



ADMINISTRATOR'S GUIDE



Table of Contents

Customer support	6
Basic information	8
Scope and feature summary	9
System requirements	18
Video server	19
Selecting the number of disks for an archive	20
Compatible operating systems	21
Compatible IP equipment	22
Installation	23
Installing compression cards	24
IP video recorder installation	25
IP video recorder network settings	26
NAS Setup	29
Configuring a QNAP Turbo NAS	30
Connecting a network storage in a Windows OS	35
Installing Guardant USB keys	38
Windows OS settings	39
Installation of the software server version	40
Installation of the software client version	44
Installation and uninstallation of the software server version in Astra Linux SE 1.7	47
PostgreSQL DBMS installation	52
Configuring the operating system to work with the PostgreSQL DBMS	56
Starting the PostgreSQL Database Server service	58
Moving a PostgreSQL database to a different server	61
Allowing external connections to the PostgreSQL DBMS	65
Connecting analog PTZ cameras	67
Configuration of the software server version in Astra Linux SE 1.7 for operation with neural network detectors	69
Working with the basic interface	71
Start the software and sign into the system	72
First server launch	73
Watchdog	74
System login	75
Main control panel	77
Settings window	79
Video monitor	80
Settings	81
Local server settings	82
Remote server settings	85
Client settings	86
License	87
EULA	89
Software update	90
Logs and dumps	91
Cloud	92
Connecting server to TRASSIR Cloud	93
Starting the MC service on Windows	95
Client connection to TRASSIR Cloud	97
Cloud cameras	99
Archive	100
Archive setup on the server	101
Archive setup on the client	104
Encrypting an archive	106
Creating and setting up RAID for archive record	108
Configuring a network storage connection in Linux-based TRASSIR OS	113

Recording network channels	115
Archive merge	116
Configuration of the archive merge session on the source server	119
Reviewing the archive merge session on the destination server	121
Screenshot management	122
Web server (SDK)	123
Configuring a server to work with the SDK	124
Access to TRASSIR WEB interface	126
Map	128
Creating a map	129
Adding objects to the map	131
Adding teleports	135
Reports	137
Report template settings	138
Database connection settings	139
Date and time	141
Network interfaces	142
Persons	144
Users	147
Adding users and user groups	149
Determining access rights	150
Determining access rights for a group	153
Per object rights	154
Examples of user rights settings	155
Audit	156
Watermark	158
Devices	159
IP devices	160
Adding IP devices manually	162
Adding IP devices that use the ONVIF protocol	164
Adding IP devices using RTSP	166
Adding video files	167
Image dewarp into several channels	168
Boards	170
Configuring device settings	171
Serial port settings	177
Remote Controls Settings	179
Channels	180
Channel settings	182
Channel recording settings	186
Video capturing parameters	188
Black zones	189
Watermarks	190
Changing image rotation and aspect ratio	191
Audio channel settings	192
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 when connecting to servers with version 3.2	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	236
Rules	237
Schedules	240
Adding an email account	242
Template loop	243
Examples of the rules and scripts	244
Plugins	261
ActiveDome - Automated PTZ-camera control	262
ActiveDome's manual and automatic operating modes	263
Creating an ActiveDome scene	264
Comparison of overview cameras and PTZ cameras	265
ActivePOS - Point-of-sale operations monitoring	267
ActivePOS features	268
Trading systems and equipment compatible with ActivePOS	269
ActivePOS incidents and detectors	271
Personal incidents and detectors creation	273
Configuring POS terminals	275
Configuring R-Keeper POS terminals	278
DSSL XML for ActivePOS	281
DSSL XML for trade objects	284
DSSL XML for hospitality business and public catering objects	290
DSSL XML for banknote counters and sorters	296
DSSL XML for warehouses	297
DSSL XML for gas stations	299
IP-video intercom	306
Connection to Asterisk server	307
SipPhone server settings	309
SipPhone on the client settings	310
AutoTRASSIR/AutoPass - Automated license plate recognition	311
Selecting, installing, and configuring cameras to work with the AutoTRASSIR/AutoPass module	313
AutoTRASSIR/AutoPass general settings	316
Setup AutoTRASSIR module on a channel	320
AutoTRASSIR (LPR5) setup	321
AutoTRASSIR settings (LPR3)	325
AutoTRASSIR settings (LPR1)	327
Setup HSC AutoPass module on a channel	331
Maintaining internal lists of license plate numbers	333
Connecting external lists of license plate numbers from a text file	336
Creating an external ODBC data source for AutoTRASSIR	338
Connecting external lists of license plate numbers on Windows	341
Connection of the external number lists in TRASSIR OS	343
Creating an AutoTRASSIR/AutoPass template	345
SIMT software-based detector	347
SIMT detector settings	348
ActiveSearch - find motion	351
Floor mapping settings	352
Slow Down Detector	356
Common Slow Down detector settings	357
Configuration of the Advanced Slow Down detector	358
Face recognizer	360

Face recognizer basic settings	364
Face recognizer settings for the channel	369
Face recognizer 2.0 settings for the channel	371
Face database	374
Neural Empty Shelf Detector	378
Empty Shelf Detector	381
Queue detector and workplace detector	382
"Queue detector" module settings	383
Workplace detector module settings	385
Head Tracker	387
"Head Tracker" module settings	388
Neuro Detector	390
Neuro Detector settings	392
Selection of the neural detector version and creation of classes	397
ArUco Detector	399
ArUco Detection	400
ArUco Marker generator	403
Bags counter	404
Abandoned items neural detector	405
Pose detector	408
Camera image quality indicator CiQi	411
Analytics	413
TRASSIR ACS	414
Devices	415
Connection of controller	416
Access points settings	421
Card reader settings	423
GPIO settings	426
Autonomous rules settings	427
Areas of use	429
Work schedules	431
Personnel	434
Creating a group	435
Creating a new person	437
Additional actions with persons	443
Data Synchronization	446
Person access levels	448
Access schedule	450
Rules of passage	453
Reports	458
Notifications	459
Visitor templates	461
Exculpatory documents	463
Pass design	465
Card protection	468
Audit	470
TRASSIR ACS Enterprise	472
Servers	473
Personnel	475
Creating a group	476
Creating a new person	477
Changing the person's data and blocking the person	481
Access levels	483
Access schedule	484
Work schedules	487
Areas of use	490
Reports	491
Audit	495
Access monitoring control and security and fire alarm systems	497

Server settings for operation with Orion Pro Access Control System	500
Connection of server to operate with "Hikvision" ACS control panels	502
Connection of server to the "Hikvision" ACS control panel	503
Server settings for operation with "Rubezh (FireSec)" fire alarm system	504
Adding Rubezh Firesec module	505
FireSec software module settings	506
Typical server settings for operation with Access Control or FAC	507
FortNet ACS server settings features	508
"Gate" ACS server settings features	509
Sigur(Sphinx) ACS server settings features	510
Access monitoring and control system NeoGuard server settings features	511
Access monitoring and control system "Itrium" server settings features	512
Specific features of the server settings for operation with Schrack security and fire alarm system	513
Specific features of server settings for operation with Spica access monitoring and control system server	514
Features of server settings for operation with Paradox access monitoring and control system panels	515
Stemax system server settings features	517
Server settings features for operation with "MaxLogic" panels	518
Configuration of Suprema (Biostar 2) Access Control	519
AMCS or security and fire alarm system objects settings tree	520



Customer support

Our company pays great attention to the customer support. As part of the information support:

- the technical support for installation and setup of TRASSIR is provided
- there is a special section on [our website](#), that contains a set of TRASSIR technical documentation, necessary drivers and utilities, as well as guidelines and information materials;

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 guide to installing, configuring and using the TRASSIR software.

The purpose of the document is to:

- to help administrators install TRASSIR on the servers and video surveillance system workstations on their own, run it and configure to meet their needs;
- provide the background information on the TRASSIR features and ways to get technical support;
- ensure quick information retrieval to resolve issues related to installation, setup, and operation.



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

Scope and feature summary

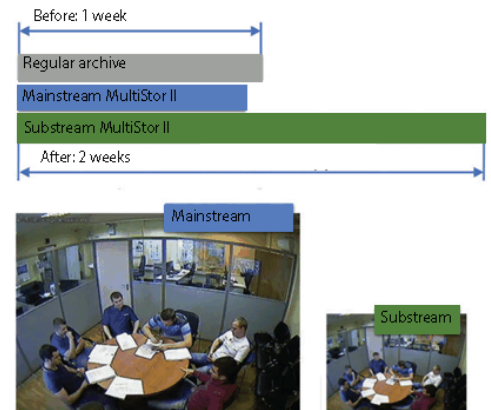
The TRASSIR software is a state-of-the-art automated system, designed to organize video surveillance, intelligent processing and storage of video information, as well as providing means of access to video information to operational and dispatch personnel.

TRASSIR covers a wide range of tasks. It is a reliable basis for creating both centralized and decentralized video surveillance systems.

The software is implemented in a network distributed architecture: it can run both on a single server and as part of multi-machine complexes. The clients using video surveillance information work on separate workstations and can connect to the servers via local network or the Internet.

TRASSIR is the cutting-edge software with the following features and technologies:

TRASSIR technologies for reliable data storage



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 (video recorders and IP cameras) support archive recording to the built-in hard drive or SD-card. TRASSIR can manage each archive separately and, in case of server failure or loss of communication, the data on the device will not be lost. After the network is restored, TRASSIR will provide access to the archive on IP devices.

Video data archive. TRASSIR supports an unlimited number of hard drives for recording, which allows you to create archives of tens of terabytes. It also supports hot-switching and connection of different types of digital media: 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.

Video archive preview. TRASSIR allows you to conveniently work with the video archive of devices regardless of where the archive is physically stored. You can view video from the archive from a single device channel display window, either directly in front of the video surveillance server monitor or by connecting to a remote server via LAN, Internet or a chain of other servers.

Video archive export. TRASSIR lets you export video clips from the archive either directly in front of the video surveillance server monitor or by connecting to a remote server via LAN, Internet or a chain of other servers. This function may be necessary to save video clips with significant episodes to the device and to transmit video clips with significant episodes to third parties (for example, episodes with violations that may be necessary for investigation).

Lost channels. This feature makes working with the archive much easier, allowing you to view it on any PC without any additional actions and settings. You can record the archive from the video server to an external disk, then connect it to any PC where {TRASSIR} is installed, and work with the archive as on the video server. You can also view such an archive using the free client application, which does not require a USB key with a license to run.

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 video surveillance system events are logged and stored in *database*, which can be either on the local or remote server. The storage time of events in the database is determined by the server settings.

Motion Archive Search. TRASSIR ActiveSearch built-in functionality of the AnyIP platform for interactive archive search based on metadata from a motion detector (or from the built-in detector on the device). It includes MultiSearch capabilities - search in one scene for fragments from different time points in the archive. The intelligent search of video fragments in the archive TRASSIR ActiveSearch feature, designed to work in conjunction with motion detectors and included in the default professional {TRASSIR} software package. It can work in conjunction with both the basic detector and SIMT object tracing detector. It also provides fast search in the archive by motion in the video camera scene area.



Search the archive by event. TRASSIR EventSearch is the archive event search software, based on the system event log. For visualization and convenience of searching for certain actions / signals / incidents, the software provides a special function {TRASSIR} EventSearch, which allows filtering events by keywords.

In addition to the default built-in labels, such as informing about the server health indicators state, user login, system shutdown, etc., you can create individual settings for displaying the information stored in the log, such as: appearance of an object in a prohibited area, identification of a car license plate number, conducting a monetary transaction, etc. In order to narrow down the search time frame, it is possible to select events in the specified days / hours / minutes interval. Also, by creating your own filters in the EventSearch, TRASSIR allows you to save them for future use.

TRASSIR Cloud is a free WEB-service that monitors the work of your servers around the clock. In addition, the TRASSIR Cloud allows you to manage your servers from your personal cabinet and display their status on map.

TRASSIR network capabilities



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 a unique TRASSIR feature, that allows you to join servers in a tree-based network.

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

Ergonomic and management features



The **open user interface** allows you to customize your workspace using ready-made 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.

The **multitasking 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.

Administrator interface lets you set up all basic server/client parameters.

Operator interface is a simple and easy-to-use monitoring tool designed to view video from cameras.



Easy navigation accelerates user operation by times.

There is a built-in player for viewing the archive, which allows you to preview fragments in any order, scroll forward and backward, increase and decrease the viewing speed, and view frame by frame. You can also export segments of the archive to a video file and create screenshots.

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.

ActiveDome speeds up PTZ camera control by 20 times. This allows you to automatically monitor large areas and zoom in objects with a single click.

TRASSIR has **built-in search tools**, which allow you to find the required event and, if necessary, go directly to viewing the archive associated with this event. In addition, you can create filters for current events, which can reduce the amount of information displayed. Using filters, you can achieve the output of only those events that are worthy of the operator's attention.

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

A **multi-level rights distribution system** is implemented in TRASSIR, allowing to prevent unauthorized access. An 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.

API. TRASSIR has SDK that allows you to link TRASSIR with any other system in use and get information from it, and manage TRASSIR with commands.

TRASSIR integration



A wide range of supported devices. Different types of devices can operate in the same video surveillance system: *Video capture cards with hardware/software compression* and *IP equipment*. Meanwhile, the software works correctly with most modern hardware platforms, and the list of supported devices is constantly expanding.

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 Control System and Security and Fire Alarm allows you to get a complete list of events from ACS. It will provide possibility to adjust response rules, manage objects using maps, perform photo and video verification and view the status of all the objects.

AutoTRASSIR is an automatic license plate recognition system, that can be used to control the entry/exit of vehicles from the territory of enterprises, as well as, by the traffic police, at checkpoints and other control points. The server provides interaction with access control systems, video and audio control and executive devices (for example, barriers).

Built-in detectors and analytics

Sound detector triggers when the volume level is exceeded and starts video recording according to a preset scenario, allowing timely response to suspicious audio incidents.

Motion Detector allows you to detect any motion in the frame - a person, animal, vehicle, moving object or the beginning of rain. There is a hardware motion detector (motion detector of the camera itself), activity detector or HD activity detector (TRASSIR software motion detector). This feature allows you to receive notifications when there is motion in the frame, as well as save the archive capacity significantly by recording only when motion occurs.

Heat Maps. The system of "heat" video analysis is aimed at raising the security level. There are 2 operation modes : Dynamic and static. The first one superimposes a color scale of activity on video, as a result of which any moving object in the frame leaves a "trail" behind it, which disappears over time. The second accumulates "heat" indicators in separate parts of the image, where the activity was most intensively recorded.

Left object detector allows you to instantly identify abandoned and forgotten items, potentially threatening the security of the facility where video surveillance is installed.

Sabotage Detector allows you to detect various actions with the camera, such as changing the shooting direction (shift), changing the size of the shooting area (defocus), sudden increase or decrease in the lighting of the shooting area as sabotage, and using the Alarm Monitor script to customize reactions to these events.

Fire and smoke detector allows detecting smoke or fire faster than fire sensors (alarms), as well as providing fire protection in open spaces where fire sensors cannot be installed.

Alarm notifications

TRASSIR allows you to receive notifications when an alarm event occurs in the form of incidents in the client or on the server, as push or sms notifications in the mobile application, as well as notifications in Telegram. To generate notifications, you need to add and run a script on the server.



- *Basic information*

System requirements

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

1. [Video server](#) is a PC on which the software will be used to process video, store the video archive, and manage the entire video surveillance system.
2. [Compatible IP Devices](#). Refer to this section if you are planning to deploy a video surveillance system based on IP 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. **Processor.** The processor is a video server key component. It is recommended to use modern multicore processors with high clock frequency to ensure smooth and stable system operation. The preference should be given to the single-processor configurations (the motherboards with 2 or more processors are not recommended).
2. **Video card.** If you plan to display video directly on the surveillance server, you should use a discrete video card. TRASSIR works with almost all modern ATI Radeon and nVidia video cards. You can find recommendations for video card selection at [our knowledge base](#).
3. **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](#).
4. **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 for proper server operation, several changes must be made to the [operating system settings](#).
5. **Monitors.** It is recommended to use monitors with a resolution of at least 1280x1024 pixels for optimal TRASSIR operation. It provides a sufficiently high image clarity and is necessary for effective video surveillance. The optimal number of monitors to be connected depends on the specification of the video card used, but in general does not exceed 8 to ensure convenient display and control of video streams.



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](#)

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 1TB in the video recorder for archive storage, then when you install a new hard disk in the server or connect a network storage to the server, the size of their logical partitions must not exceed 2TB.



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

Compatible operating systems

TRASSIR supports all modern versions of the Windows x64 operating system. Here is the list of compatible operating systems:

- Windows Server 2022 (Build: 10.0.20348)
- Windows Server 2019 (Build: 10.0.17763)
- Windows Server 2016 (Build: 10.0.14393)
- Windows 11 (Build: 10.0.22623)
- Windows 10 (Build: 10.0.19045)

TRASSIR can also be run under the **Astra Linux SE** operating system (versions 1.7.0 and 1.7.4).



For TRASSIR proper operation, in **Windows** and **Astra Linux SE** you should customize a number of settings. You can find a list of the required settings in our [knowledge base](#).



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

Compatible IP equipment

TRASSIR provides complete operation with IP equipment, and the list of supported manufacturers and models of equipment is constantly expanding. A complete list of compatible IP equipment, as well as a list of RTSP and ONVIF IP equipment, is always available [on our website](#).



- [Installing compression cards](#)
- [IP video recorder installation](#)
- [NAS Setup](#)

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. Server *OS setup* for proper software operation.
3. *Installation of Guardant USB key drivers on all servers.* USB keys are used to protect licensed copies of the software 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. Installation of the software as *standalone app* or *Windows service*.
6. *Installation of the software client version* to all workstations that will be used for video surveillance.

Please note that video surveillance can be performed either via the client or via the server. In addition, you can also choose not to install the software on the operators' workstations at all. To do so, you need to configure *web-server*. All the video surveillance functions will be available using a regular browser. You only need the Mozilla Firefox browser installed on your workstation and a video surveillance extension, which is installed by clicking on the corresponding link in the browser.

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 lets you use both hardware and software compression cards in one 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.

IP video recorder installation

TRASSIR supports operation with various IP video recorders. The instructions below will help you to prepare them to connect to the server.



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



We strongly recommend you check the user manual and device compatibility list before connecting any equipment to the IP video recorder.

follow the next steps before connecting IP video recorder to the server:

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. Stabilize the IP video recorder and power it on.
8. Open WEB-interface of the device and format the hard drive.
9. Set up IP video recorder using [SADP app](#).

After that, you can [add device](#).

IP video recorder network settings

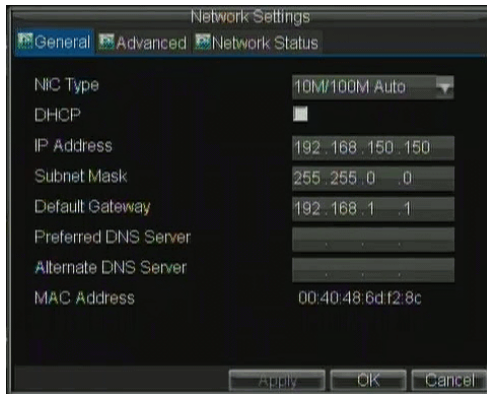
After *preparing the IP Video Recorder* and before *adding* it to the server you need to set the device network parameters: *IP address*, *subnet mask* and *gateway*.

