an analytics server the same way as to a regular **TRASSIR server**.
- **Remote analytics** should be enabled in the user interface settings, from which the camera servers will be connected to analytics server.
- Some modules require the specific licenses on the analytics server to operate properly. You can find more information in a particular module description.

## Access monitoring control and security and fire alarm systems

TRASSIR allows to arrange integrated security system in which the videosurveillance system interacts with access control systems and security and fire alarm systems. TRASSIR and the connected system can interact both on the same server as well as on different servers connected via the local network.

Operation with the following systems is integrated into TRASSIR:

- **Orion Pro** of *Bolid* company.
- **Hikvision** from *Hikvision Digital Technology Co.,Ltd.*
- **FortNet** of *FortNet Security Systems* company.
- **Gate** of *Ravelin Ltd.* company.
- **Sigur(Sphinx)** of *PromAvtomatika* company.
- **Itrium** of *ITRIUM* company.
- **NeoGuard** of *Insight Software* company.
- **Schrack** of *Schruk Seconet AG* .
- **Spica** of *Spica International* company.
- **Paradox** of *Paradox Distribution Centre* .
- **Stemax** of *NPP Stels*.
- **MaxLogic** from *Mavili Elektronik A.S.*

List of TRASSIR features used for work depends on the connected system:

Feature	Orion Pro	Hikvision	FortNet	Gate	Sigur	Itrium	NeoGuard	Schrack	Spica	Paradox	Stemax	MaxLogic
Automatically load the tree of objects corresponding to the devices in the system.	+	+	+	+	+	+	+		+	+	+	+
<i>Bind system devices to TRASSIR channels.</i>	+	+	+	+	+	+	+	+	+	+	+	+
Locate system devices on TRASSIR maps.	+	+	+	+	+	+	+	+	+	+	+	+
Arrange system devices status monitoring with SMS ( <i>TRASSIR tree of objects</i> ).	+	+	+	+	+	+	+	+	+	+	+	+
<i>Accept system events</i> from systems devices and	+	+	+	+	+	+	+	+	+	+	+	+

Feature	Orion Pro	Hikvision	FortNet	Gate	Sigur	Itrium	NeoGuard	Schrack	Spica	Paradox	Stemax	MaxLogic
conduct search by them.												
To set TRASSIR response using <i>rules and scripts</i> for acquired events.	+	+	+	+	+	+	+	+	+	+	+	+
Manage system objects or to change system objects status from TRASSIR.	+	+	+		+				+	+		



- *TRASSIR settings for operation with Orion Pro access monitoring and control system*
- *TRASSIR settings for operation with Hikvision ACS panels*
- *Typical TRASSIR settings for operation with access monitoring and control system and security and fire alarm system*
- *FortNet ACS server settings features*
- *"Gate" ACS server settings features*
- *Sigur(Sphinx) ACS server settings features*
- *Access monitoring and control system "Itrium" server settings features*
- *Access monitoring and control system NeoGuard server settings features*
- *Specific features of TRASSIR settings for operation with Schrack security and fire alarm system*
- *Specific features of TRASSIR settings for operation with Spica access monitoring and control system server*
- *Specific features of TRASSIR settings for operation with Paradox access monitoring and control system panels*
- *Stemax system server settings features*
- *TRASSIR settings features for operation with "MaxLogic" panels*

## TRASSIR Access Control

**TRASSIR Access Control** is an access control and management system built into TRASSIR, which can:

- determine who, where and when is allowed or not allowed;
- register entrance events and attempts;
- build various types of reports, including time tracking reports.
- *Add persons and assign access levels to them.*

You can find a detailed description of all features in the "Operator's guide" in section [???](#).

**TRASSIR Access Control setup procedure:**

1. *Connect one or several access controllers to TRASSIR. Configure access points and scanners.*
2. *Add access points to the usage area.*
3. *Create one or several access levels and bind the corresponding access points to them.*
4. *Add persons and assign access levels to them.*
5. *Creation of pass request templates.*



You can access **TRASSIR Access Control** settings not only using TRASSIR software, but also via web browser. Read more in [???](#).



You can check the **TRASSIR Access Control** module features in [TRASSIR software demo version](#). **TRASSIR Access Control** in TRASSIR demo version has the following functional limitations:

- 1 access controller;
- 1 access level;
- 5 persons (including visitors for whom the pass requests have been created).



## Devices

This section is dedicated to connection of the Access Control controllers to TRASSIR and their parameters configuration.



Before connecting the controller, learn more about its setup and operation features as part of TRASSIR:

- [Features of Hikvision controllers setup and operation.](#)
- [Features of ZKTeco devices setup and operation.](#)

In order to connect the controller to TRASSIR go to the server settings to the **Plugins** -> **Access Control** -> **Devices**, press **Add Controller** and enter the connection parameters into the opened window.

In case of the controller successful connection to TRASSIR you will see access points on the device connection page. Otherwise, the error message appears.



All persons, created in [TRASSIR Access Control](#), are automatically uploaded to all connected controllers. Use the [Upload persons](#) link to modify data on any particular controller, if necessary.

## Access points settings

The number of access points is determined by the controller technical characteristics. You need to configure them for further user of Access Control in TRASSIR.

To do this, select the access point and configure the following parameters:

- **Name** which will be displayed in the [object tree](#).
- Select the door sensor state in which the door is in the closed position in the **Door open sensor type**.

- Select the button state the same way in the **Door exit button type** field.
- Set the time period within which the door lock will be unlocked in the **Door opening duration** field. The countdown will start immediately after the button pressing or card reading.
- The amount of time in the **Door holding alarm timeout** defines how long the door can be in the open state. In case upon this time expiration the door remains open, it will trigger the alarm event.
- In the **Associated Channels** field, select the video channels to link them to all events that will occur on this access point. When reviewing all occurred events, the video from these channels will be displayed in the **TRASSIR Access Control template** or on the active monitor.

## Card reader settings

There are usually two readers connected to the access point, one of which can be used to provide entrance to the room and the other to exit.

In order to set up the reader, enter its **Name** and select the **Location**. In the **Authentication Mode** setting, select one of the ways by which the person will verify their identity: by card, by card and pin code, by card and face, by fingerprint, etc.



The amount of the authentication modes depends on the functionality of the connected card reader.