Parameters can be set in two ways:

- in SADP app, which you can download from *our website*;
- in the device's interface.

IP video recorder setting via its own interface

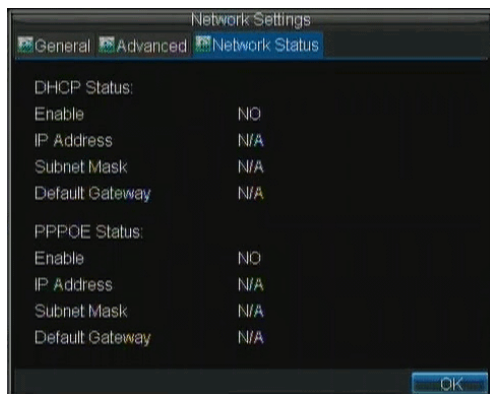
1. Connect monitor and mouse to the device.
2. Turn on the IP video recorder.
3. Open network settings menu by selecting **Menu > Settings > Network**.
4. Select the **General** tab in the opened menu.



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:

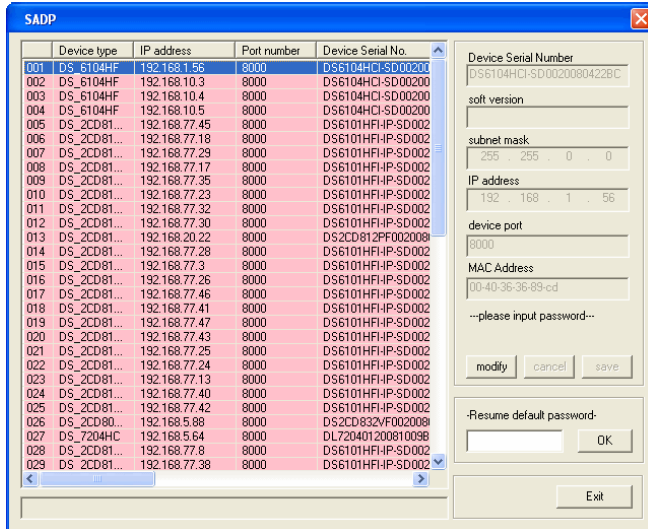


- **Manual network settings** -set the following values:
 - **IP address** - The address that is to be assigned to the device;
 - **Mask** - The subnet mask;
 - **Gateway** - The IP address of the gateway (this is usually your router);
 - **Primary DNS server, Secondary DNS server** - The primary- and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

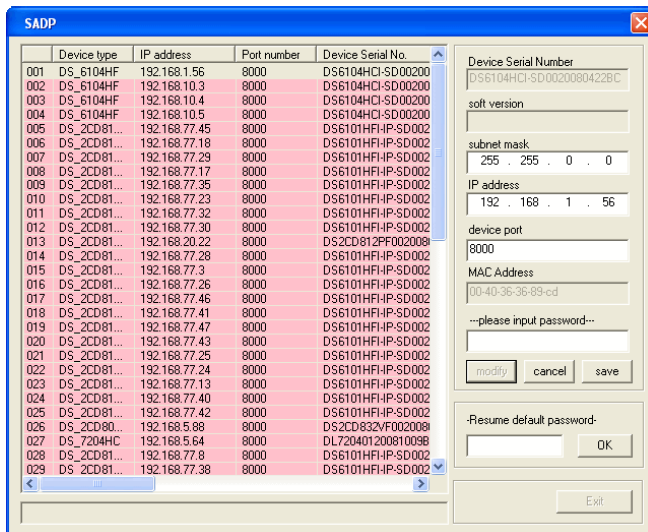
6. Press **OK** button to save the settings.

IP video recorder setting using SADP utility

1. Download SADP app from [our website](#) and install it.
2. Run the utility. Press **Enter** in the window that opens.
3. In the list of the discovered devices, select the device. Click **Modify**.



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



7. Click **Save**.



• **IP video recorder 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. Almost any iSCSI network storage can be used on a server as a video archive.



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

Setting up a network storage connection in the software depends on the operating system in which it runs:

- *Windows operating systems*
- *"Linux-based TRASSIR OS"*
- *Astra Linux SE 1.7*



- *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.

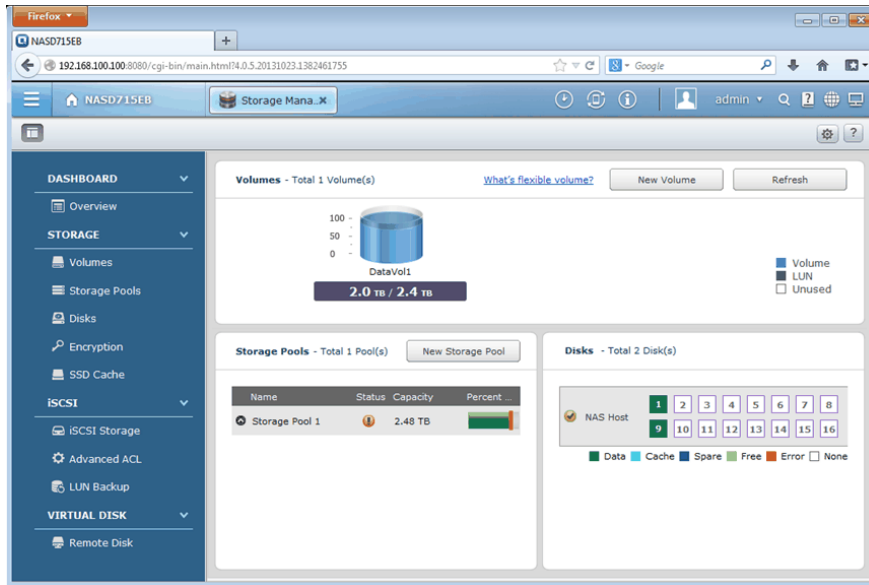
If the connection is successful, a sign-in window will appear in the browser.



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

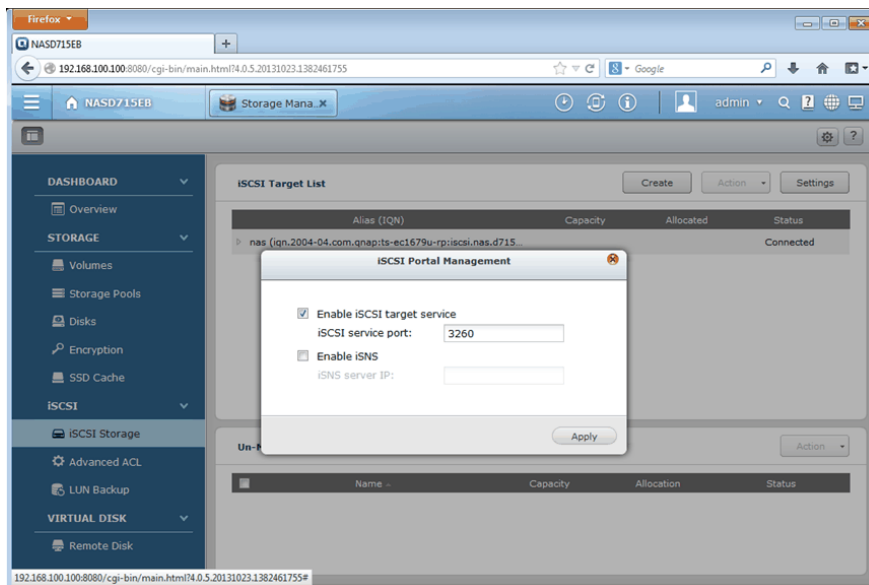


3. Run **Storage Manager** and click the **Dashboard** -> **Overview** link. This page contains information about the hard disks installed in the network storage, their state, and size.

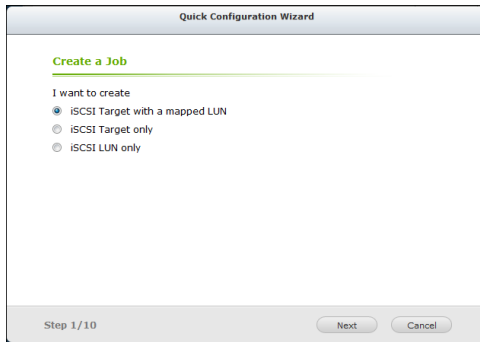


You need to create one or several volumes to use the network storage as a video archive. Please note that all logical disks to which the archive will be recorded, should be of approximately equal volume and must not differ in size by more than 2 times. You can use a RAID array to ensure data storage 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

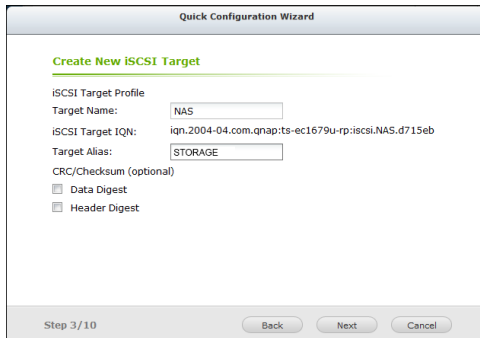
I want to create

- ☒ 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)

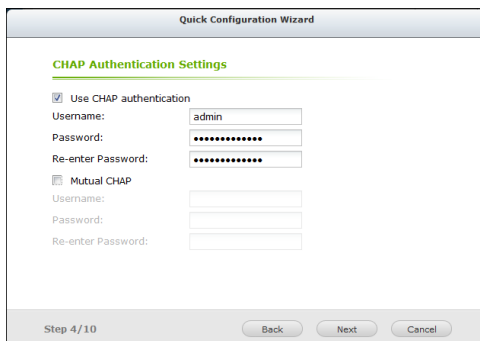
- ☐ Data Digest
- ☐ Header Digest

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:

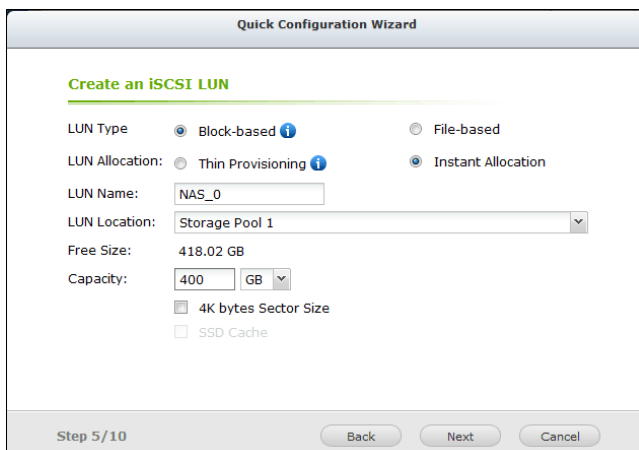
Re-enter Password:

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

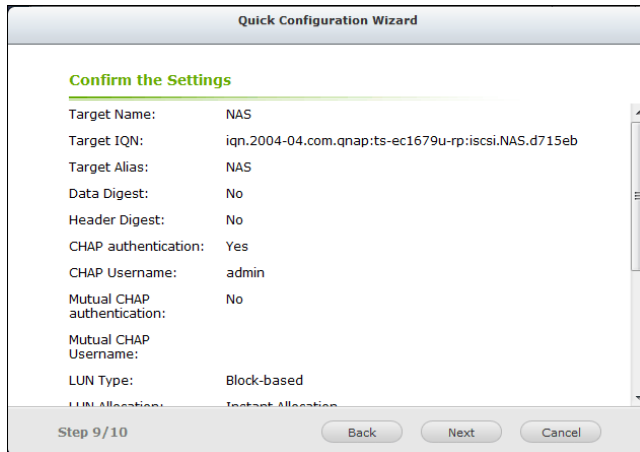
☐ SSD Cache

Step 5/10

Back Next Cancel

Click **Next** to continue.

9. In step 9, confirm the selected settings.



Quick Configuration Wizard

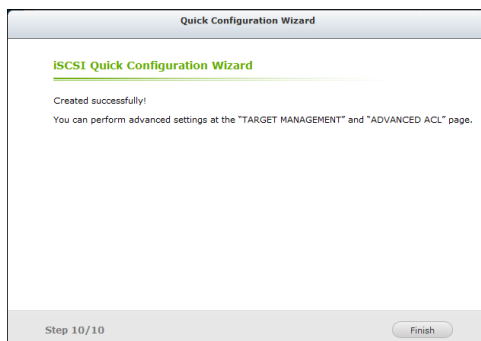
Confirm the Settings

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

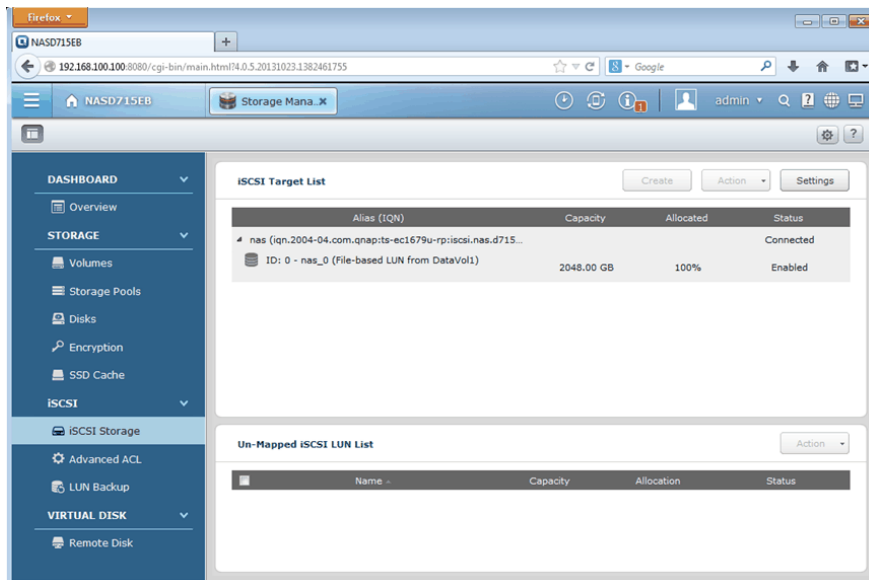
iSCSI Quick Configuration Wizard

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:



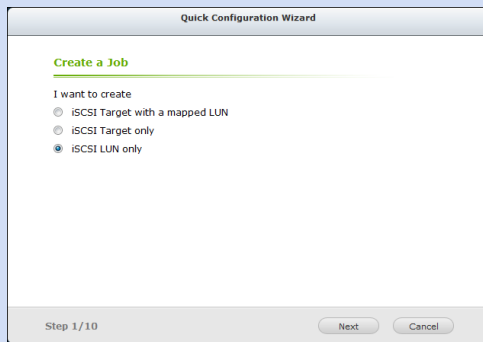
The screenshot shows the web interface of a NASD715EB device. The left sidebar contains a navigation menu with sections: DASHBOARD, STORAGE, and VIRTUAL DISK. The 'STORAGE' section is expanded, showing 'iSCSI Storage' as the selected option. The main content area displays the 'iSCSI Target List' with a table containing one entry:

Alias (IQN)	Capacity	Allocated	Status
nas (iqn.2004-04.com.qnap:ts-ec1679u-rp:iscsi.nas.d715... ID: 0 - nas_0 (File-based LUN from DataVol1)	2048.00 GB	100%	Connected Enabled

Below the table, there is an 'Un-Mapped iSCSI LUN List' section, which is currently empty.



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.



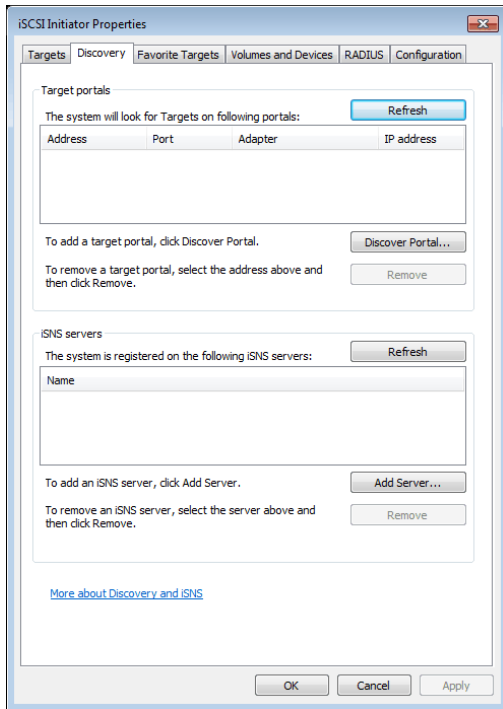
- [NAS Setup](#)
- [Connecting a network storage in a Windows OS](#)
- [Configuring a network storage connection in Linux-based TRASSIR OS](#)
- [Archive setup on the server](#)

Connecting a network storage in a Windows OS

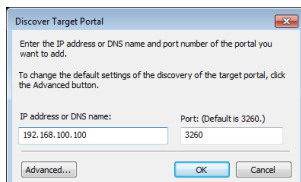
Volumes that were configured on the network storage when connecting in a Windows OS will be displayed as logical disks. In other words, all commands that apply to logical disks can be used when working with these disks.

Network storage connection procedure and settings in a Windows OS:

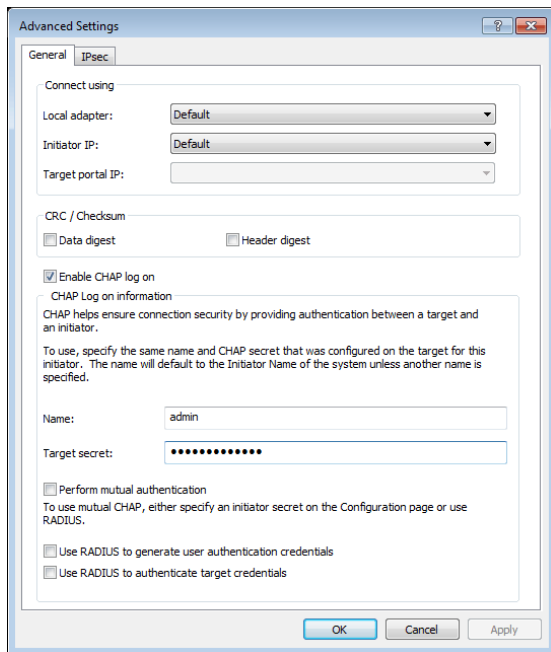
1. Open **Start -> Control Panel -> Administration -> iSCSI Initiator**



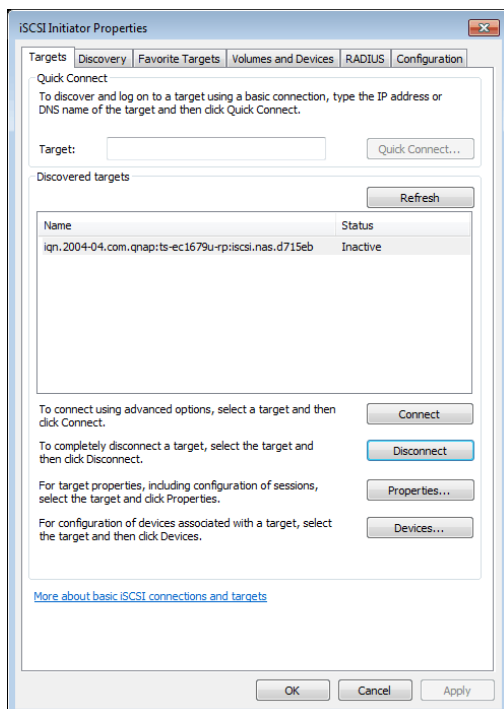
2. Go to the **Discovery** tab and click the **Discover Portal...** button to connect to the network storage
3. Enter the IP address of the network storage and specify the iSCSI service port that was entered during *configuration of the network storage*.



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

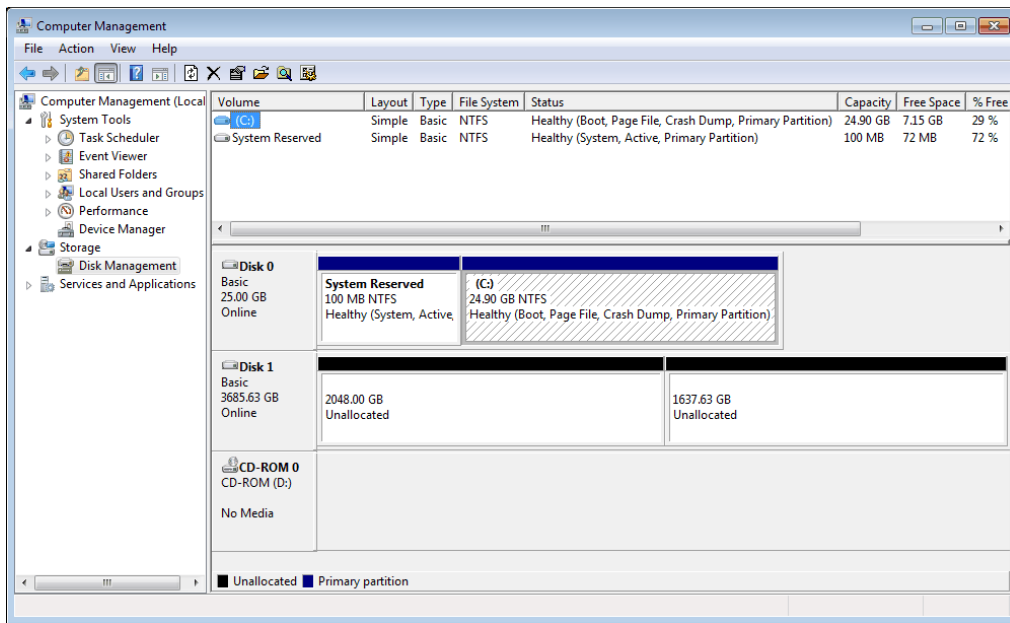


5. If there the network storage successfully connects, its identifier will appear in the **Targets** tab. And it's status will be "Inactive".



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 and partition the drive before using it. Please note that all logical disks to which the archive will be recorded, should be of approximately equal volume and must not differ in size by more than 2 times.



- [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 dongle is a device designed to protect the server and associated data from unauthorized use and duplication. Each license contains information about the USB key number that should be used to start and run the software.

You will not be able to use the server in the following cases:

- USB key is not connected to the PC on which the software is installed;
- USB key drivers are not installed, or some errors occurred during the installation;
- the USB key physical number and the number, specified in the license, do not match.

To install drivers for Guardant USB keys on Windows, you need to:

1. Make sure that you have administrator rights. Otherwise, driver installation will not be possible.
2. You can download drivers for Guardant USB key from the manufacturer's website, or [our website](#). You should consider version and bit-type of your operating system when downloading the drivers.
3. Disconnect all other keys (if they were connected). The Guardant USB key should be connected to the port only after the drivers have been installed. If the key was plugged in prior to the driver installation and the standard Windows device installation wizard started running, remove the key from the port and complete 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, check the Guardant USB-key operability. To do this:
 - Connect the Guardant USB-key.
 - Be sure that the key's network indicator is constantly lit.
 - Make sure the Guardant USB key is listed in Windows Device Manager.



You can install Guardant key drivers during the software installation, as the distribution package contains the necessary key drivers.



No driver installation is required in **Astra Linux SE 1.7** OS. You can plug the Guardant key into the USB port of the server.

Windows OS settings

This section contains the network ports used by the server (default values are indicated):

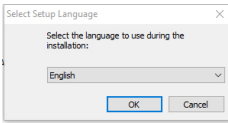
- PostgreSQL database cluster port - 5432;
- Server control port - 3080;
- Video broadcast port - 3081;
- Web server port - 8080;
- RTSP broadcast port - 554.
- HTTP broadcast port (flv, mjpeg) - 555.
- Cloud Connect activation port - 443/UDP.



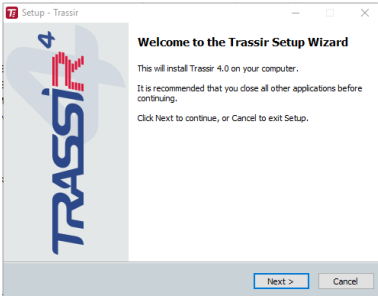
Make sure that the installed antivirus software does not control the ports used to connect to network devices. If necessary, allow the use of the specified ports and add the software to the list of trusted programs after the installation.
You can change the default port values.

Installation of the software server version

Run the setup file, select your language and press **OK**.



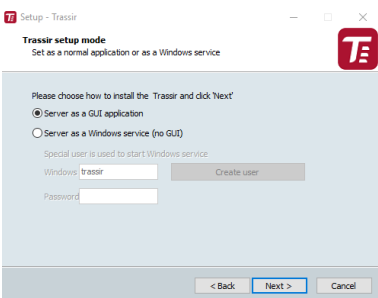
An installation wizard will start after the language selection. Press **Next**.



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**.

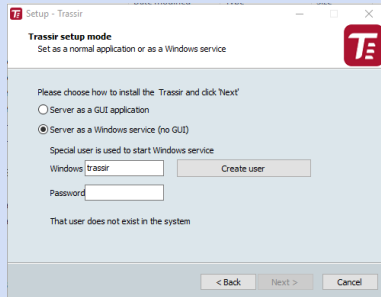


At the next step select the installation option **Server as GUI application** and press the button **Continue**.



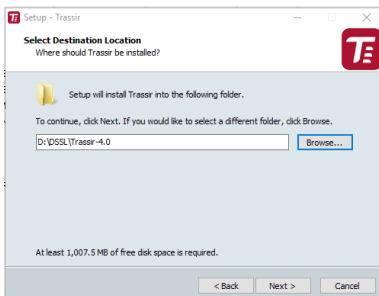


If you want to install the server as a Windows service, select **Server as Windows service (without GUI)** installation option and enter the user data which will be used to run the service. In case such user is not available yet, you can create it, pressing **Create new user....** Press **Next** to proceed.

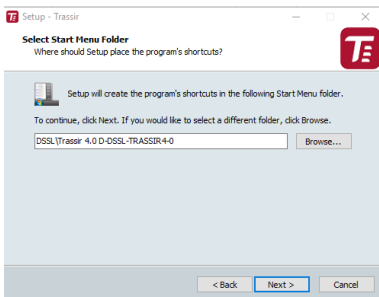


You can use the **client software version** in order to connect to the server installed as a Windows service. Learn more about connecting to a server in [Connecting to a new server](#).

Specify the installation folder manually or by using the **Browse** button. Click the **Next** button after that.



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



Next step, the installer will prompt you to install and configure the PostgreSQL DBMS. All events recorded in the server, will be stored in the database. Although the software can work without a database connection, we strongly recommend using one. Moreover, certain modules require a database.

- In case a PostgreSQL database is already installed on a PC, the installation wizard 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 install the database automatically, download the archive with the installation files from [our website](#) and unzip it into the same folder as the installation file. Alternatively, you can always download PostgreSQL from the [official site](#) and perform the [manual database installation](#).



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.



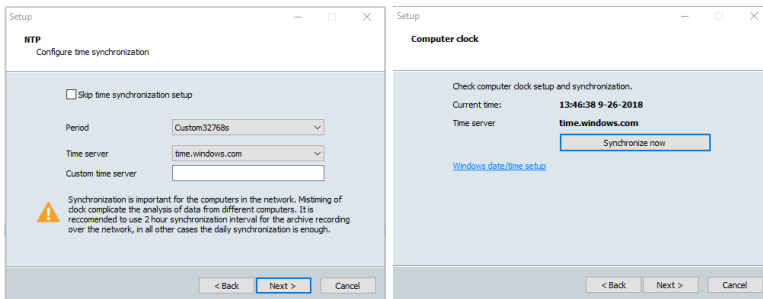
The **PostgreSQL superuser's password** can be selectable and you can subsequently create new database users.

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.

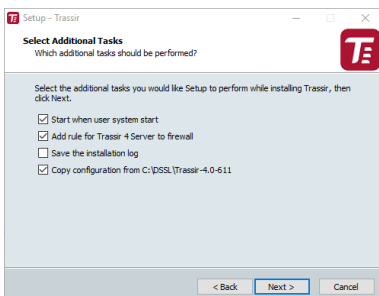
- If the installer cannot find the installation files for the DBMS, and PostgreSQL DBMS is not installed on the PC, the installer will issue a warning. Click **Next** to skip the installation of the DBMS, or verify that the DBMS installation files are in the same folder as the installer file and restart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

Next step, the installation wizard will offer you to configure the time synchronization service (NTP). Select a synchronization **Period** and **Time server**. You can also 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 installation wizard 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**.

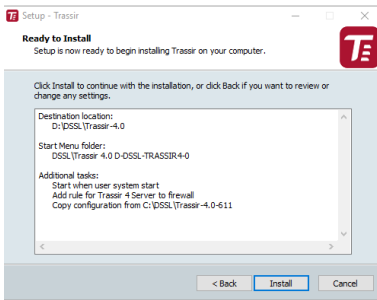


Select any additional installation settings. Click **Next**.

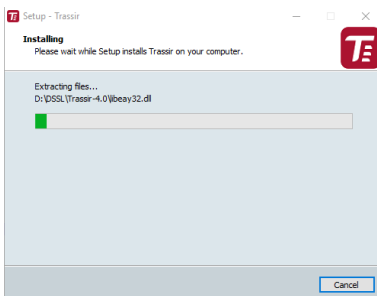


- **Start when user system starts** lets you restore a system to working order in the event of potential hardware failures, for example, if the electricity supplied to the site is unreliable.
- If you plan to use the standard Windows Firewall, then set the **Add rule to firewall** checkbox.
- If needed,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

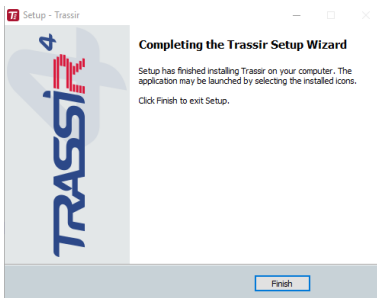
The wizard will show the selected installation parameters in the final step. Click the **Install** button.



The files will begin to be copied.



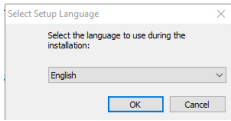
Click **Finish** to complete the installation.



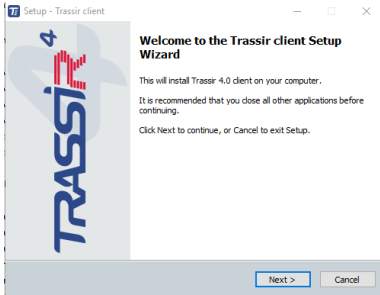
- *Installing Guardant USB keys*
- *Start the software and sign into the system*
- *Working with the basic interface*
- *Settings*
- *Installation of the software client version*

Installation of the software client version

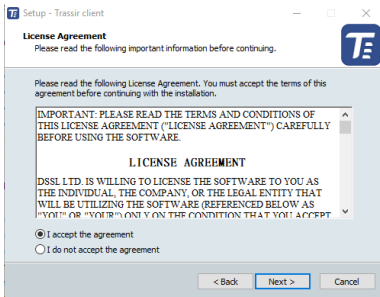
Run the executable file, select your language and press **OK**.



An installation wizard will start after the language selection. Press **Next**.

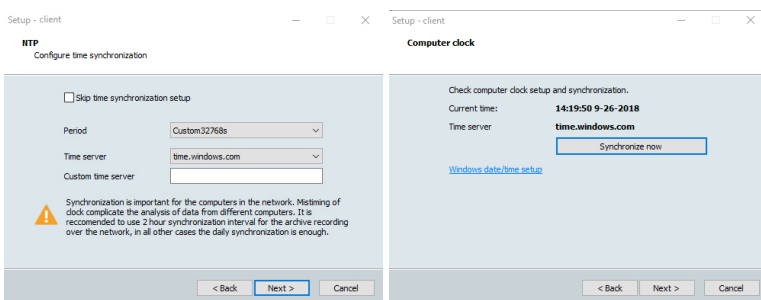


You can review the text of the license agreement on the **License agreement** screen. After reviewing the agreement, select **I accept the agreement** and click **Next**.

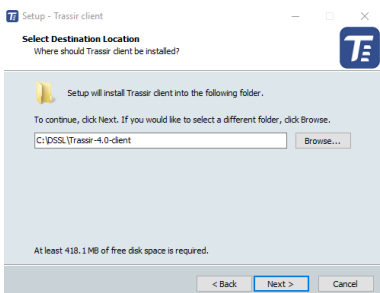


Next step, the installation wizard will ask you to configure the time synchronization service (NTP). Select a synchronization **Period** and **Time server**. You can also specify the address of an arbitrary NTP server or cancel the configuration of NTP by setting the **Skip time synchronization setup** checkbox. Click **Next**.

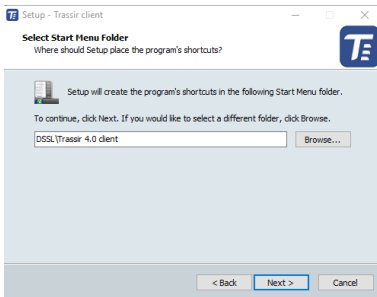
The installation wizard will ask you to verify the correctness of the server current date and time. You can synchronize time using an NTP server by clicking the corresponding button, or click the **Windows date/time setup** link to quickly navigate to the settings window. Click **Next**.



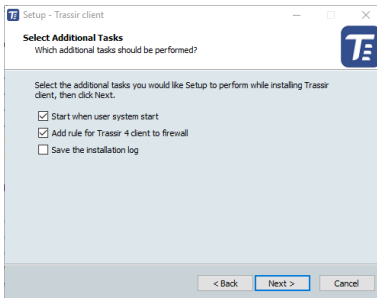
Specify the installation folder manually or by using the **Browse** button. Click the **Next** button after that.



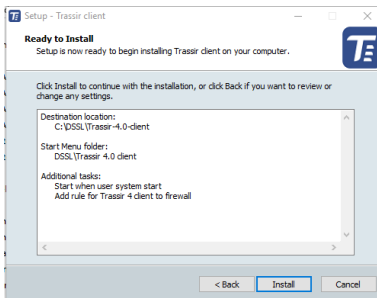
Specify the Start Menu folder where application shortcuts will be created. Click **Next**.



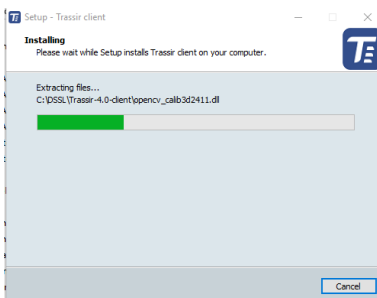
Select any additional installation settings. Automatically launching the application makes it possible to bring the system back in operation in case of server hardware failures, for example, an unreliable supply of electricity to the site. If you plan to use the standard Windows Firewall, then set the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



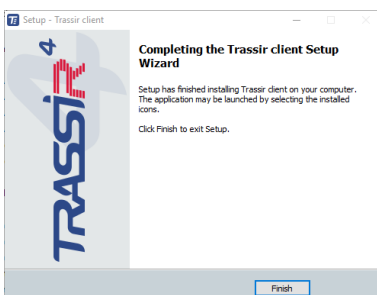
The wizard will show the selected installation parameters in the final step. Click the **Install** button.



The files will begin to be copied.



Click **Finish** to complete the installation.





- *Working with the basic interface*
- *Connecting to a new server*
- *Installation of the software server version*

Installation and uninstallation of the software server version in Astra Linux SE 1.7



The installation and uninstallation of the software server version in Astra Linux SE 1.7 is performed by console commands.

Preliminary preparation before the software server version installation

1. Check that only the following repositories are connected in the `/etc/apt/sources.list` file:

```
# Main repository
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-main/      1.7_x86-64 main contrib non-free
# Operational updates to the main repository
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-update/    1.7_x86-64 main contrib non-free
# Base repository
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-base/      1.7_x86-64 main contrib non-free
# Extended repository
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/  1.7_x86-64 main contrib non-free
# Extended repository (astra-ce component)
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/  1.7_x86-64 astra-ce
```

2. Check for ca-certificates

If it is not available, download and install it using the commands:

```
wget https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-base/pool/main/c/ca-certificates/ca-
certificates_20220331+astra3_all.deb --no-check-certificate
sudo dpkg -i ca-certificates_20220331+astra3_all.deb
```

3. Update packets from connected repositories

```
sudo apt update
```

4. Install the packets required for further installation of the software server version:

```
sudo apt install linux-headers-$(uname -r) build-essential libglvnd-dev pkg-config libc6-i386
```

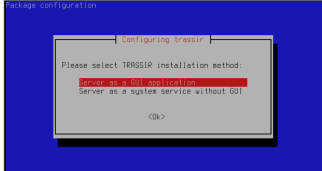
Installation of the software server version

1. Download the deb packet of the software server version.
2. Check that the folder contains a deb packet with the same version. Run the installation with the command:

```
sudo apt-get install --reinstall ./trassir-*.deb
```

All necessary updates will be downloaded and installed during the installation process.

3. During the installation process, select one of the options:



After the first installation, the method selection is saved and used when reinstalling or upgrading the software later.

In order to change the software operation mode, run the command:

```
sudo dpkg-reconfigure trassir
```



When installing the software in **File Manager** (QApt application), you cannot select an installation method, so the **Server as GUI application** option will be automatically selected, or the last selected method will be used if the software has already been installed.

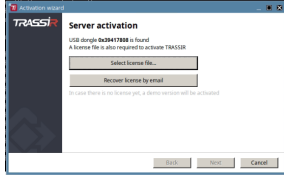
4. After installation, the server will reboot.
5. If **Server as a GUI** is selected, open **Start -> Network -> TRASSIR Server** to run the software.
If you select **Server as a system service without GUI**, the software will automatically start in the background immediately after the installation or automatically when the server boots.

Licensing

The licensing process differs depending on the installation option selected:

- **Server as a GUI application**

Once installed, the **Server Activation** service will start.



Follow the service prompts.

- **Server as a system service without GUI**

Copy file "license.txt" to the /var/lib/vms/.

The license can be updated, if necessary. For details on license update procedure, see [Local server settings](#).

Uninstalling the software server version

- **With configuration file and license file saving**

```
sudo apt remove trassir
```

After uninstallation, the archive and data will remain in the /var/lib/vms folder.

- **Completely**

```
sudo apt purge trassir
```

After uninstallation, only the archive will remain in the /var/lib/vms folder.



- *Configuration of the software server version in Astra Linux SE 1.7 for operation with neural network detectors*

PostgreSQL DBMS installation

All events, registered on the server, 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 as 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.