If the TRASSIR modules will be used for authentication, enable the corresponding module in the **Authentication by TRASSIR** setting and specify the video channels to be used for authentication in the **Associated channels** field.

Select **AND** in order to enable simultaneous use of **Authentication mode** and **Authentication by Trassir**. Select **OR** to use any of the configured authentication methods.



All modules used for authentication should be enabled and configured. Read more in: **Face recognizer** and **AutoTRASSIR - Automated license plate recognition**.

The built-in into TRASSIR **Persons** base will be used for face recognition. The license plate numbers specified in **personnel settings** will be used for license plate recognition.

The **Additional access conditions** parameter lets you enable the **Temperature control** for persons authenticating with this card reader. In case the employee has a temperature

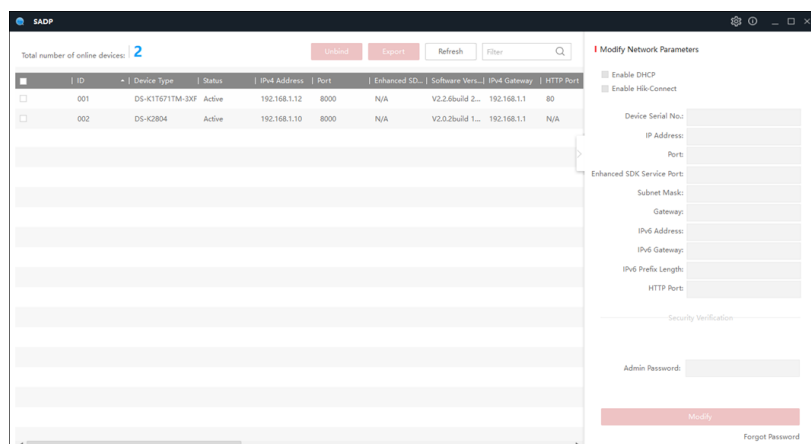
above the value specified in the **Upper threshold** field, the event log will display a corresponding warning and the entry will be blocked for this person.



Select the **Temperature** mode in the **Authentication mode** setting, enable **Temperature control** and set the **Upper threshold** to make the reader operate in the thermometer mode, determining the temperature of people passing by. Other modes of authentication will not be available in this mode.

## Features of Hikvision controllers setup and operation

Before connecting Hikvision controllers to TRASSIR it is required to enable the controller, connect it to the local network and configure network parameters. Use the **SADP** utility to search for the controller in the local network.



Check the controller's user manual for more information on the controller settings.

## Features of Hikvision controllers operation as part of TRASSIR Access Control

- The card numbers read out on Hikvision controllers operating on Wiegand-26 interface, can be used for authentication on ZKTeco devices, and vice versa.
- The Hikvision controllers check the uploaded person photos. If the uploaded photo is not suitable for authentication, you will see a message on the screen.

## Features of ZKTeco devices setup and operation

Before connecting ZKTeco device to TRASSIR, you need to switch it on, connect to your local network, and configure network settings parameters. To do this, open **COMM.** -> **Cloud Server Setting** in the device menu and set the following values:

- **Server address** - TRASSIR server IP address, to which the device will be connected;
- **Port** - the default value is **8899**;
- **HTTPS** - **enabled**.

After that, open the **System settings** and set the following value:

- **Device Type Setting** - **Access Control Terminal**.



In order to increase Access Control security, it is recommended to create a new user with the administrator privileges and use it to connect to TRASSIR Access Control.

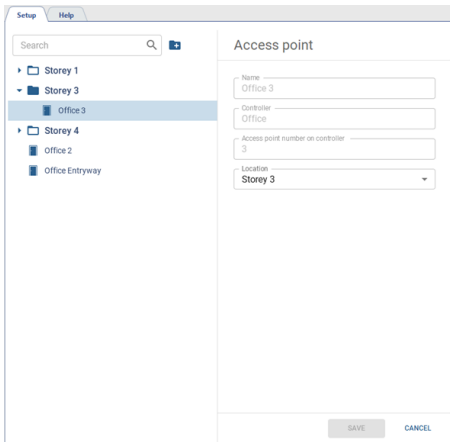
#### Features of ZKTeco devices operation as part of TRASSIR Access Control


- TRASSIR Access Control does not support some authentication modes (by palm, finger veins or QR code), available on ZKTeco terminals. You can see the list of all supported modes in the [reader settings](#), after connecting the device.
- The card numbers, read out on ZKTeco terminals, can be used for authentication on Hikvision terminals, operating on Wiegand-26 interface, and vice versa.
- The fingerprints read on other manufacturers' devices are not supported on ZKTeco terminals. If you use other manufacturers' access control devices, each device must be uploaded with "own" fingerprints.
- ZKTeco devices do not check uploaded person photos.

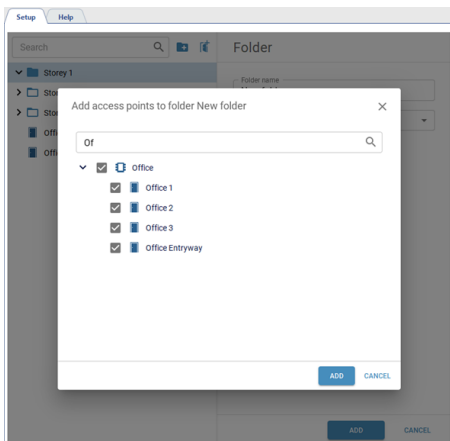
## Areas of use

Open the **Plugins** -> **Access Control** -> **Areas** section to set up the zones.

All **access points** appear in the **Areas** section automatically. You can also group them into folders for your convenience. To do this, create the required folders amount and select **Location** in the access point settings.



In order to add several access points to a single folder, select the folder in the object tree and press  and then in the opened menu, select the access points that should be in this folder.



## Personnel



At least one **access level** should be created for operation with TRASSIR Access Control persons.

This section allows you to create and edit Access Control persons, as well as assign the appropriate access levels to them. All Access Control persons are stored in the **person database**. Be careful when editing or deleting persons, as they may be used by other TRASSIR modules (for example, by **Face Recognizer**).

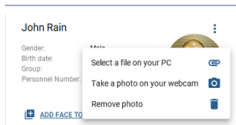
Open **Plugins->Access Control->Personnel**.

Press **Add** to create a new Access Control person.

And follow the steps below:

1. Enter the employee's **Name**. Specify **Gender**, **Birth date**, **Group**, **Personnel number** and other person's data, if necessary.