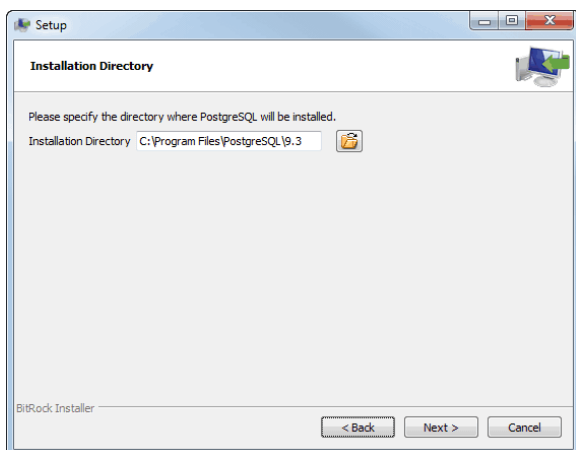
Before installing the PostgreSQL DBMS, review [Configuring the operating system to work with the PostgreSQL DBMS](#)

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

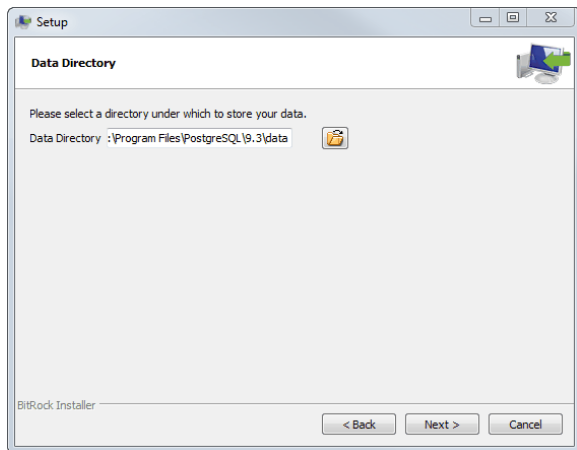
1. Download the PostgreSQL distribution from the [PostgreSQL website](#) (it's free).
2. Launch the installer and click **Next >** in the window that opens.



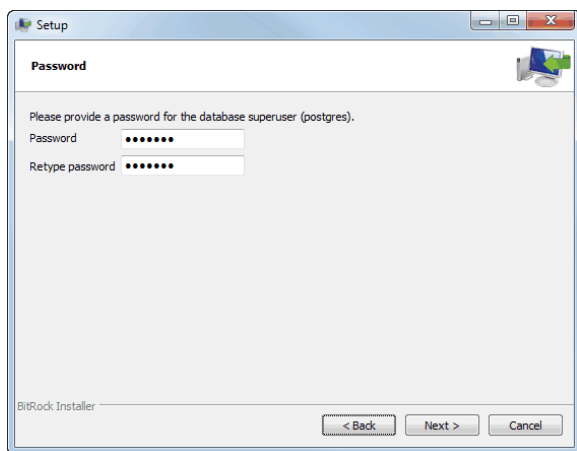
3. Select the database installation folder and click **Next >**.



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

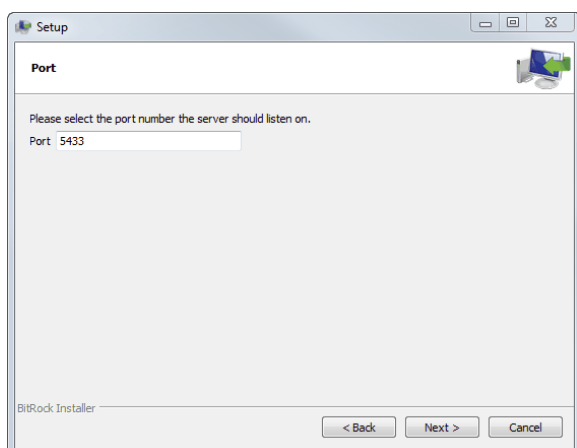


5. In the next step, enter the DBMS's superuser's password. Click **Next >** to continue.

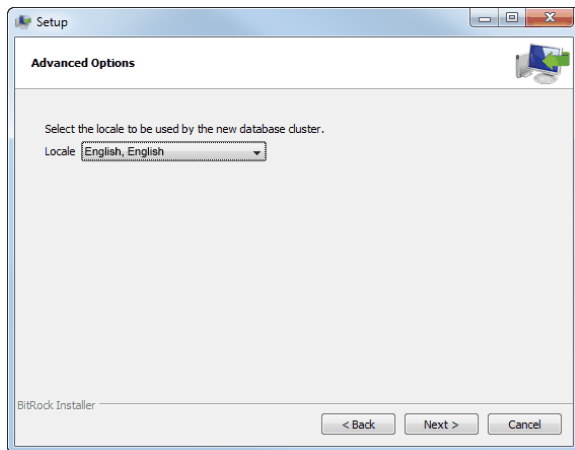


We strongly recommend that you memorize or write down the superuser's password. This password is required to *configure the database connection* and create a backup copy if the *DBMS is moved to a different server*.

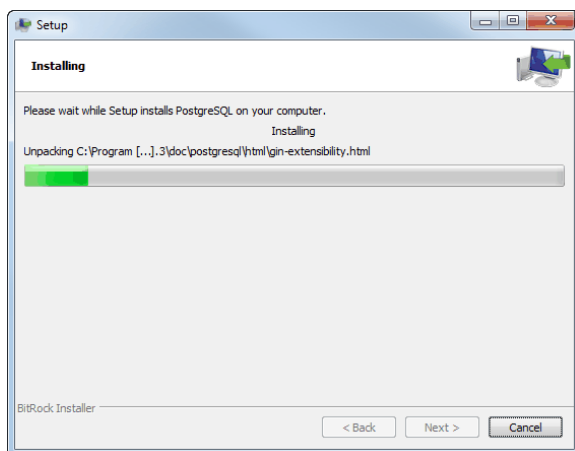
6. If needed, you can change the DBMS connection port. Click **Next >** to continue the installation.



7. In the next stage, select **English, English** 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**.





The installation process of PostgreSQL DBMS in **Astra Linux SE 1.7** OS is described *in the OS knowledge base*.



- *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*

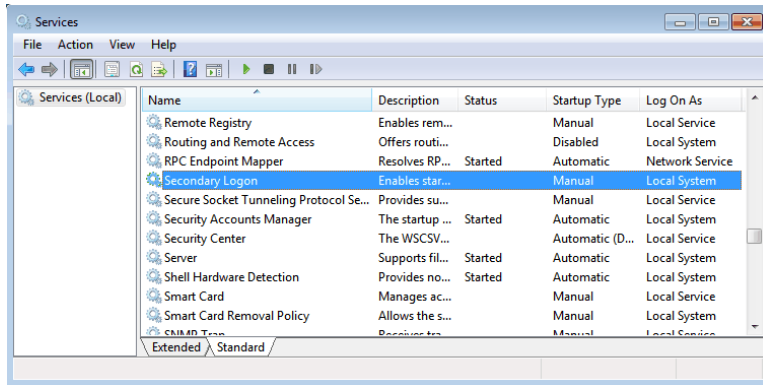
Configuring the operating system to work with the PostgreSQL DBMS

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

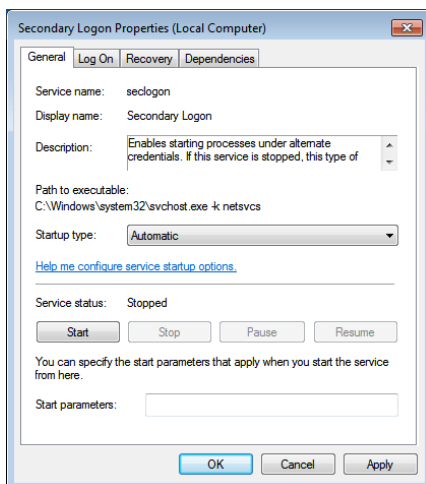
If the service is disabled, you will not be able to install the PostgreSQL DBMS.

To start the Secondary Logon service:

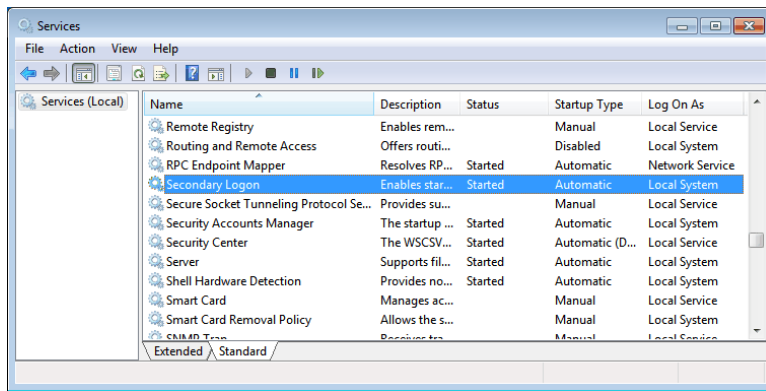
1. Bring up the Windows services management window by running `services.msc`.



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").



The process of **Astra Linux SE 1.7** OS configuration to operate with PostgreSQL DBMS is described *in the OS knowledge base*.



- *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 PostgreSQL DBMS installation, the PostgreSQL Database Server service will be enabled by default. If the service is disabled, the server 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:

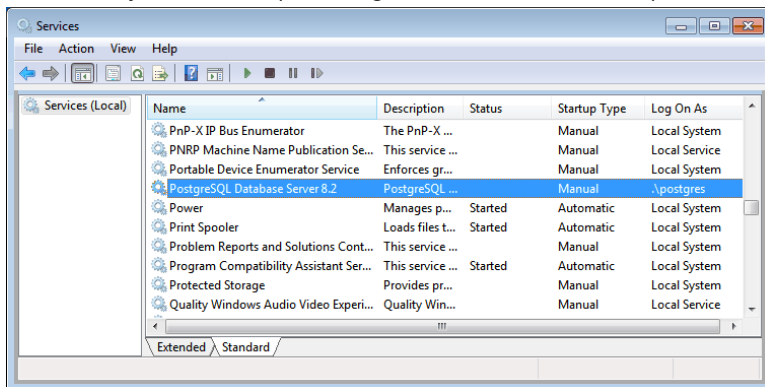
- using the standard tool for managing Windows services;
- using the pgAdmin III utility, which is installed together with PostgreSQL DBMS.



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

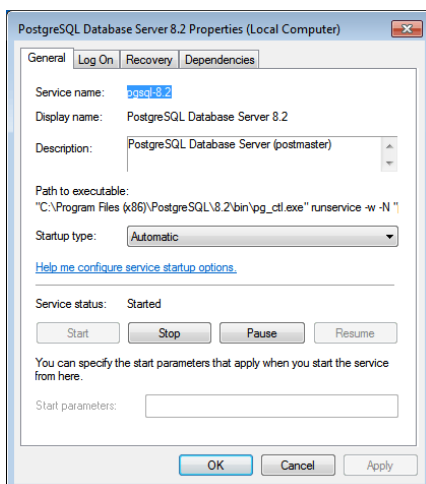
To verify that the service is enabled using the standard Windows tool:

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).

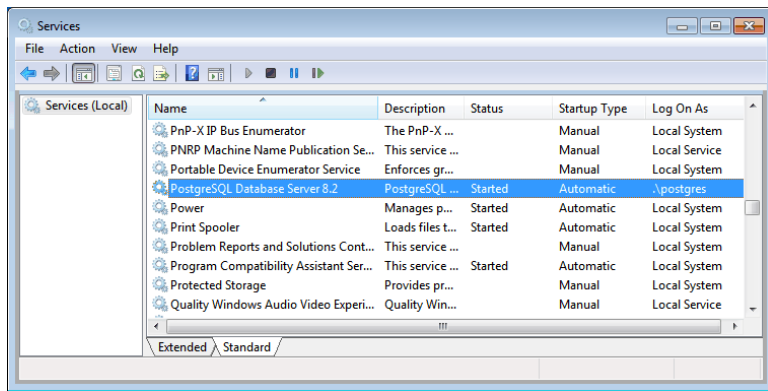


3. If the service is disabled, then open its settings window by double-clicking with the mouse. In the service's settings window:

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

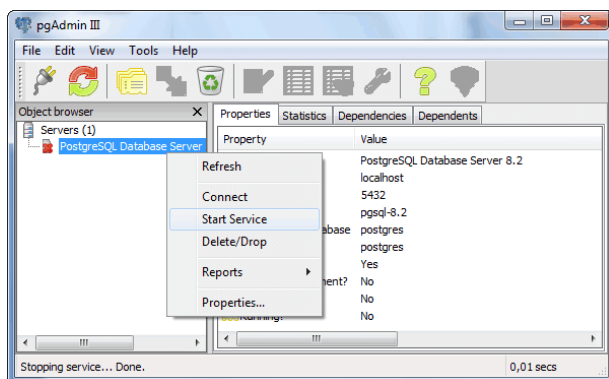


4. Verify that the service started successfully in the window with the list of services (the **Status** field should say "Started").

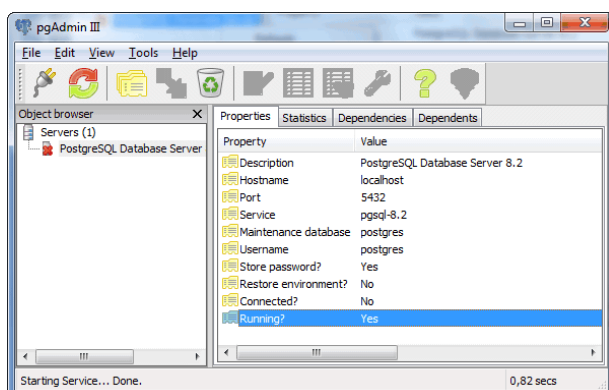


To verify that the service is enabled using the pgAdmin utility:

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").





The process of running PostgreSQL DBMS in **Astra Linux SE 1.7** OS is described *in the OS knowledge base*.

The process of PostgreSQL DBMS autorun configuration is described in *our knowledge base*.



- *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

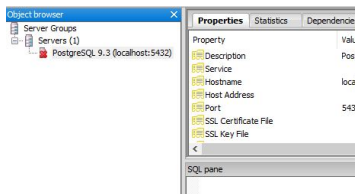
These instructions will help you move a PostgreSQL database from one server to another. We will consider the process of moving a database using PostgreSQL DBMS version 9.3.4 on Windows 7 as an example.

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

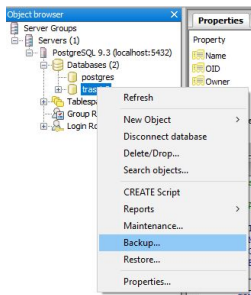
- *Configure the operating system to work with the DBMS;*
- *Install the DBMS;*
- *Launch the PostgreSQL Database Server service.*

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*.

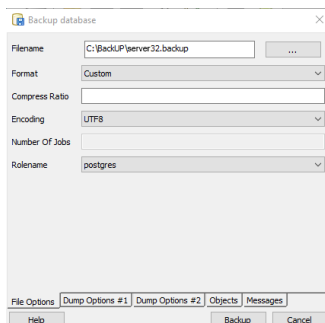


3. In the tree, select the database that you want to move to the new server and select **Backup...** in the context menu

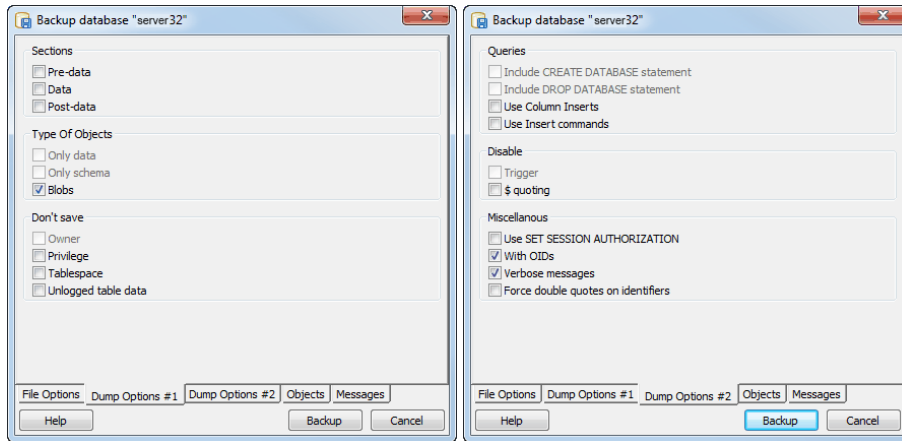


4. On the window that opens, in the **File Options** tab:

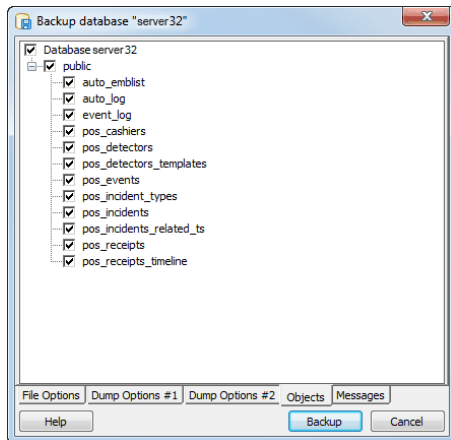
- Enter the **Filename** of the backup;
- In the **Format** field, select **Custom**;
- Leave the **Compress Ratio** field unchanged;
- In the **Encoding** field, select **UTF8**;
- In the **Rolename** field, select **postgres**;



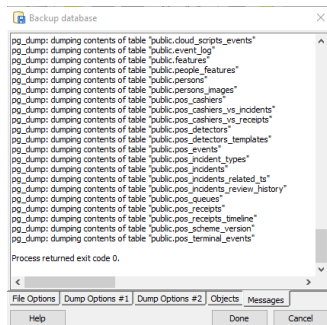
5. In the **Dump Options #1** and **Dump Options #2** tabs, set the checkboxes as shown in the images below:



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



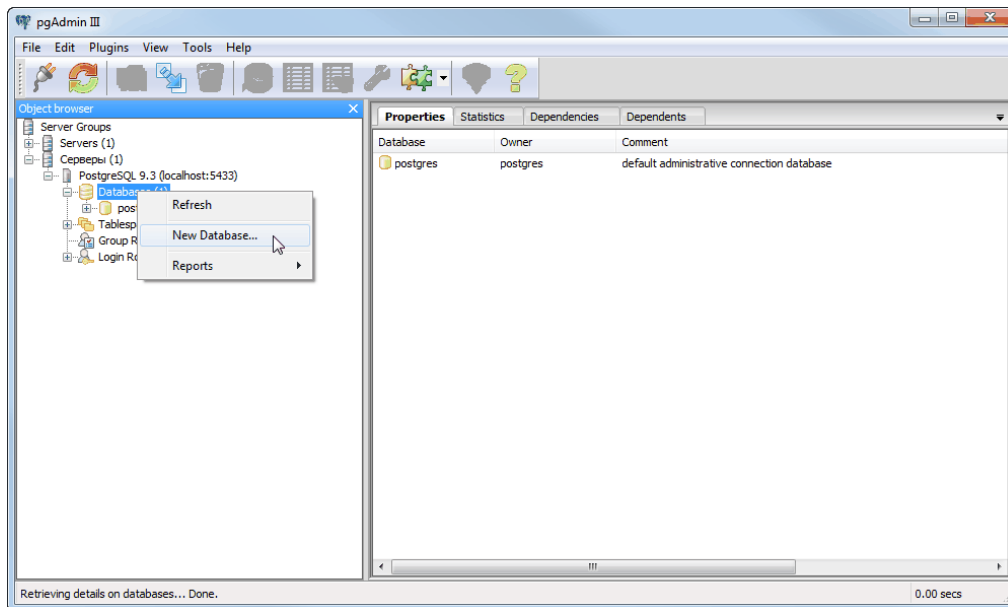
7. Go to the **Messages** tab and start backing up the database by clicking the **Backup** button.



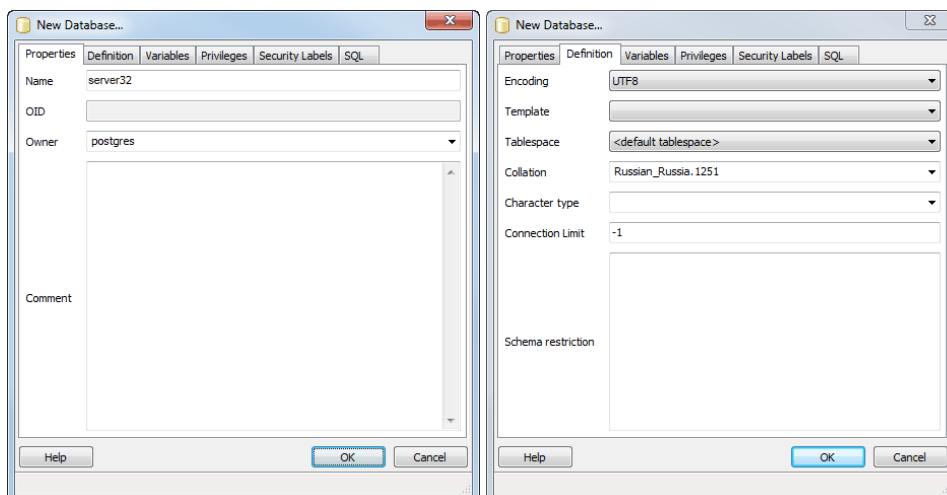
As the backup is created, messages will be displayed in the window. If the backup is created successfully, then **Process returned exit code 0** should appear last. Otherwise, verify the settings described above and repeat the process to create a backup.

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

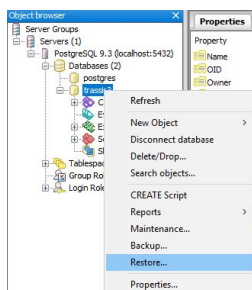


4. In the window that opens, in the **Properties** and **Definition** tabs, enter the parameters just as they appear in the images below:



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.

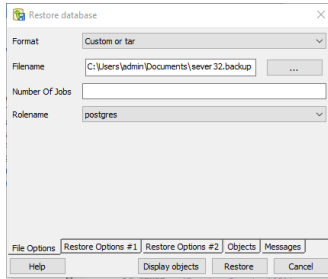
5. Select in the tree the newly created database and select **Restore...** in the context menu



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

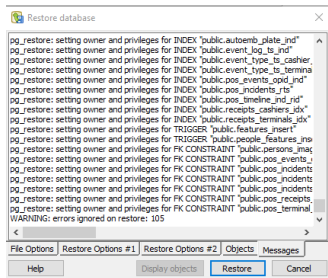
- In the **Format** field, select **Custom or tar**;
- In the **Filename** field, enter the path to the previously saved backup;
- Leave the **Number of Jobs** field unchanged;

- 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](#).



- [Database connection settings](#)

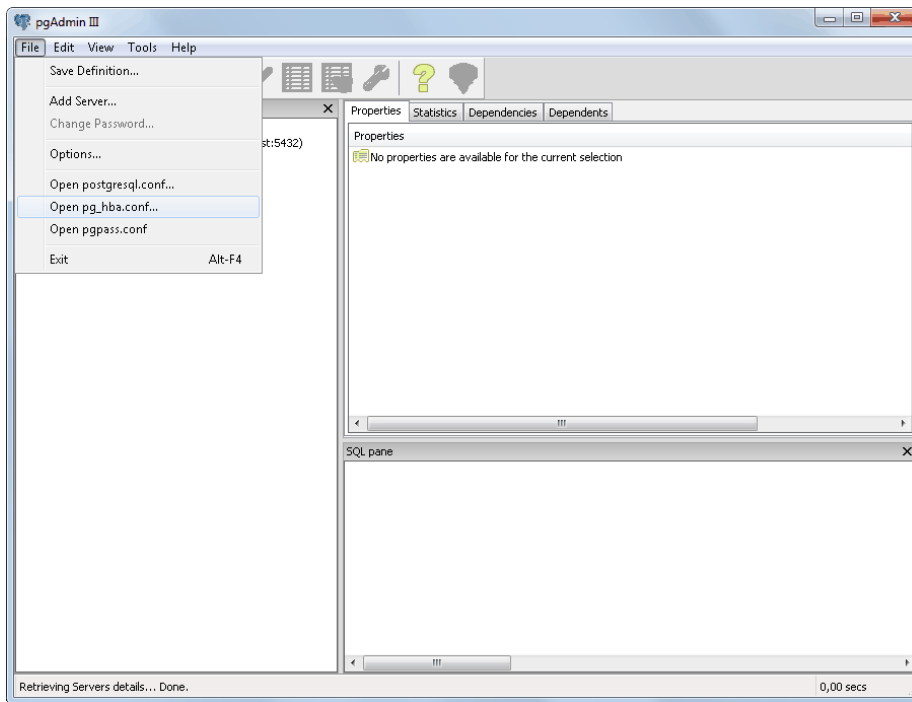
Allowing external connections to the PostgreSQL DBMS

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

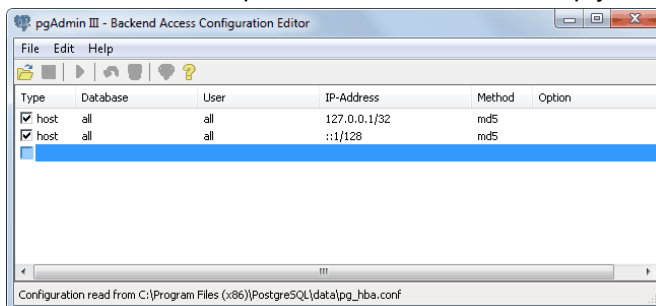
The file `pg_hba.conf` is located in `C:\Program Files (x86)\PostgreSQL\<version number>\data`. You can edit it in any text editor or with the pgAdmin utility.

To configure external connections using the pgAdmin utility:

1. Run the pgAdmin utility.
2. In the **File** menu, select **Open pg_hba.conf...**

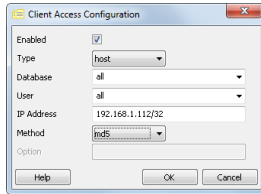


3. Select `pg_hba.conf` to configure the external connections.
4. In the window that opens, double-click in the empty checkbox for adding a new authorized connection.



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).

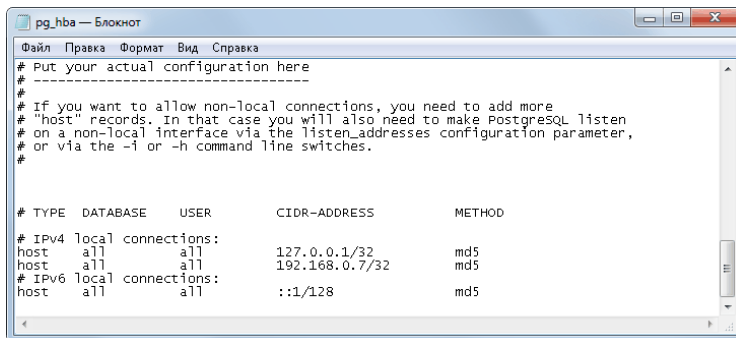


All addresses correspond to a "zero" subnet mask (signified by /0). A specific IPv4 address corresponds to a subnet mask with a 32-bit prefix (signified by /32).

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).

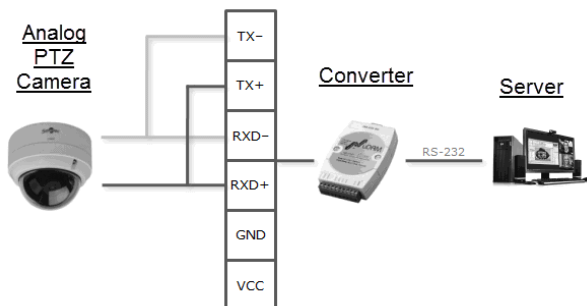
PTZ cameras have an RS-485 control interface. This interface can control video cameras at a distance of up to 1200 m in full-duplex mode when connected with a 4-wire cable, or in half-duplex mode - when connected with a 2-wire cable.

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.

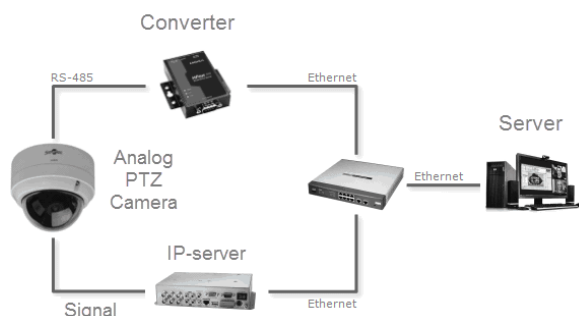


2. **Connecting using a network converter.** A network converter connects directly to the local network and has its own IP address, which must be bound to the server's serial port.

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.

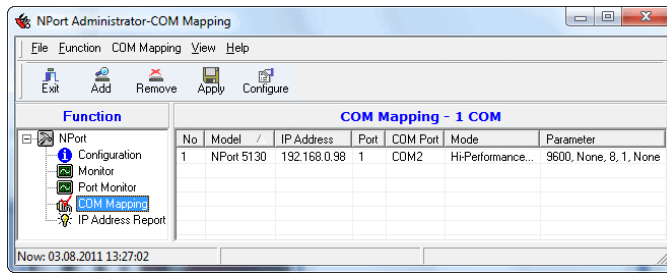
Connection procedure:

- 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*

Configuration of the software server version in Astra Linux SE 1.7 for operation with neural network detectors



For correct GPU operation in **Astra Linux SE 1.7** operating system, it is necessary to uninstall old drivers and install new ones by downloading them from the vendor's website.

For the software server version to operate with neural network detectors, it is necessary to configure the OS. To do this:

1. Download the Nvidia driver from the [official website](#).
2. Disable the Nouveau drivers. To do this, create a new configuration file:

```
sudo vi /etc/modprobe.d/blacklist-nouveau.conf
```

Add the following strings into it:

```
blacklist nouveau
options nouveau modeset=0
```

Save the file changes and update with the command:

```
sudo update-initramfs -u
```

3. Install the Nvidia driver using one of the selected options:

- **Without closed software environment**

Restart the server in non-GUI mode. To do this, enter the following commands and restart the server.

```
sudo systemctl set-default multi-user.target
```

Open the folder where the driver was downloaded and start the driver installation:

```
sudo chmod +x NVIDIA-Linux-x86_64-xxx.xxx.run && ./NVIDIA-Linux-x86_64-xxx.xxx.run
```

Upon successful driver installation, return the GUI:

```
sudo systemctl set-default graphical.target
sudo systemctl reboot
```

Rename xorg.conf file

```
sudo mv /etc/X11/xorg.conf /etc/X11/xorg.conf.`date +%s`
```

- **With closed software environment**

Restart the server in non-GUI mode. To do this, enter the following commands and restart the server.

```
sudo systemctl set-default multi-user.target
```

Open the folder where the driver was downloaded and unzip the driver archive:

```
sudo chmod +x NVIDIA-Linux-x86_64-xxx.xxx.run && ./NVIDIA-Linux-x86_64-xxx.xxx.run -x
```

The **NVIDIA-Linux-x86_64-xxx.xxx** folder will appear next to the driver. Sign all *.so files and all executables in the root directory of this folder.

Start the driver installation:

```
sudo ./nvidia-installer
```

The error message will appear at the end of the installation: **DIGSIG:[ERROR] MODULE VERIFICATION FAILED.**

To fix the error, you need to sign the assembled nvidia-*.ko modules located in:

```
/usr/lib/modules/`uname -r`/kernel/drivers/video/
```

In order to verify correct installation, run:

```
sudo nvidia-debugdump -D
```

If the command output is empty, the installation is successful.
Upon successful driver installation, return the GUI:

```
sudo systemctl set-default graphical.target  
sudo systemctl reboot
```

Rename xorg.conf file

```
sudo mv /etc/X11/xorg.conf /etc/X11/xorg.conf.`date +%s`
```

4. Install the libraries necessary for neural network detectors operation.

Create an empty folder and run the command:

```
wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu1804/x86_64/  
libcublas-11-1_11.2.1.74-1_amd64.deb  
https://developer.download.nvidia.com/compute/cuda/repos/ubuntu1804/x86_64/cuda-  
cudart-11-1_11.1.74-1_amd64.deb  
https://developer.download.nvidia.com/compute/cuda/repos/ubuntu1804/x86_64/  
libcufft-11-1_10.3.0.74-1_amd64.deb  
https://developer.download.nvidia.com/compute/cuda/repos/ubuntu1804/x86_64/  
libcurand-11-1_10.2.2.74-1_amd64.deb  
https://developer.download.nvidia.com/compute/cuda/repos/ubuntu1804/x86_64/  
libcusolver-11-1_11.0.0.74-1_amd64.deb  
https://developer.download.nvidia.com/compute/cuda/repos/ubuntu1804/x86_64/libnpp-11-1_11.1.1.269-1_amd64.deb  
https://developer.download.nvidia.com/compute/cuda/repos/ubuntu1804/x86_64/cuda-  
nvrtc-11-1_11.1.74-1_amd64.deb  
https://developer.download.nvidia.com/compute/cuda/repos/ubuntu1804/x86_64/  
libcudnn8_8.1.0.77-1+cuda11.2_amd64.deb  
https://developer.download.nvidia.com/compute/machine-learning/repos/ubuntu1804/x86_64/  
libnvinfer7_7.2.1-1+cuda11.1_amd64.deb  
https://developer.download.nvidia.com/compute/machine-learning/repos/ubuntu1804/x86_64/libnvinfer-  
plugin7_7.2.1-1+cuda11.1_amd64.deb  
https://developer.download.nvidia.com/compute/machine-learning/repos/ubuntu1804/x86_64/  
libvonnxparsers7_7.2.1-1+cuda11.1_amd64.deb
```

After downloading all the packs, enter the command in this folder:

```
sudo dpkg -i *.deb
```

5. Reboot the server

```
sudo reboot
```



In order to use neural network detectors for software operation in Astra Linux SE 1.7 in closed program environment mode, all libraries must be signed.

The process of signing libraries is described in the OS knowledge base:

- [Create embedded signature in ELF files for CSE mode](#)
- [Packet signing](#)
- [A scenario to perform DLL file signing and signature verification](#)

Working with the basic interface

- *Start the software and sign into the system* - This section describes the first launch procedure and how to log 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 includes the server and the client parts.

You can sign in to the system locally on the server, or remotely using another server, client, or Web interface.

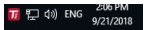
- The Guardant USB-key connected to the server and the license file are required to run the server.
- Running the client application does not require a USB key or license.



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

The software can be run in two modes: in regular mode and in "no restart on failure" mode.

- **As usual** - start the **watchdog-vc142.exe** file from the root folder). In this case, a dedicated module - *Watchdog* will monitor the server status.
- In **"no restart on failure" mode** -run **t1server-vc142.exe** or **t1client-vc142.exe** from the root folder).

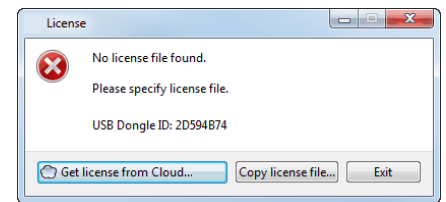


If the program launched successfully, the main control panel icon will be displayed in the top part of the screen and icon availability in the task panel.



- *First server launch*
- *System login*
- *Main control panel*

First server launch

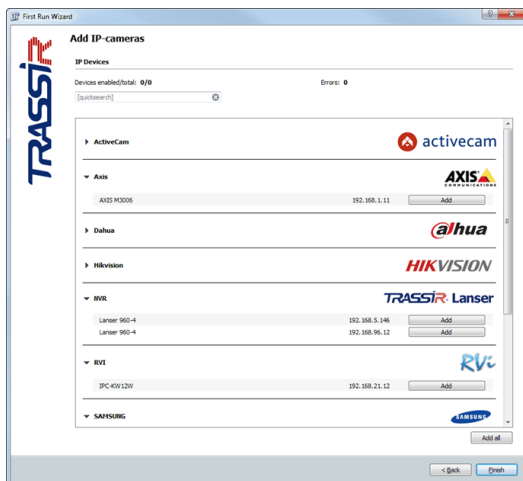


The first time you start the server, you will see a license file selection window.

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

After that, the server will start 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 runs, check the **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 the server, monitor its status, and restart it in case of critical failures. The Watchdog settings are stored in `watchdog-t1server.config`(`watchdog-t1client.config`) file.

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-vc142`; for the client it is `t1client-vc142`.
- `keepalive` - is the main parameter of the watchdog settings. In case the watchdog module does not receive information about the software status within this period, it will be forced to restart. The value of this parameter must be greater than 60 seconds for the software to work properly.
- `executable-arguments` - additional settings for internal use.
- `log` - the name specified in this parameter will be assigned to the log file when the software is terminated by the watchdog module.



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



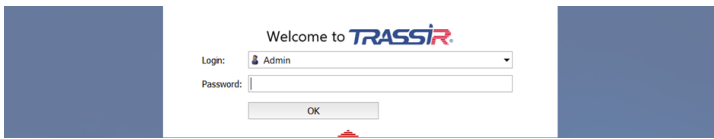
In order to run the watchdog module on a server with **Astra Linux SE 1.7** OS, run the command:


```
/opt/vms/tech1/run_watchdog.sh
```



- *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.

The administrator password in TRASSIR OS and in the server version installed as a Windows service is **12345**.

The administrator of the server, installed as a Windows application, does not have a password.

The **Admin** and **Operator** users on **Astra Linux SE 1.7** OS servers have no passwords.



For security reasons, change the user passwords. For more information about working with users, see [Users](#).

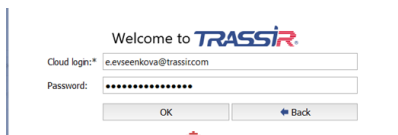
Log in for TRASSIR Cloud system users

TRASSIR Cloud service users can also log in.

To do this:

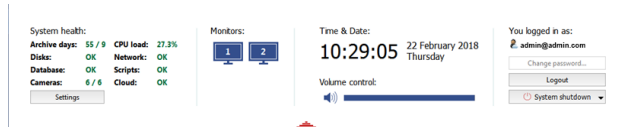
- server needs to be connected with the cloud user account (see section [Connecting server to TRASSIR Cloud](#));
- account user is allowed to access to this server (see [Guidance on TRASSIR Cloud](#)).

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 server launch*
- *Main control panel*

Main control panel



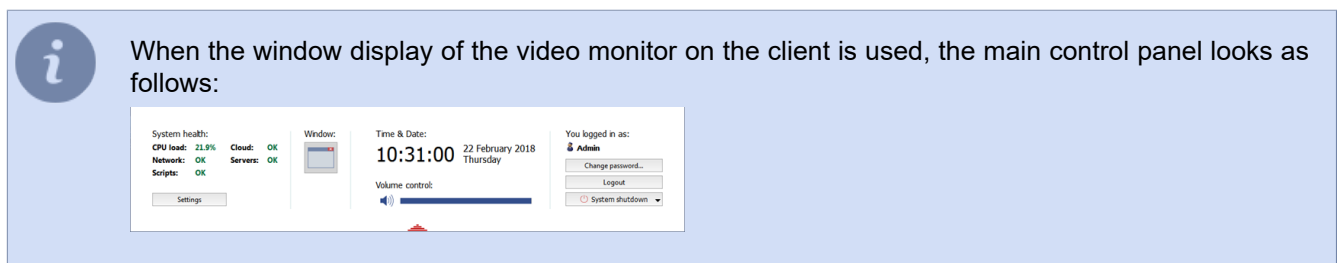
After signing in, the main control panel is grouped as follows:

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" (???)