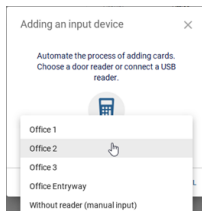
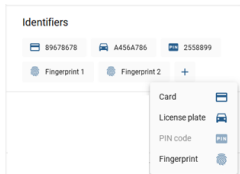
2. Press **Select a file on your PC** or **Take a photo on your webcam** to upload the employee's photo.



In order to use a face for authentication in *Face Recognizer*, click the **Add face to face DB** link. If the controller that can recognize faces has been added to Access Control, the face photo will be automatically uploaded to the controller.

Press **Remove photo** to remove all person's photos, including previously uploaded ones.

3. in order to manage an employee's working hours, select **Work schedule**.  
Use various settings to create any work schedule (read more in *Schedule settings*).
4. Add identifiers that will be used by the employees to authenticate in Access Control.



**Card** - select identity card data input type and enter:

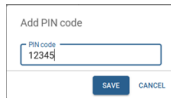
- using USB reader connected to TRASSIR client/server;
- using the reader installed at the access point;
- by entering the card data into the input field manually.



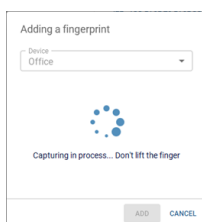
Data input from an ID card using a USB reader is only supported in **TRASSIR for Windows**.



**License plate** - enter the vehicle license plate number that will be used for *AutoTRASSIR* module authentication.



**PIN-code** - enter the pin code that will be entered by the employee on the controller panel.

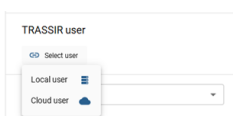


**Fingerprint** - select the fingerprint scanner and attach your finger to the sensor.



All identifiers will be used for Access Control authentication, depending on the **Authentication mode** selected in the *controller's settings*.

5. Enter local or cloud user account to allow this person using *WEB interface* or *mobile application* to operate with TRASSIR Access Control.





The access rights to the TRASSIR Access Control module are set depending on the user type:

- local users - in server settings (check [Determining access rights](#));
- cloud users - in TRASSIR Cloud settings (check [???](#)).

6. Assign the corresponding **Access level** to the person. Only one level can be assigned.



In case you need to add a large number of persons, you can use the **Import Persons** feature. To do this, go to **Automation** section, click **Create New Script**, select **Load example... -> pacs\_import** in script editor menu and click **Save and Run**.

Press **Parameters** in order to check the script guidelines and configure the script parameters.

Read more about the usage of the scripts in [Integrated script editor](#).



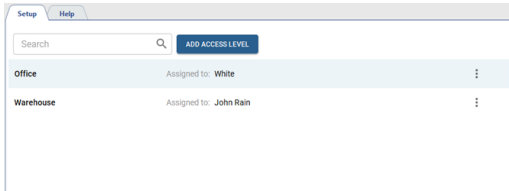
## Person access levels



At least one access level should be created for operation with TRASSIR Access control.

Open the **Plugins** -> **Access Control** -> **Access Levels** section to set up access levels.

With the help of access levels, you can allow people to access the entire area or only certain rooms. The settings page shows all created access levels and the persons to whom they are assigned to.



Press **Add access level** to create a new access level. Select an access level and **Edit** to edit the existing one.

In the opened window, enter the name and add access points that will be allowed to be used by the persons with this access level. Add groups of people or individuals to whom this access level will be assigned to.

Press **Setup Schedule** to choose days and time when this access level will be allowed to use. Use various settings to create any access schedule you want (read more in [Schedule settings](#)).

## Schedule settings

TRASSIR Access Control has a built-in flexible scheduling system that is used for:

- in the [person's settings](#) to specify employee's business hours by building [reports](#);
- selecting the time when this level of access will be allowed to use in the [access level settings](#).

You can create two schedule types in TRASSIR Access Control: **Calendar Week** and **Shifts**.

Follow the next steps to create a **Calendar Week** schedule type:


1. Use **Working day** / **Day off** flags to specify working days and days off.
2. Select one of the working days and use sliders or **Beginning** and **End** fields to set up the working day start and end time and add one or several breaks, if necessary.
3. In order to copy the created schedule to the other workdays, click **Duplicate to all work shifts**.

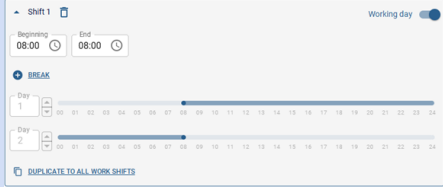
i

Use the **Holidays** tab to add the dates when another work schedule or access schedule will be in effect, depending on the created schedule purpose, e.g. on pre-holidays or holidays.

Follow the next steps to create a **Shifts** schedule type:

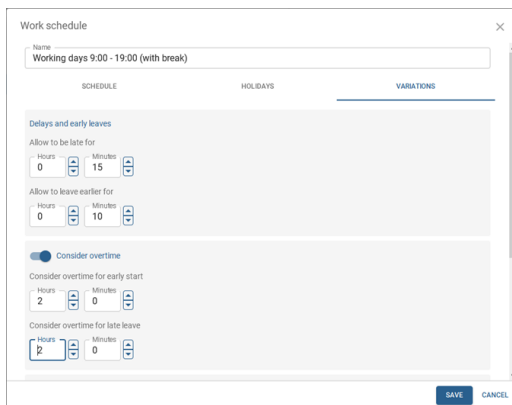
1. Set the first shift start date and create the required number of working and weekend shifts.
2. Select one of the working shifts and use sliders or **Beginning** and **End** fields to set up the shift start and end time and add one or several breaks, if necessary.

 In order to create a shift that starts at one day and ends at another, in the **End** field choose the time that is less than or equal to the time specified in the **Beginning** field.



3. In order to copy the created schedule to the other shifts, click **Duplicate for all work shifts**.

The **Variations** tab contains the parameters which you can use to create more flexible work schedules for your employees.