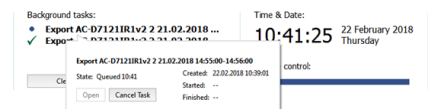
The **Settings** button - opens the **settings window**.

2. The **Monitors** group - the button to show / hide the operator interface. If several monitors are connected to the computer system unit, then there will be several icons for hiding / showing the interface (each monitor has its own interface).

After installation, the operator interface is hidden. Click on the monitor image to display. Click one more time to hide the video monitor interface again. You can read more about working with the monitor interface in the "Operator's Guide" (???)



3.



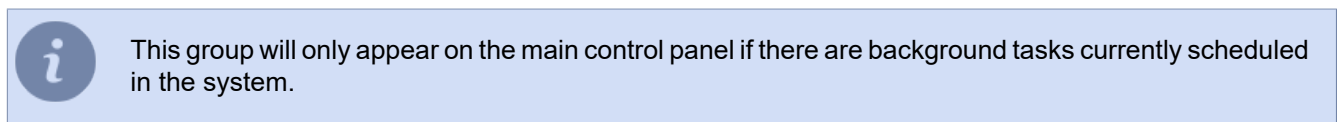
The **Background tasks** group shows a list of tasks whose execution has been postponed. The delayed export of an archive is an example of such a task.

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.

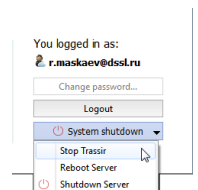
The **Clear** button removes all completed tasks from the list.



4. The **Time & Date** - group displays the server's system date and time.

Volume - use the slider, to adjust the overall volume of the sound.

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.



After changing the **Admin** user password, the **Limited Functionality Mode** will be enabled on the server.
Read more about this mode in [License](#).



If the server was started in "no restart after failure" mode, then when the **System shutdown** button is clicked, the dropdown menu will not be shown. Instead, the software will be closed.



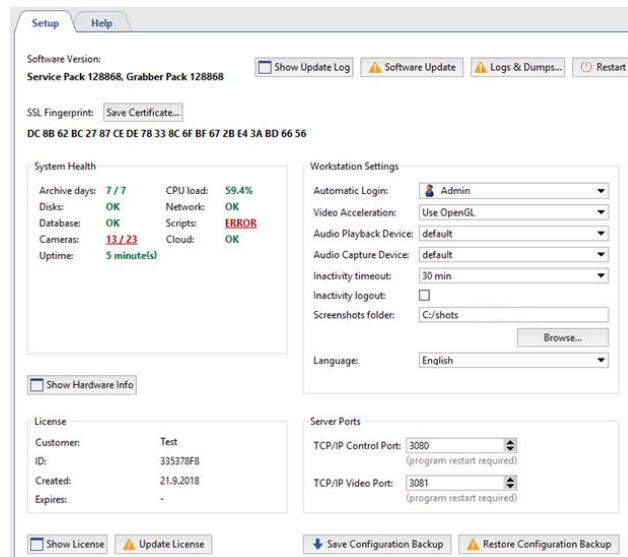
- [Start the software and sign into the system](#)
- [Settings window](#)
- [Video monitor](#)

Settings window

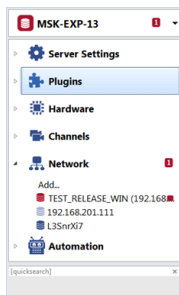
The administrator can configure all parameters of the server operation in the **Settings** window. All server settings are represented as an object tree. However, other servers can also be objects of the settings tree - just set up a network connection to them, and you can configure them remotely.



A remote server configuration is possible only in case the account being used for connection has the *necessary rights*. Remember that each 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.

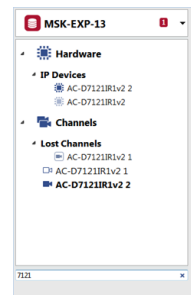


In case certain menu entries have errors in the settings, they will be automatically highlighted.

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.

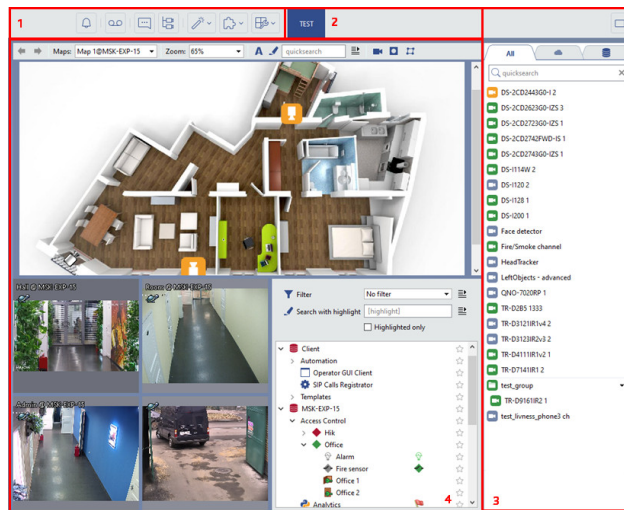


You can check the description of all server settings in the following sections: [Settings](#) and [Plugins](#)









- [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

You can start working after the server installation immediately. That is, the settings made during *installation of the server* and at *first launch* are already enough to work the server.

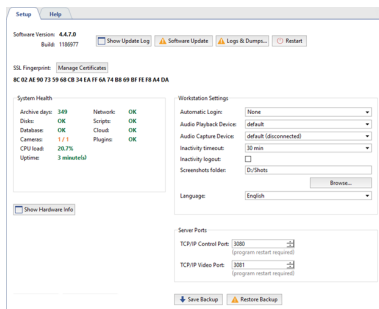
However, to extend the basic server capabilities, you need to perform additional server settings:

- *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 servers*;
- *create rules and scripts* to automate the server.

Moreover, due to *additional plugins* you can significantly expand the basic server functionality.

Local server settings

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



- **Software version** is the current version of the software, which consists of the Service Pack number - the main module version, and Grabber Pack number - the version of the IP camera and video capture cards drivers.

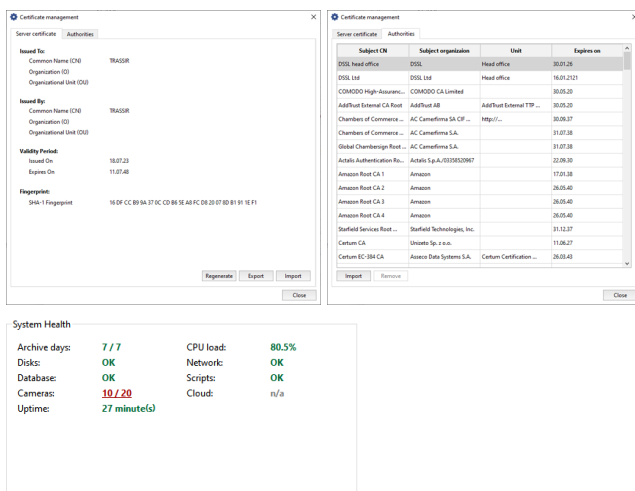
Buttons:



- **Update log** displays the log of installed Service Pack and Grabber Pack updates.
- **Software Update** is intended to update the software modules and drivers of IP cameras without reinstalling the software. After the update, the server will automatically restart. For a detailed description of the feature, please refer to [Software update](#).
- **Logs & dumps...** opens a server system files selection window to be sent to the technical support service. For a detailed description of the feature, check [Logs and dumps](#).
- **Restart** is intended for the server operational reloading (**Software**) or the whole server (**Hardware**) from the administrator's interface.

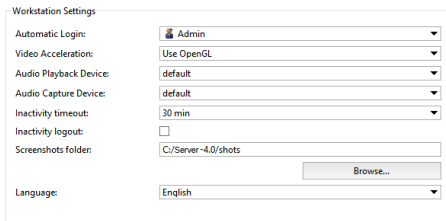
SSL certificate fingerprint - every server has a unique identifier to verify it while connecting to the network. Press **Manage certificates** to:

- **Regenerate** the current **Server certificate** used to create secure connection to other servers (see [Connecting to a new server](#)).
- Use **Export** and **Import** buttons on the **Server certificate** tab to save it on your HDD or upload to server.
- Press **Import** on the **Authorities** tab to upload your certificate to create secure connection to other devices.



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:

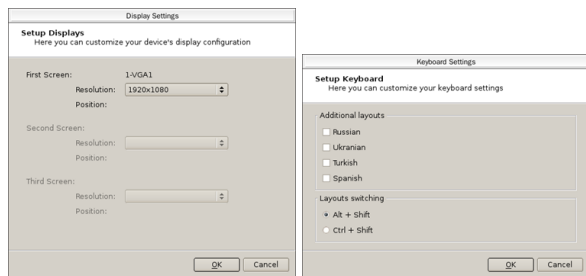



- **Automatic Login** indicates the username for the account that will be used to sign in to the server when launching. The default value is "None", e.g. a username and password are required to sign in to the server.
- **Video Acceleration** - "OpenGL" or "DirectDraw". Specify the value that is best 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 during which the operator wasn't using the operator interface in his work. Set the **Inactivity logout** flag. Upon the selected time expiration, the screen will display a warning that the current session will end in 60 seconds and the time 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: None

Audio Playback Device: default

Audio Capture Device: default

Inactivity timeout: 30 min

Inactivity logout: ☐

Language: English

Hardware acceleration: ☐

Display Setup... Keyboard Setup...

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:	3080 <small>(program restart required)</small>
TCP/IP Video Port:	3081 <small>(program restart required)</small>

Server ports:

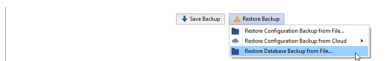
- **TCP/IP Control Port** - The server control port.
- **TCP/IP Video Port** - The video broadcast port.

Buttons:

- **Show Hardware Info** - Displays the OS version and the server's hardware configuration.
- **Save Backup** - you can save your system configuration or system database backup copy any time and save it as a file or to the TRASSIR Cloud.
When you save the configuration to a file, a text file of settings is created `_tlserver.settings`, which is located in the installation folder by default.
When you save the database, a file is created `*.dump`.



- **Restore backup** - allows you to restore the system configuration or database from a previously created backup.

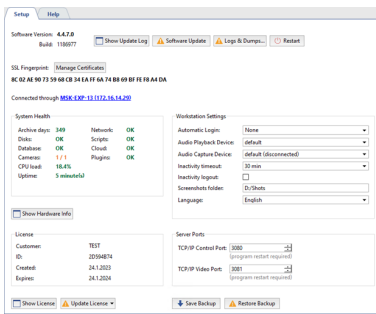


You need to reboot the system, after loading the database from a file.
Learn more about saving backup copies to TRASSIR Cloud in [Connecting server to TRASSIR Cloud](#).



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

Remote server settings



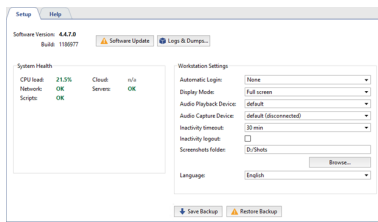
The main settings window for a remote server displays the same information as that for *local server settings*.



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 the software, which consists of the main modules' version number (Service Pack).

Buttons:

- **Software update** is intended to update server/client modules and IP camera drivers without reinstalling the software. On update's completion, the server/client will restart automatically. See detailed description in the [Software update](#).
- **Logs & dumps...** opens a server system files selection window to be sent to the technical support service. For a detailed description of the feature, check [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 client. The default value is "None", e.g. a username and password are required to sign in to the server.
- **Video Acceleration** - "OpenGL" or "DirectDraw". Specify the value that is best for the video card being used.
- **Display mode** - select the way to display the operator interface: in a separate window or on the full screen.
- **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 during which the operator wasn't using the operator interface in his work. Set the **Inactivity logout** flag. Upon the selected time expiration, the screen will display a warning that the current session will end in 60 seconds and the time countdown will start.

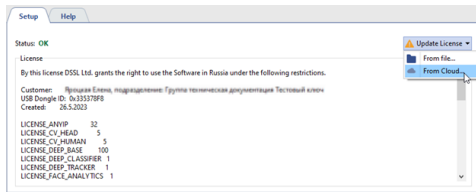


In case **Inactivity logout** box is not checked, notification does not appear. Operator's inactivity can be traced with audit (see section [Audit](#)).

- **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.

License

This section lets you view and manage server license. Click **Update license** to select a new server license file. It may be required, for example, when expanding the system.



There are several ways to update a license:

- **From file...** - a license file upload window will open.
- **From cloud...** - a license file will be uploaded from cloud storage directly.

Operation of server in limited functionality mode

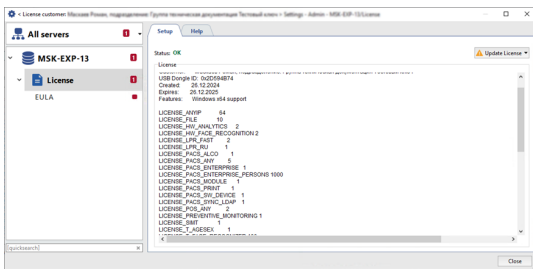
Limited functionality mode is a server operation mode in which some of the user functions are limited, such as:

- all server settings are unavailable (except for **License** and **EULA**);
- watching archive and video from channels is unavailable on server;
- no access to the operator interface.



Specifics of server operation in **limited functionality mode**:

- The server continues to operate with all current settings (channels are running, archive recording is in progress, analytics modules detect events, automation scripts are running, etc.). The server operation time in this mode is unlimited.
- When connecting a client to a server running in this mode, there is also no access to server settings, operator interface, archive and video from channels.
- When connecting a client version 4.4.x or lower to a server running in this mode, an error message is displayed in the connection settings.

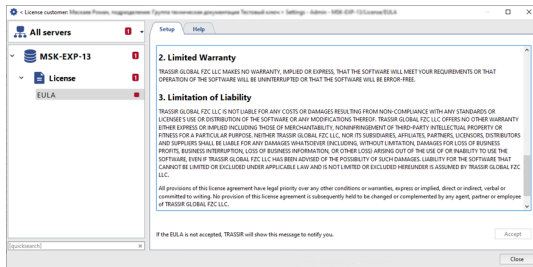


A **limited functionality mode** is enabled on server after the following user actions:

- license file update;
- changing password of the **Admin** user;
- updating software to the version in which the **License Agreement** was changed.

EULA

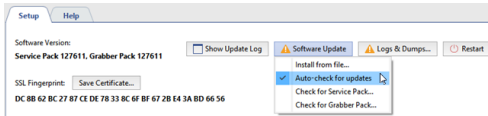
To access all server features, you need to read the license agreement and confirm it by clicking **Accept**.



Software update



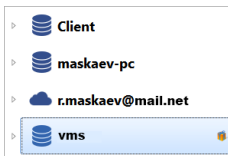
You can update the server software either locally or remotely, by *connecting to the server* via the client.



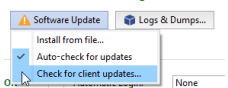
The **Software Update** feature allows you to update the server software and IP device drivers. Select one of the items to check for the updates:

- **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.

In addition, you can download the update file from *our website* yourself and update the server manually. In this case, select **Install from file...** and specify the update file.



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

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



In order to update software in **Astra Linux SE 1.7** OS, it is necessary to uninstall and then install server software. You can find a detailed description of procedures in *Installation and uninstallation of the software server version in Astra Linux SE 1.7*.



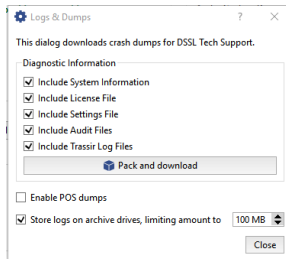
- *Local server settings*
- *Remote server settings*
- *Client settings*

Logs and dumps

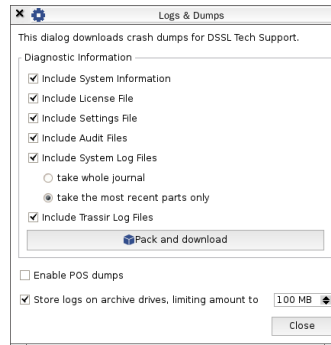
All server actions are recorded in the log. In the case of the software crash, dumps with information about the failure are created on disk. This function collects and prepares all necessary information, using which the technical support staff can find the cause of the failure and offer recommendations for its elimination.

The list of items to select depends on the operating system:

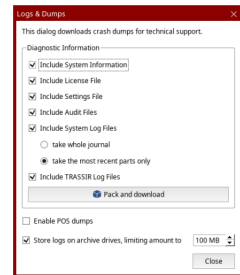
Windows



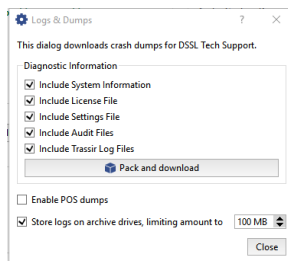
TRASSIR OS



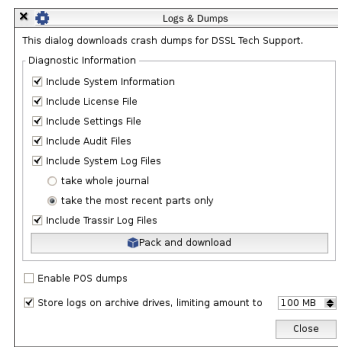
Astra Linux SE 1.7



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*

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, the **TRASSIR Cloud** is the network-attached storage of the license files and 4.x version server settings, which in case their loss can be recovered in the cloud. It will allow returning server in operating status in a few minutes.



If you don't have a TRASSIR Cloud account yet, create one using [our cloud service](#). See functions and capabilities of the cloud service in details in [Manual on TRASSIR Cloud](#).

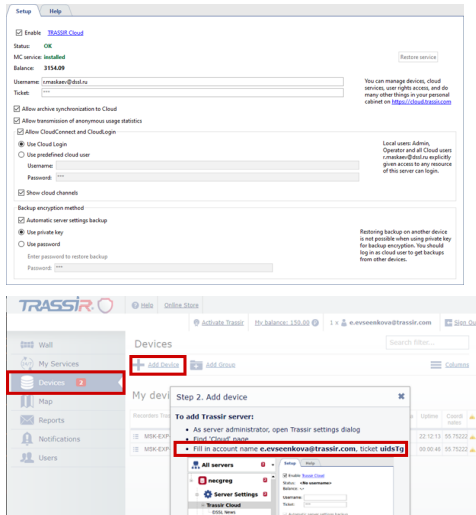


- [Connecting server to TRASSIR Cloud](#)
- [Client connection to TRASSIR Cloud](#)

Connecting server to TRASSIR Cloud



If you don't have a TRASSIR Cloud account yet, create one using [our cloud service](#). Read more about the features and capabilities of a cloud service, see the [Guideline for TRASSIR Cloud](#).