- The **Delays and early leaves** parameter determines the maximum time intervals that will be used to calculate late arrivals and early leavings. If an employee comes in late or leaves earlier than the specified time period, the difference between the actual time and the scheduled time will be reported as **Being late** or **Early leave**.
- The **Consider overtime** parameter sets the minimal time which will be used for overtime calculations. If an employee comes in earlier or leaves later than the specified time period, the time worked by the employee will be displayed as **Overtime** in the reports.
- The **Allow work on weekends** set the minimal time which will be used for overtime calculations for weekend work. If an employee works more than the specified time on a day off, the actual time worked will be displayed as **Overtime** in the report.
- The **Work area leaving** parameter sets the minimal time for which an employee can leave his/her workplace. If the employee will be absent longer than the specified period, this absence time will be displayed in the reports as **Absenteeism**.



Features of schedules created for access level settings:

- the **Variations** setting is absent;
- the schedule may not include more than 3 working intervals per day;
- the **Calendar Week** schedule is activated immediately upon saving.

## Visitor templates

This section allows you to create or edit visitor templates. The **Visitor templates** are the special TRASSIR Access Control forms, using which a person can create requests for temporary visitor pass issue.

In order to access the section, go to **Plugins -> Access Control -> Visitor templates**.

Press **Add** to create a new template for visitors and follow the next steps:

1. Enter the **Name** of a new template.

2. Select a person or a group of persons who will have access to the option of creating pass requests.

3. Choose one of the ways of **Pass issue**:

- To activate the pass immediately after creating a request, set the **Automatic pass issue** flag.
- If you want a special person to activate and issue passes (for example, a guard at the gate or the head of security), then select those who will confirm visit requests and issue passes in the **Users allowed to issue passes** list.

4. Select and set up one or more identifier types (**Card** or **License plate number**) that the visitors will use for authentication.

Specify the number of days and hours during which the pass will be valid in the ID type settings.



The start of the pass validity time depends on the selected method in the **Pass issue** setting:

- If **Automatic pass issue** is selected, then the pass time countdown starts from the moment the pass request is created.
- If a list of persons issuing passes is selected, the countdown of the validity time starts from the moment of confirmation and issuing of the pass by this person.

When the pass expires, it is archived. The storage time of passes in the archive is determined by the TRASSIR database settings. All archived passes with the date of issue older than **The record retention period** will be deleted (see section **Database connection settings**).



The **Card** identifier type can't be used with **Automatic card issue** as for issuing a pass with the card, you need to enter the number of the card to be issued. Read more in **???**.

5. Select the **Access Level** that will be granted to a visitor who is given a temporary visitor pass.



The process of the request creation is described in the "Operator's Guide" (in section **???**)

## TRASSIR settings for operation with Orion Pro access monitoring and control system



TRASSIR software works with Orion Kernel 1.11 (release 2, build 1713) and Cloud 1.11 (release 2, build 949) and newer. If you are using older versions, you must update your Orion Pro software.

In the **Settings window**, the settings for connecting to an Orion server are specified on the **Modules -> Orion** tab.



**For Windows.** Before setting up the connection to the "Orion Pro" server, an **ODBC source driver** should be installed and configured, if necessary. You can read about the configuration procedure in [Connecting the data source \(ODBC\)](#).

**For TRASSIR OS.** The driver installation and configuration is not required.

- **Protocol** - protocol of connection to the "Orion Pro" access control system server.
- **Address** - IP-address or DNS-name of Orion Pro access monitoring and control system server.
- **Port** - Orion Pro access monitoring and control system server port number.
- **User name** and **Password** - account name and password on Orion Pro access monitoring and control system server (by default: **ADMINISTRATOR** and **ORION**).



Please note that the **Username** and **Password** are case sensitive!

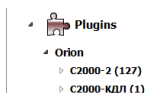
Error "**Not enough rights (error 112)**", in most cases indicates the incorrect user name or password in Orion Pro access monitoring and control system server.

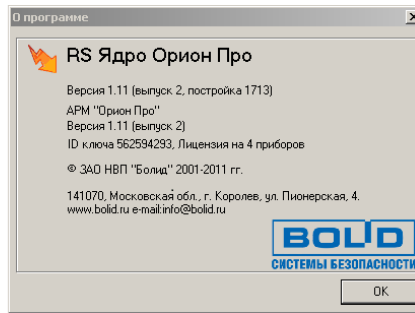
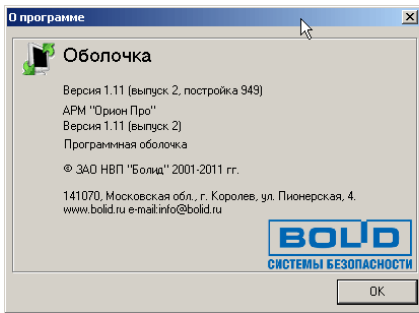
- **This server address** - IP-address or DNS-name of the current TRASSIR server for feed back to Orion Pro server.
- **Feed back port** - port number of the current machine for feed back to Orion Pro server.
- **ODBC Data Source** is a full database name, that can be found in the Orion server settings on the "Central server Orion: Database".
- **ODBC user** and **ODBC password** are user name and password to connect to Orion Pro access monitoring and control system data base.



By default Orion Pro access monitoring and control system creates user **sa** and the password **123456**. In these credentials are invalid, we recommend to contact the company which has installed Orion Pro access monitoring and control system.

The **Status** field indicates the connection state. If all the parameters are set properly, an **Orion connected** entry is displayed and the new FACS "Orion Pro" objects appear in the TRASSIR object tree.





System objects settings is described in the *AMCS or security and fire alarm system objects settings tree*.

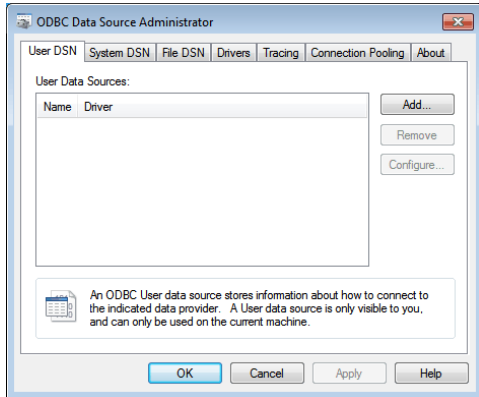
## Connecting a data source (ODBC)



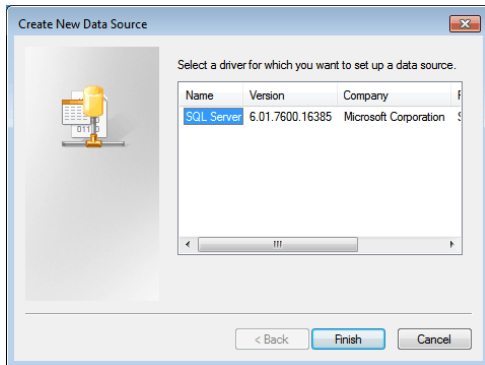
This instruction is for servers with Windows OS.

If you use **TRASSIR OS**, skip it and go to [connection to Orion Pro server](#) settings.

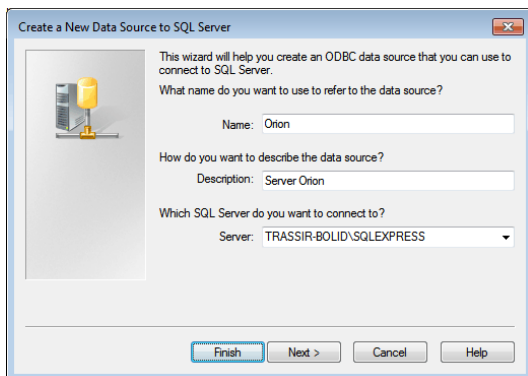
1. Run `sqlnativeclient.msi` - This is an ODBC driver for SQL Server 2005. You can download it from the Microsoft website.
2. Run **ODBC Data Sources Administrator** (Start -> Administration -> Data sources (ODBC)). Create new data source. To do this, click on **Add**.



3. **New data source creation** window will open. Select SQL-server in the list and click **Done**.

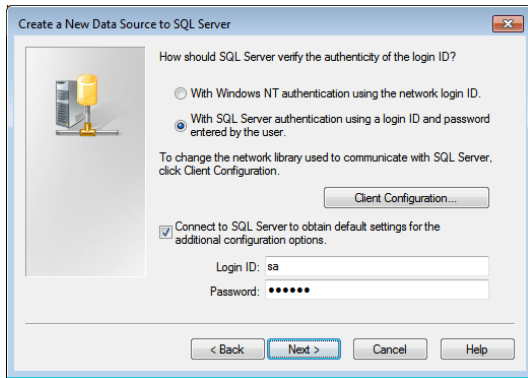


4. Give the data source a name and description (any values). Click the arrow on the server selection combobox and wait for the list of servers to load. Then select the Orion database server.

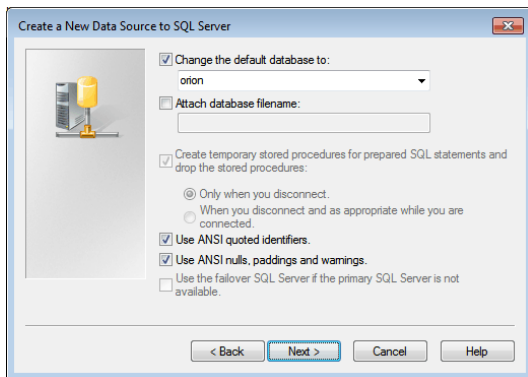


5. Click **SQL Server account verification** item, enter user and password specified under Orion data base installation/settings.

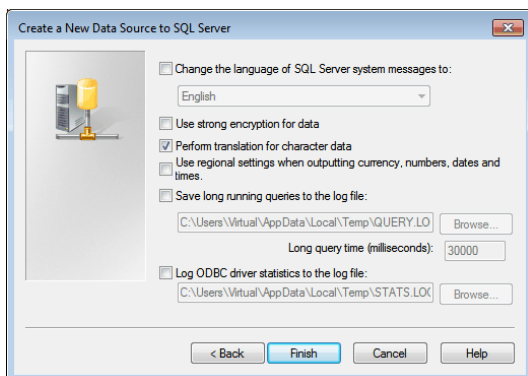




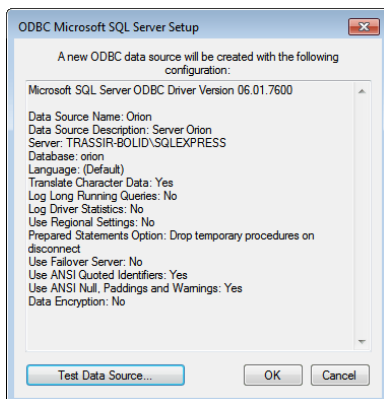
6. Check **Default database** box and check data base specified in Orion server settings in combobox.



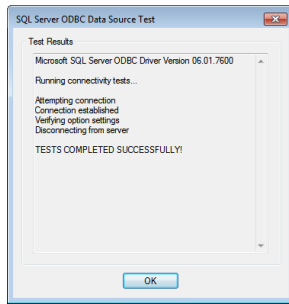
7. Click **Done**.



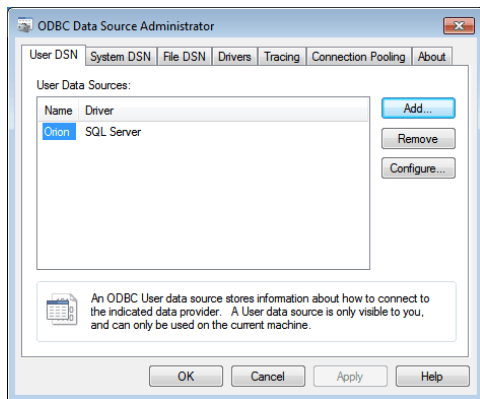
8. When the next window will appear, click **Verify data source**.



9. After that the verification window will open, on verification completion status **Test completed successfully** shall appear.

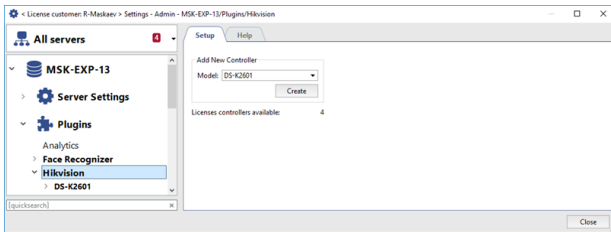


10. Upon completion, the new server should appear in the list of sources.



## TRASSIR settings for operation with Hikvision ACS panels

Select the panel model, to which TRASSIR will be connected, in the **Settings window**, on the **Plugins -> Hikvision** tab.



The maximal amount of the panels that can be connected to TRASSIR is defined by the licence and displayed in the **Available licences** field.