Before connecting to the TRASSIR Cloud cloud service, make sure that the **Activate cloud** box is checked. Type in **User name** and **Ticket**. The 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.



In **TRASSIR for Windows**, the **MC service** field displays the status of the Monitoring Center service. For more information about starting it, see [Starting the MC service on Windows](#). In **TRASSIR OS**, the Monitoring Center is integrated directly into the operating system.



To display server status information transmitted by the Monitoring Center to the cloud, the corresponding service must be enabled. For details, see [Guideline for TRASSIR Cloud](#).

Each server, which is connected to the cloud, keeps a backup of its settings. Set the **Automatic server settings backup** flag and the server will save the configuration settings file in the cloud (`_tlserver.settings`) and the license file (`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](#).

In order to access the cloud channels and users, you should link the server with your cloud account. To do this, set the **Import users and channels from Cloud** flag, and select the one of the methods to connect to the cloud:

- **Use Cloud Login** - in this case, you need to sign in to the server with the cloud user that has the server added to the list of available devices. In addition, you'll get 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 the **Show cloud channels** box to display cloud camera channels in the list of connected devices. The cloud cameras operation depends on the tariff of their connection to the TRASSIR Cloud. See details on restrictions in [Cloud cameras](#) section.

The **Backup Encryption Method** block lets you configure secure storage of your server settings cloud backup and ensure that they can be quickly restored in case of system failures:

- Set the **Automatic server settings backup** flag to automatically save the current server settings to the cloud storage.
- Set the **Use private key** flag to encrypt the backup copies of settings stored in the cloud. Using the private encryption keys provides an additional protection level against unauthorized access and prevents the saved backup from being restored to other devices.
- You can set a password to restore the backup for additional protection of the saved settings. To do this, set the **Use password** flag and enter the password in the corresponding field.



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

Starting the MC service on Windows

MC service is a Monitoring Center (MC) service that collects and processes hardware status data using the server's internal services. All server status data is sent by the MC Service to the TRASSIR Cloud cloud service.

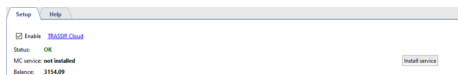


Key features of starting and operating the **MC service**:

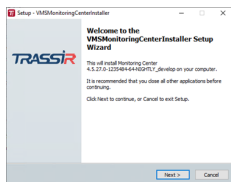
- The service must be installed under an account with administrator privileges.
- The service operates automatically without requiring additional configuration or regular updates.

To start the MC service, follow these steps:

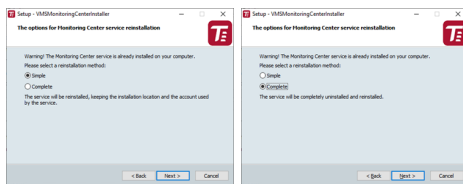
1. In the server settings, open the **Cloud** tab and click **Install Service**.



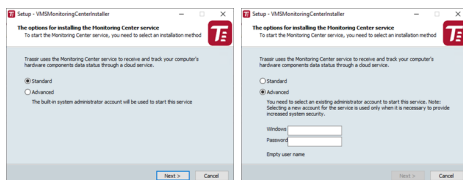
2. Click **Next** in the installation wizard.



3. Select the service installation option and click **Next**.

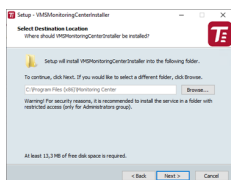


4. If the **Complete** option is selected, choose the installation mode in the next wizard window: **Standard** or **Advanced**, then click **Next**.

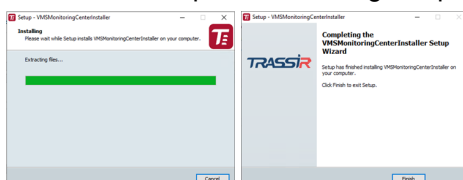


In **Advanced** mode, enter the administrator account credentials under which the service will operate. In **Standard** mode, the current OS user account is used.

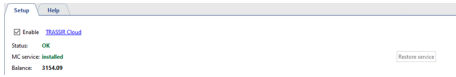
5. Select the installation folder by manually specifying the path or using the **Browse** button, and click **Next**.



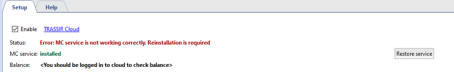
6. The installation process will begin. Upon completion, click **Finish**.



7. After a successful installation, the status of the **MC service** will change to **installed**.



If errors occur in the operation of the MC Service, an error message will appear, and the **Restore service** button will become available. Clicking this button will launch the installation wizard.



Client connection to TRASSIR Cloud



If you don't have a TRASSIR Cloud account yet, create one using [our cloud service](#). See details on cloud service functions and capabilities in the [TRASSIR Cloud Guide](#).

Make sure that **Activate Cloud** box is checked, before connecting to TRASSIR Cloud cloud service. Select one of the ways to access cloud devices:

- **Access to any cloud account devices**

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 the **Bind to cloud user** field is blank, a user will receive the rights of the client's administrator after the authorization.

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

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**

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

The **Backup Encryption Method** block lets you configure secure storage of the client settings cloud backup and ensure that they can be quickly restored in case of system failures:

- Set the **Automatic server settings backup** flag to automatically save the current client settings to the cloud storage.
- Set the **Use private key** flag to encrypt the backup copies of settings stored in the cloud. Using the private encryption keys provides an additional protection level against unauthorized access and prevents the saved backup from being restored to other devices.
- You can set a password to restore the backup for additional protection of the saved settings. To do this, set the **Use password** flag and enter the password in the corresponding field.



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

Cloud cameras

Cloud cameras work with some limits, which depend on the connection tariff.

Feature	Basic	SD standard	HD standard	HD+ standard
Live video watch	3 minutes	10 minutes	30 minutes	60 minutes
Archive review	3 minutes	10 minutes	30 minutes	60 minutes
Archive export Maximum fragment length	10 minutes	10 minutes	3 hours	3 hours

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



The **View archive** and **Archive export** features on cameras with the **Base tariff** use the camera built-in archive. If there is no built-in archive, these features are not available.



- [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.

The work of the archive has a number of features that should be considered when building a video surveillance system, such as:

- TRASSIR can also work without an archive. In this case you will be able only to watch live video in the system, without saving it to disk.
- TRASSIR can't use the system partition to record the archive.
- 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.

the 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 record buffer. If the buffer is consumed and there are still insufficient resources, an error message will appear and a 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*](#)

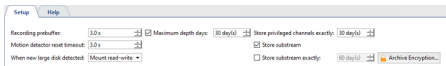
Archive setup on the server



This section contains the information on the archive setup on 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** is the size of the video buffer in seconds (from 0 to 10 seconds). A buffer of the indicated size will always be stored in memory. When an event occurs, the buffer is appended to the associated video. This lets the operator later review 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 the software 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 the archive files, they will be available 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 of two video streams coming from devices: the main stream and the additional stream (substream). Since the additional stream is generally several times smaller than the main stream, recording it substantially increases the archive depth without changing the required disk space. Moreover, using the sub stream significantly lowers network bandwidth requirements when 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.

- **Maximum depth days** allows you to set the archive depth for all channels.
- **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](#)).

You can use [encryption of video recordings](#) in order to prevent unauthorized access to an archive. To configure encryption, click **Archive encryption...**

Disk	Enable	Read only	Capacity	Current State
D1	<input type="checkbox"/> Enable	<input type="checkbox"/> Read only	663.51 GB	0.00 MB/s, 0 errors
E1	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Read only	1176.42 GB	0.00 MB/s, 0 errors
F1	<input type="checkbox"/> Enable	<input type="checkbox"/> Read only	1068.02 GB	0.00 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, it will be labeled as "Not suitable" in the list. You will not be able to use such a disk for the archive recording. But if it contains the archive files, then it will be displayed in the list and marked as "Read-only".

New mount point - adds any folder for subsequent use of its disk space by the archive. Adding a new mount point may be useful if, for example, you need to view the 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 as [lost channels](#).



Do not merge archive disks of different servers or disks of the same server connected at different time. This may result in the entire archive incorrect operation.

Archive statistics	Merge statistics
Main Stream: 346.12 GB / 47.3 Days ~ 11.97 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: 0.00 GB / 0.0 Days ~ - 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.

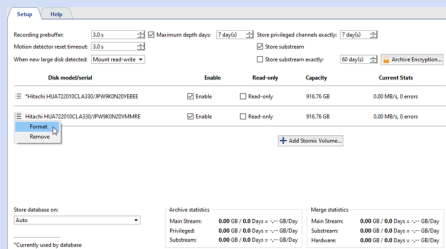


The archive of 4.0 version supports gradual upgrade of the archive from 3.1 version. The entire archive from the older versions will be available as *lost channels* and will be erased as the new archive is written.



TRASSIR OS and **Astra Linux SE 1.7** have some differences in the archive setting menu, such as: **TRASSIR OS** has some differences in the archive settings menu. That is:

- **TRASSIR OS** does not have a *New mount point* setting, which means you won't be able to mount an arbitrary folder to the archive;
- in **Astra Linux SE 1.7** the *New mount point* setting is used to connect NAS (the NAS configuration is described in *NAS Setup*);
- you can run *Format* command from the context menu, which will delete old records of the 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 database on. The selected disk in the list of archive disks will be marked with (*').



- *Archive*
- *Encrypting an archive*
- *Selecting the number of disks for an archive*
- *NAS Setup*
- *Recording network channels*
- *Lost channels*

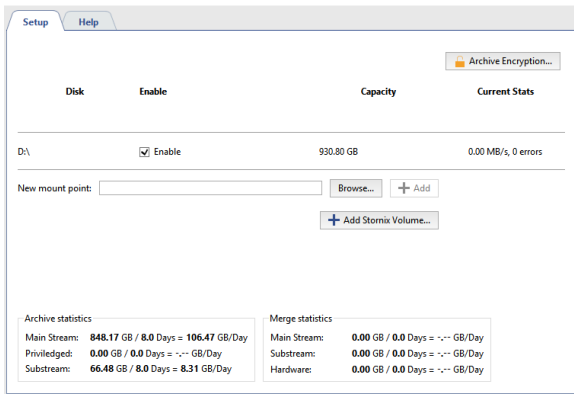
Archive setup on the client



This section contains the information on the archive setup on 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 the archive files, check **Enable** to view them.

New mount point - adds any folder for subsequent use of its disk space by the archive. Adding a new mount point may be useful if, for example, you need to view the 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 as **lost channels**.



Do not merge archive disks of different servers or disks of the same server connected at different time. This may result in the entire archive incorrect operation.

Archive statistics	Merge statistics
Main Stream: 348.12 GB / 8.0 Days = 116.71 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: 0.00 GB / 0.0 Days = --- GB/Day	Hardware: 0.00 GB / 0.0 Days = --- GB/Day

You can **encrypt stored video data** in order to prevent unauthorized access to the archive. Press **Archive encryption...** to set up.

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.



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

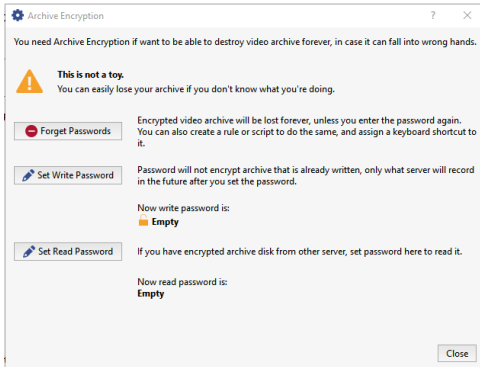


- *Archive setup on the server*
- *Selecting the number of disks for an archive*
- *Lost channels*

Encrypting an archive

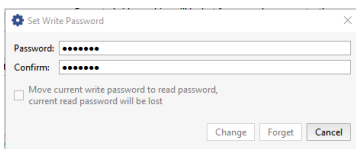


The improper use of the archive encryption feature may result in the permanent loss of an archive. We recommend that you contact our technical support before using this feature.



TRASSIR does not use archive encryption by default. That is, an archive stored on one server may be freely transferred and viewed on a different server.

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

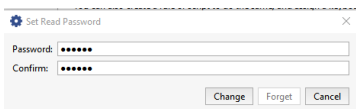


The portion of the archive saved before encryption was enabled will be stored in unencrypted form. The entire portion of the archive recorded after the password is set will be encrypted. Moreover, archive encryption in no way affects the current operation of the server, i.e. all archive operations will 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.

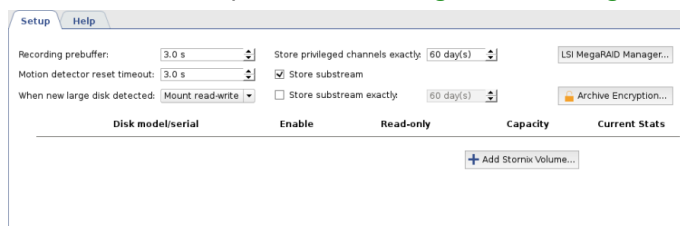


To create and set up RAID on **UltraStation** servers a **MegaRAID** utility is used, which is embedded into TRASSIR OS.

You can download the utility from www.broadcom.com and run on any PC, if necessary.

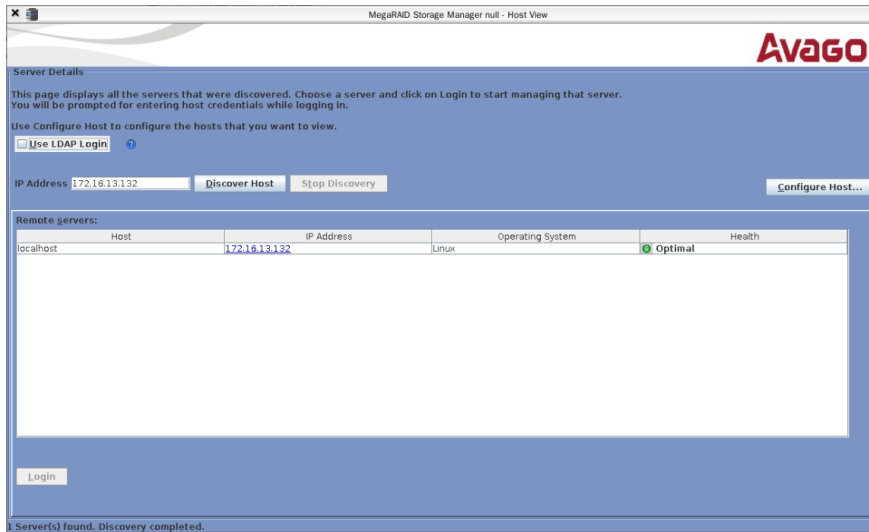
To start the utility:

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

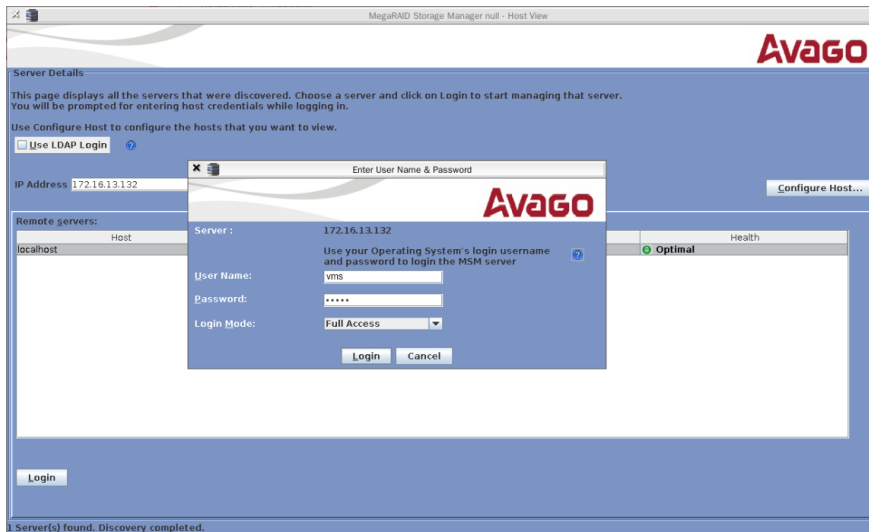


RAID Creation

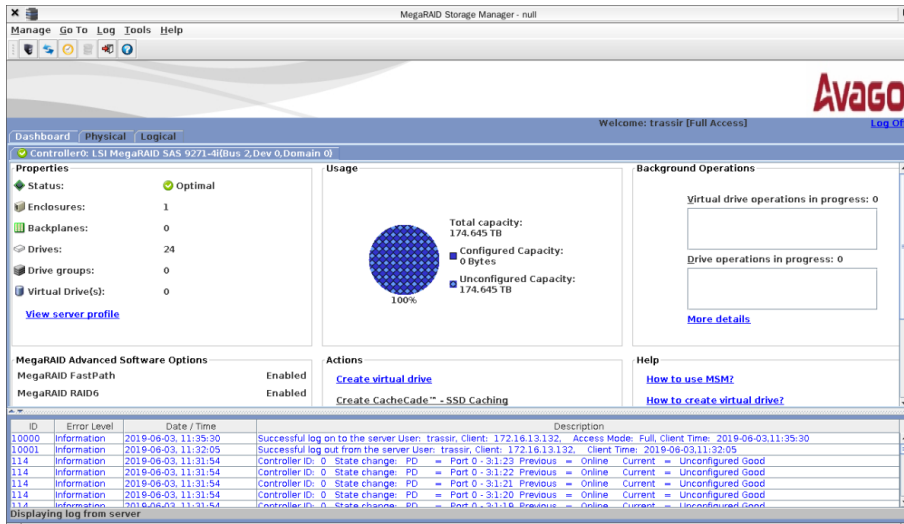
1. Enter server IP address into **IP Address** field and press **Discover Host** button.
The found server will be displayed in the **Remote servers** list.



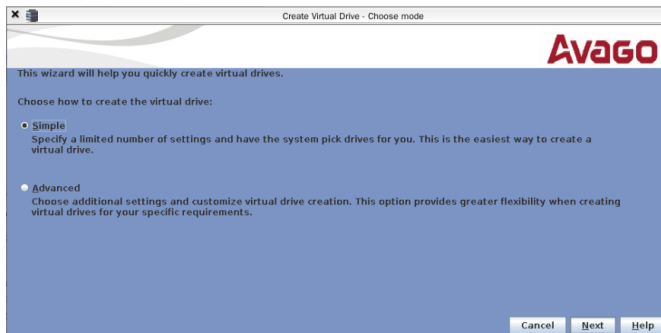
2. Select the server from the list to connect and press **Login**. In the opened window:
 - in the **User Name** field enter **vms**;
 - in the **Password** field enter the **Administrator** user password (12345 by default);
 - in the **Login Method** field select the **Full Access** connection mode.



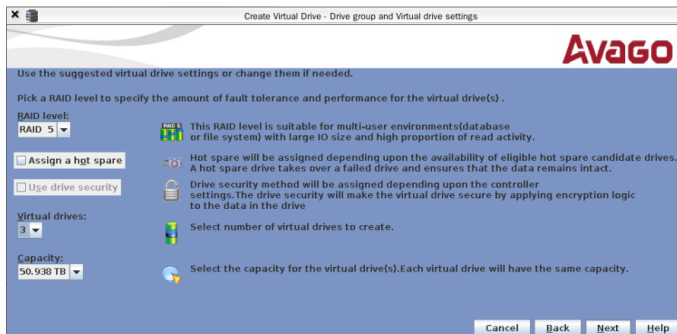
3. After the connection establishment click the **Create virtual drive** link on the **Dashboard** tab.