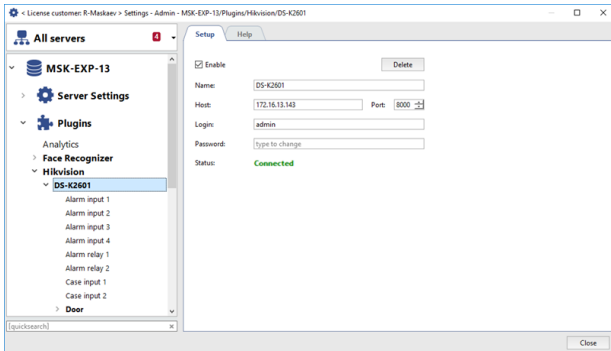
Select the connected controller model and press **Create**. The created controller will appear in the TRASSIR settings tree. After that you should set up **TRASSIR connection to the panel**.



- **Connecting TRASSIR to Hikvision ACS panel**
- **AMCS or security and fire alarm system objects settings tree**

## Connecting TRASSIR to Hikvision ACS panel

In order for TRASSIR to start working with the *previously created* Hikvision ACS Panel, the following parameters should be setup:



- **Name** - name, displayed in the settings tree.
- **Address** - IP address or DNS name of the connected controller.
- **Port** - controller connection port.
- **User Name** and **Password** - controller user account credentials.

Set the **Enable** flag. After that the **Status** field will display the connection state. If all parameters are set properly, the **FACS Connected** and the objects of the connected control panel will be added to TRASSIR object tree.

Read more about control panel object settings in the *AMCS or security and fire alarm system objects settings tree*.

## Typical TRASSIR settings for operation with access monitoring and control system and security and fire alarm system



Before connection setup get aware of the specific features of the corresponding system:

- *FortNet ACS server settings features*
- *"Gate" ACS server settings features*
- *Sigur(Sphinx) ACS server settings features*
- *Access monitoring and control system "Itrium" server settings features*
- *Access monitoring and control system NeoGuard server settings features*
- *Specific features of TRASSIR settings for operation with Schrack security and fire alarm system*
- *Specific features of TRASSIR settings for operation with Spica access monitoring and control system server*
- *Specific features of TRASSIR settings for operation with Paradox access monitoring and control system panels*
- *Stemax system server settings features*
- *TRASSIR settings features for operation with "MaxLogic" panels*

To connect TRASSIR to the system select in the **Settings window** the name of the module corresponding to the system being connected and set the following parameters:

- **Name** - name of the module displayed in the settings tree.
- **Address** - system server IP-address or DNS-name.
- **Port** - connection to the system port.
- **User name** and **Password** - account data on the systems server.

Set the **Enable** flag. After that in the **Status** field the connection state will appear. In case all parameters are entered properly, the **FACS Connected** message will appear and the connected system objects will be added to TRASSIR object tree.



While working with Gate ACS the objects will appear after the *controller creation*.  
While working with Schrack security and alarm system the object will appear after the *configuration file loading*.

System objects settings is described in the *AMCS or security and fire alarm system objects settings tree*.

## FortNet ACS server settings features



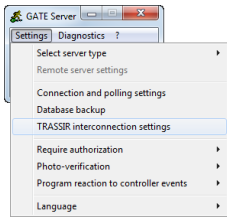
Modify the configuration file before connecting TRASSIR to FortNet access monitoring and control system server `fortnet.ini` server. The following block should be added to the end of the file:

```
[HTTPService]
Active=1
Port=8080
```

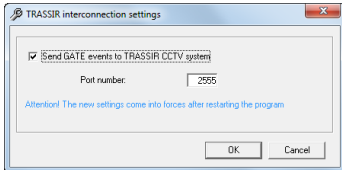
You can specify a different value for the network port. Make sure the port is not being used by third-party software.

## "Gate" ACS server settings features

Before connecting TRASSIR to ACS it is necessary to set events transfer from Gate server objects to TRASSIR. To do this go to Gate server settings **Settings** -> **TRASSIR transmission settings**



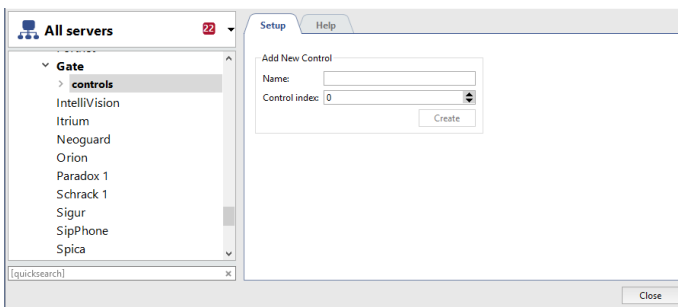
Check **Send events to TRASSIR** box and specify **Communication port number** with which data transfer from Gate ACS to TRASSIR will be done.



Restart the server to apply settings. Click **TRASSIR to ACS connection settings**.

## "Gate" ACS controller creation

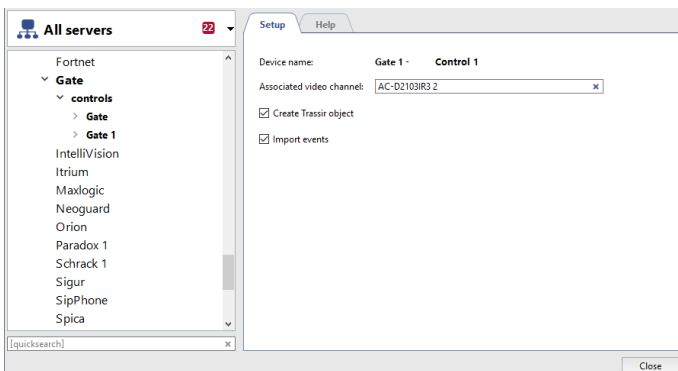
TRASSIR is connected to Gate ACS via controller. For creation, open the **Plugins** -> **Gate** -> **Controllers** tab.



Add a new controller by specifying the following parameters:

- **Name** - controller name displayed in the settings tree.
- **Control index** - The controller's address configured in the Gate ACS.

ACS objects will be created automatically after the controller creation.



See description of the settings in **AMCS or security and fire alarm system objects settings tree**.

## Sigur(Sphinx) ACS server settings features



TRASSIR supports "Sphynx" software, version 1.0.54.44.s or higher and controllers with 28 or higher software version.

When using "Sigur" Access Control with "Face Recognizer" module, the "Sigur" software should be updated to 1.1.0.24.s or higher.



## Access monitoring and control system NeoGuard server settings features

**NeoGuard** is a dispatching and monitoring software provided for optimal management of the data received from monitoring stations along with such data processing and transmission to dispatchers and response teams.



TRASSIR connection to NeoGuard system is possible only after server system preset.  
To receive appropriate instructions refer the technical support service of [Insight Software](#) company.

## Access monitoring and control system "Itrium" server settings features

To connect TRASSIR to Itrium AMCS server you need **Client DNO**, which can be downloaded at [trassir.com](http://trassir.com). Proceed as follows:

1. Unzip archive content on PC where Client DNO will be started.  
Client DNO can be started at any PC being in the same local network with TRASSIR and Itrium AMCS servers. We advise to run it at the same PC where AMCS server is installed.
2. Install "OpenOPC Gateway Service". To do this, run **OpenOPC-1.3.1.win32-py2.7.exe** from archive.
3. Start **Client DNO** with the following parameters:

```
OpcClient.exe 15234 localhost 7766 C:\OpenOPC\bin
```

whereas:

- **15234** - port via which TRASSIR will connect to Client's security and fire alarm system. Same value shall be specified in [system connection settings](#).
- **localhost** - IP-address or DNS-name of PC on which "OpenOPC Gateway Service" is running.
- **7766** - Itrium AMCS server port (set in AMSC).
- **C:\OpenOPC\bin** - path to exe files of "OpenOPC Gateway Service" (to be selected during service installation process).



Client DNO should be started under that has user administrator rights.  
Any amount of TRASSIR servers can be connected to a single DNO Client.

After that you can go to [TRASSIR to AMCS connection settings](#).

## Specific features of TRASSIR settings for operation with Schrack security and fire alarm system

TRASSIR supports operation with all Schrack security and alarm systems operating with ISP protocol.

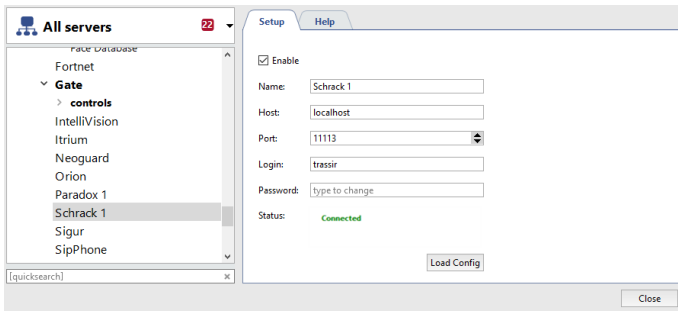


Schrack does not support automatic loading of the system objects.

To get objects in TRASSIR it is necessary to load configuration file with the connected object settings. You can get information on configuration files creation at "[Schrack Seconet AG](#)" company technical support.

Configuration file is downloaded immediately following TRASSIR connection to Schrack security and fire alarm system.

To do that click **Download configuration** and select the file to download. After the download, security and fire alarm system objects will appear in TRASSIR server objects tree.

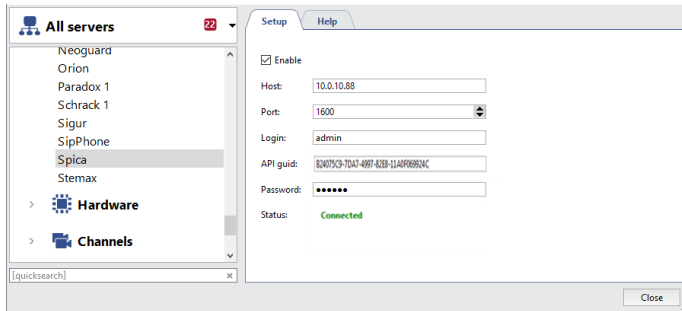


## Specific features of TRASSIR settings for operation with Spica access monitoring and control system server



TRASSIR supports operation with Spica software of 10.00.B. and newer versions.

During TRASSIR to Spica AMCS server connection it is necessary to enter **API identifier**. It can be received from *Spica International* company technical support service.



## Specific features of TRASSIR settings for operation with Paradox access monitoring and control system panels



TRASSIR supports operation with the following control AMCS control panels:

- SP4000
- SP5500
- SP6000
- SP7000
- MG5000
- MG5050
- EVO192
- EVOHD

To connect to TRASSIR server of Paradox system, you need the **Paradox-Trassir-client** which can be downloaded from [trassir.com](http://trassir.com). Then do the following:

1. Unzip the application archive on a PC used for launching the application.  
**Paradox-Trassir-client** can run at any PC with Windows OS being in the same local network with TRASSIR servers and Paradox system control panels.
2. In the configuration file `connection.ini` specify client connection parameters to Paradox system control panel and TRASSIR server.

```
#Paradox-Trassir client utility ini file
#Connection settings to Paradox server:

#Panel 1
host 192.168.1.69
port 10000
panel_id 1
login 1234
password paradox

#Panel 2
host 192.168.1.68
port 10000
panel_id 2
login 1234
password paradox

#Local settings:
local_port 10050
#local port should be specified at Trassir when connects to Paradox
```

whereas:

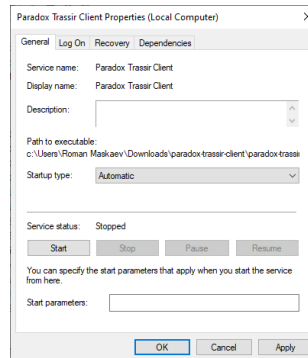
- **host** - control panel IP-address
- **port** - connection port.
- **panel\_id** - number of the panel to be used by TRASSIR for its identification.
- **login** and **password** - code of user and password which will be used to connect the Client to control panel.
- **local\_port** is the port via which TRASSIR will connect to "Paradox Trassir Client". Same value shall be specified in [system connection settings](#).

3. Install Paradox Trassir Client service on your PC. To do this, press **paradox-trassir-client-vc120.exe install**.



The user should have admin rights.

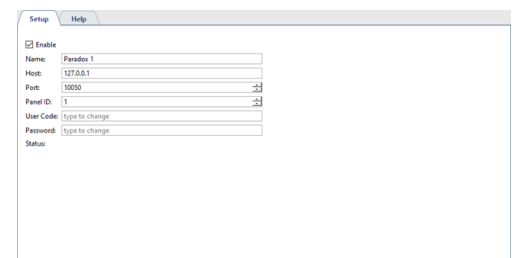
4. For automatic start of the service, change **Run type** in its settings.



Now you can move to *to adjust TRASSIR connections for Paradox system client*.



One PC with Paradox Trassir Client system installed may be connected to multiple TRASSIR servers.



The following parameters should be specified in TRASSIR connection to "Paradox Trassir Client" settings:

- **Address** - IP-address or DNS-name of PC where "Paradox Trassir Client" has been started.
- **Port** - port of connection to "Paradox Trassir Client" specified in configuration file `connection.ini`.
- **Panel ID** - identification number of the panel to which TRASSIR is connected as specified in the configuration file `connection.ini`.
- **User code** - identification code of user set on connected panel and specified in configuration file `connection.ini`.
- **Password** - password corresponding to identification code of user.

## Stemax system server settings features

In order to connect TRASSIR to Stemax system server you need **Stemax-Trassir-client**, which can be downloaded at [trassir.com](http://trassir.com). Then do the following:

1. Unzip the application archive on a PC used for launching the application.  
**Paradox-Trassir-client** can run at any PC with Windows OS being in the same local network with TRASSIR servers and Paradox system control panels.
2. In the configuration file `connection.ini` specify client connection parameters to Stemax system server and TRASSIR server.

```
#Stemax-Trassir client utility ini file
#Connection settings to Stemax server:
host    localhost
port    5000
login   admin
password admin

#Local settings:
local_port 5050
#- this port should be specified at Trassir when connects to Stemax
```

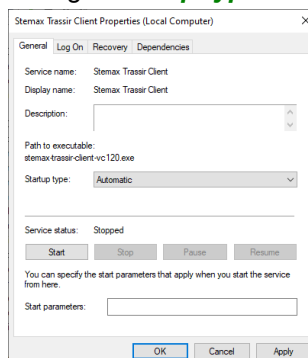
whereas:

- **host** - IP-address or DNS-name of PC where Stemax system server has been started.
  - **port** - Stemax system server port (is set in the server).
  - **login** and **password** - user name and password which will be used to connect client to Stemax system server (are set in server).
  - **local\_port** is the port via which TRASSIR will connect to "Stemax Trassir Client" service. Same value shall be specified in the [system connection settings](#).
3. Install "Stemax Trassir Client" service to your PC. To do this run **stemax-trassir-client-vc120.exe**.



The user should have administrator's rights.

4. To enable automatic startup of the service, change **Startup type** in its settings.



Proceed to [TRASSIR connection settings to Stemax system Client](#).



Any number of TRASSIR servers can be connected to a single PC with "Stemax Trassir Client".

## TRASSIR settings features for operation with "MaxLogic" panels



TRASSIR supports the following panels:

- ML-1207.MX
- MLY-1219.MX

**ModbusServer** is required to connect TRASSIR to the "MaxLogic" panels. You can download it [trassir.com](http://trassir.com). After that do the following:

1. Unzip the archive content to the PC on which the app will be started.  
**ModbusServer** should run on Windows PC to which MaxLogic is connected.

2. Run ModbusServer with the following parameters setup:

```
ModbusServer.exe 15234 COM3 19200
```

where:

- **15234** - is the port through which TRASSIR will connect to "ModbusServer. The same value should be set in [System connection setup](#).
- **COM3** - is a serial port, to which the panel is connected.
- **19200** - is the connection speed of the serial port.

After that proceed to [TRASSIR to "ModbusServer" connection setup](#).

The screenshot shows the 'Setup' window of the TRASSIR application. It has two tabs: 'Setup' and 'Help'. The 'Setup' tab is active. Inside the window, there is a section for connection settings. A checkbox labeled 'Enable' is checked. Below it, there are input fields for 'Name' (containing 'Maxlogic'), 'Host' (containing '127.0.0.1'), 'Port' (containing '5050'), 'Login' (empty), and 'Password' (containing 'type to change'). At the bottom, the 'Status' is displayed as 'Connected' in green text.

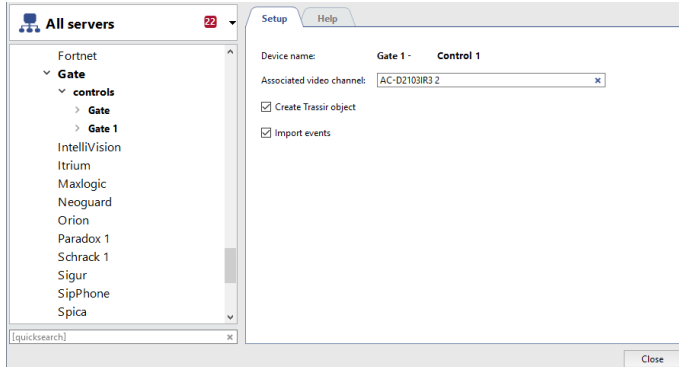
Enter the following parameters in the TRASSIR to "ModbusServer" connection settings:

- **Address** - IP address or PC DNS name where "ModbusServer.exe is run.
- **Port** - "ModbusServer.exe" connection port, which is specified in the app startup parameters.
- **User name** and **Password** - these fields can be left unchanged.



## AMCS or security and fire alarm system objects settings tree

After connection setup to the system server all the objects corresponding to connected system objects will be created in TRASSIR. If necessary, select only those objects required for integration with videosurveillance system. All objects of connected system need to be bound to corresponding channels.



To do this set the following parameters in each system's object settings window:

- **Device name** - The name of the device received from system server. To change device name it is necessary to rename corresponding object on the system server.
- **Associated channel** is a video channel connected with given object. Single channel can be bound to the several objects. For example if several readers for access control are installed on the door to the corridor, all of them can be bound to the same camera.
- **Create objects** is the box establishing the necessity to create an object in TRASSIR for the given device. The box is checked by system for all the objects as default setting. In case such a device is not used in videosurveillance system this box shall be unchecked. It will allow to refrain from unnecessary objects creation and enhance substantially your work with server.
- **Import events** is the box establishing the necessity to import events of the given device from AMCS. System checks this box by default for all the objects.



This section describes the procedure of connection to AMCS or security and fire alarm system. Principles of operation with the objects and events of the systems are described in "Operator's Guide".