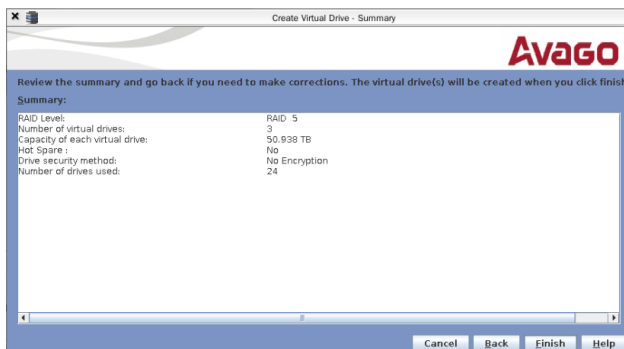
4. Select **Simple** and press **Next** to continue.



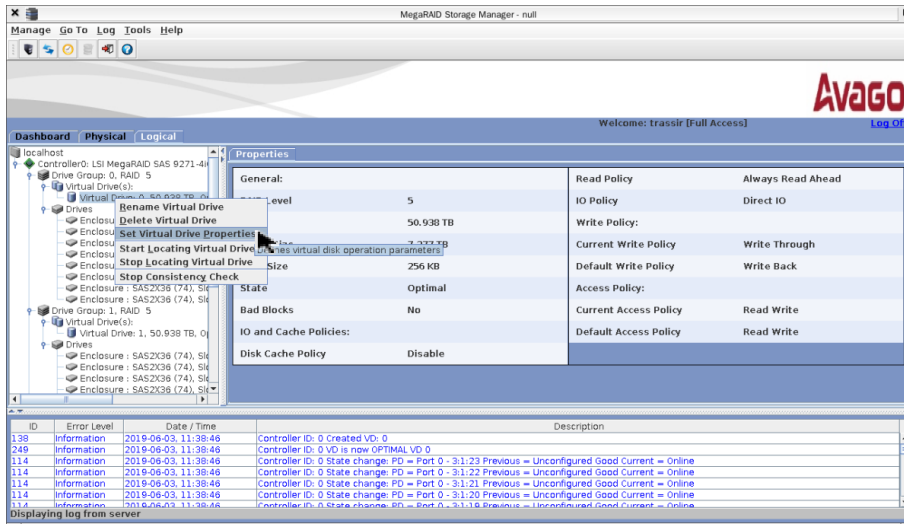
5. After that in the **RAID level** field select the RAID level (RAID 5 by default). In the **Virtual drivers** field select the amount of the virtual drives. Press **Next** to continue.



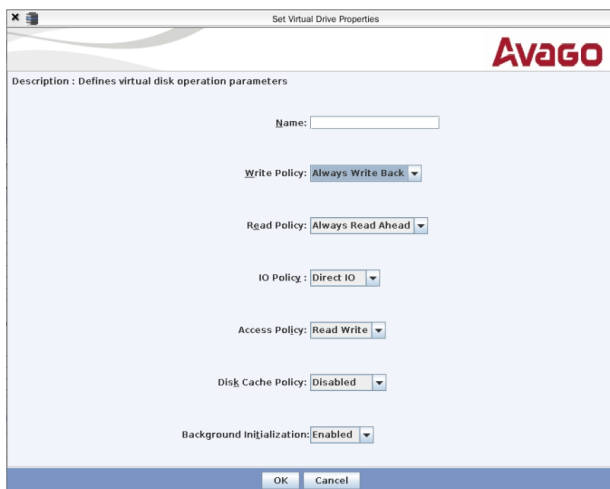
6. Press **Finish** to complete.



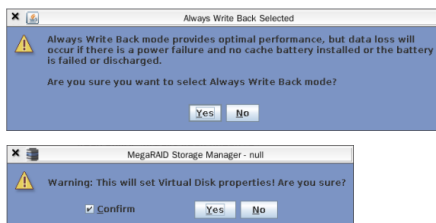
7. Open the **Logical** tab and then with the right click on the virtual drive select the **Set Virtual Drive Properties**



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.

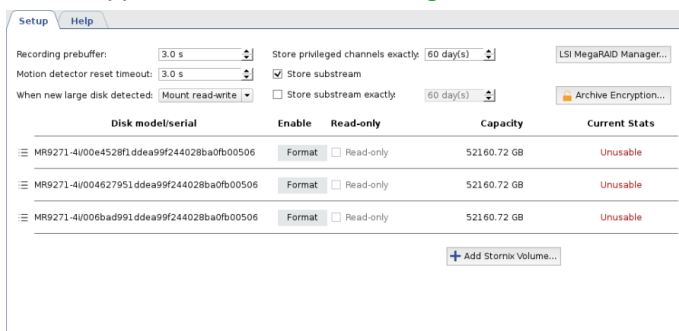


After that, in the notifications displayed, press **Yes**, then check the **Confirm** mark and press **Yes** once more.



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 on the **Server settings** -> **Archive** tab.



The drives will become available for use after the formatting.

SetupHelp

Recording prebuffer: 3.0 s

Store privileged channels exactly: 60 day(s)

LSI MegaRAID Manager...

Motion detector reset timeout: 3.0 s

☒ Store substream

When new large disk detected: Mount read-write

☐ Store substream exactly: 60 day(s)

Archive Encryption...

Disk model/serial	Enable	Read-only	Capacity	Current Stats
MR9271-4/00e4528f1ddea99f244028ba0fb00506	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Read-only		51952.97 GB	0.00 MB/s, 0 errors
MR9271-4/004627951ddea99f244028ba0fb00506	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Read-only		51952.97 GB	0.00 MB/s, 0 errors
MR9271-4/006bad991ddea99f244028ba0fb00506	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Read-only		51952.97 GB	0.00 MB/s, 0 errors

+ Add Storix Volume...



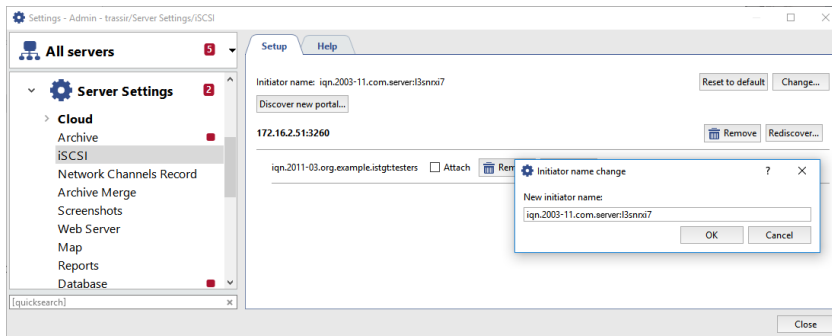
- [Archive](#)
- [Archive setup on the server](#)
- [Encrypting an archive](#)

Configuring a network storage connection in Linux-based TRASSIR OS

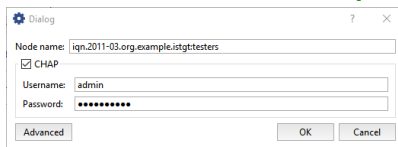


The description of this feature is intended to be used in the Linux-based TRASSIR OS. All network storage hard drives that will be used to store the archive must be formatted to the EXT4 file system.

In order to configure server connection to the network storage via iSCSI, go to the iSCSI tab and click the **Change** button, if necessary, and enter an **Initiator name**. This name will be displayed in the network storage's log when the server connects to it.

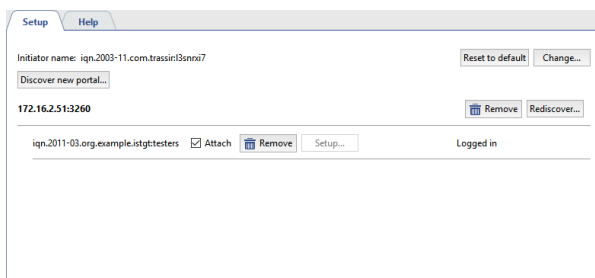


Then click the **Discover new portal...** button and enter the settings for the portal being connected to:

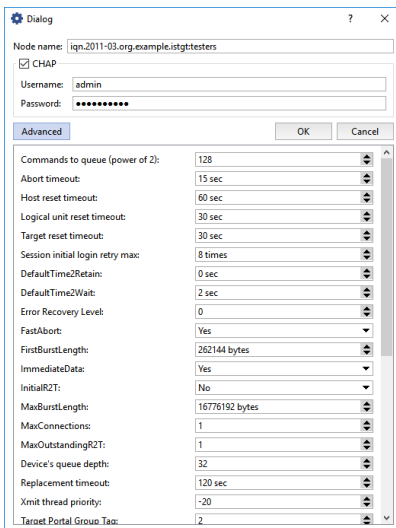


- **Portal** - The IP address or DNS name of the portal being connected to.
- **Port** - The iSCSI port, *configured in the network storage*.
- If you entered CHAP authentication parameters when configuring the network storage, set the **CHAP** checkbox and enter your username and password.
- Click the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

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



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.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 the server to the 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 on the **Archive** tab.



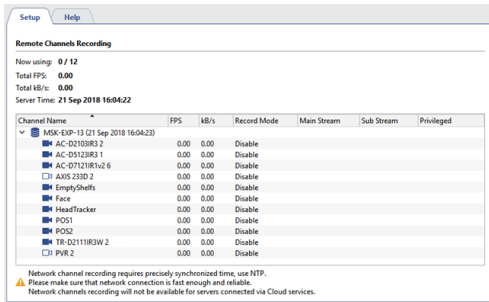
- [NAS Setup](#)
- [Configuring a QNAP Turbo NAS](#)
- [Connecting a network storage in a Windows OS](#)
- [Archive setup on the server](#)

Recording network channels

The server version of the software supports recording of an archive from devices connected to another server as if these devices were connected directly to it.



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)	0.00	0.00	Disable			
AC-02103R3 2	0.00	0.00	Disable			
AC-05123R3 1	0.00	0.00	Disable			
AC-07121814 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			
POST	0.00	0.00	Disable			
TR-Q211183W 2	0.00	0.00	Disable			
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.

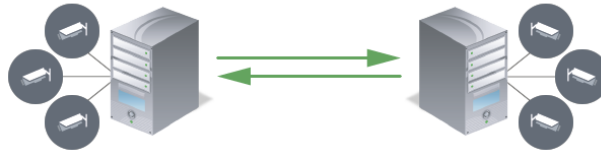


- [Archive setup on the server](#)
- [Archive](#)
- [Lost channels](#)

Archive merge

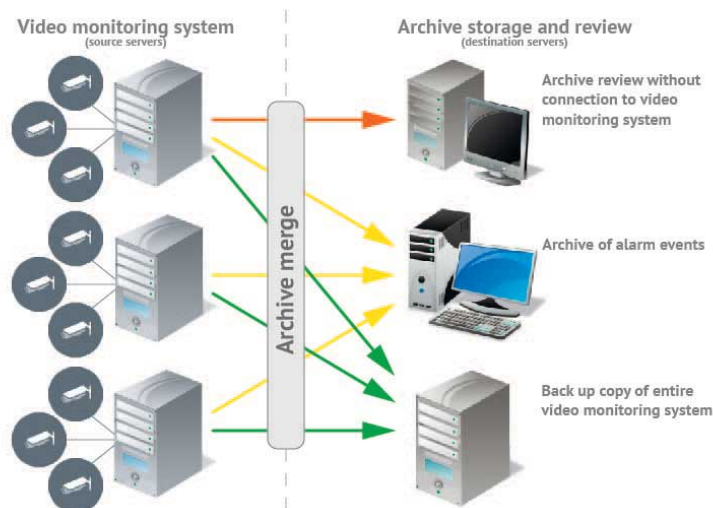
Archive merge - is a unique technology, allowing to share an archive from a server to which the video surveillance devices are connected, and which has the archive record set up, to one or several other servers.

Merging archives of two servers



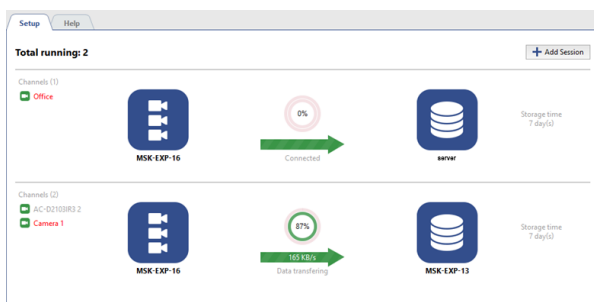
The purpose of the archive merge:

- **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.** There is no need to search for an archive fragment with a particular event captured. You can configure the server to mark a fragment as an armed one. The archive merge will allow you to copy all these fragments to any server, where you can review and analyze them.



Settings highlights:

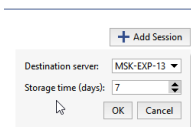
- Archive merge is activated and configured on the source server.
- The amount of the channels that can be uploaded to the destination server is defined by the quantity of licenses on it.



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*



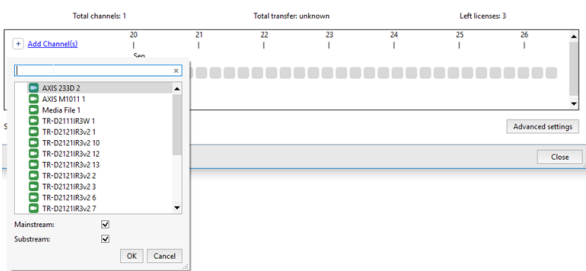
- *Connecting to a new server*

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.

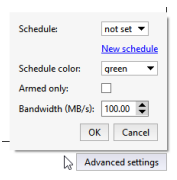


The number of channels added to the session is defined by the number of licenses on the destination server. The number of remaining licenses is displayed in the **Left licenses** field.



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.

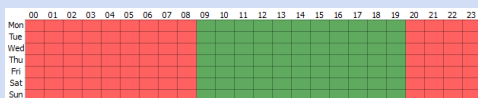


It will let you:

- **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.

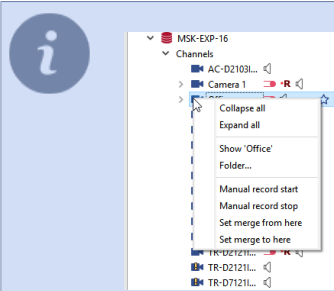


Usually the archive merge is set up at the least loaded time of the day, i.e. at night (red area).



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

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



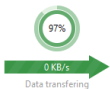
You can mark the recorded archive as armed:

- **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.

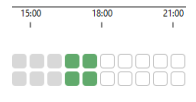
- **Set the merge speed.** In the **Bandwidth (MB/s)** field set the maximum value.



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.



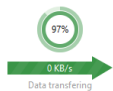
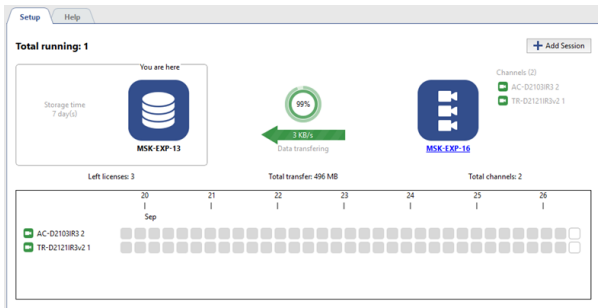
- [Archive merge](#)
- [Connecting to a new server](#)

Reviewing the archive merge session on the destination server

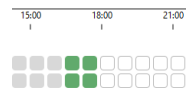
The archive merge session settings page on the destination server looks exactly the same as [on the source server](#). This page does not allow any configuration, it shows the info on the **Archive merge** operation.



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

The software supports saving frames (screenshots) while viewing live video, as well as when working with the archived recordings. There are many ways to take a screenshot: the operator can do it 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 with the help of SDK.

There is a special module for working with screenshots. It lets you view captured frames as well as copy them to removable drives (including exported video archives), and delete them. When connecting to another 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 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 server in the browser.

SDK is a set of tools for interaction with TRASSIR. It makes it easy to integrate third-party applications with server functionality. You can read more about features in [???](#).

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 SDK](#)
- [Access to TRASSIR WEB interface](#)

Configuring a server to work with the SDK

Check **SDK** flag to enable access to 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 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 **Allow access from browser** flag to enable. Click the link next to the flag and the WEB-interface will open. Read more about connecting to server from the browser in [Access to TRASSIR WEB interface](#).



Check the **Redirect from port 80** box to use only the server IP address in the browser address bar to access the WEB interface.

Access to TRASSIR WEB interface



The following ports are used to connect to the WEB interface by default:

- **8080** and **80** are main and additional ports of access to access WEB-interface. You can modify the main 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.

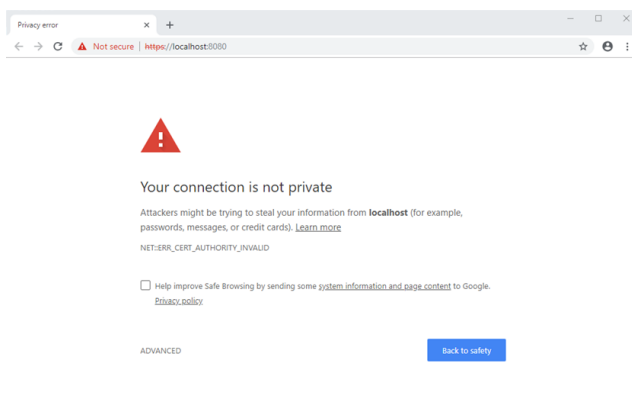
Follow the next steps to connect to the WEB interface:

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



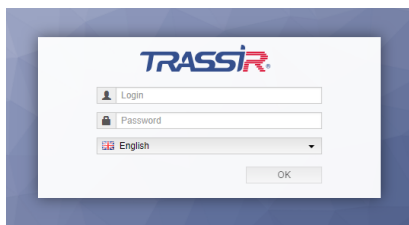
In case the **Redirect from port 80** box is checked in the settings, you can use only the server IP-address to log in, for example, <https://192.168.1.201>.

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



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

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



4. You can start the work after that!



- *Configuring a server to work with the SDK*

Map

You can 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 on a server, each of which will cover, for example, a floor of a building or a group of rooms.

Follow the next steps to add a map:

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 objects to the map*. After creating a map, you need to place various objects on it (cameras, access control system devices, automation scripts, floor area, etc.). Placing objects on the plan allows you to simplify the perception of information and in case of an event (for example, movement), you know exactly where in the building it occurred.
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.

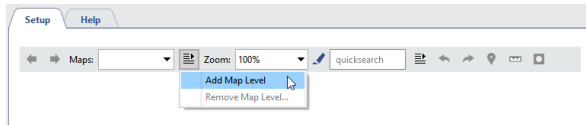


- *Creating a map*
- *Adding objects to the map*
- *Adding teleports*

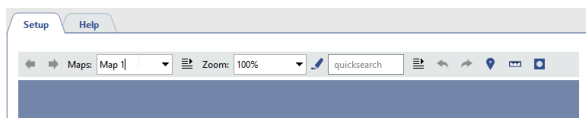
Creating a map


To create a map:

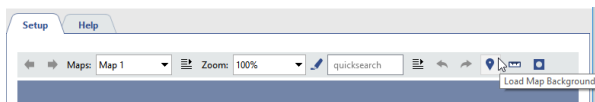
1. Click **Map** in the server settings.
2. Expand the **Maps** dropdown list and select **Add Map Level**.



3. Enter a name for the new map.



4. To upload image press the button .



5. Select the image file.



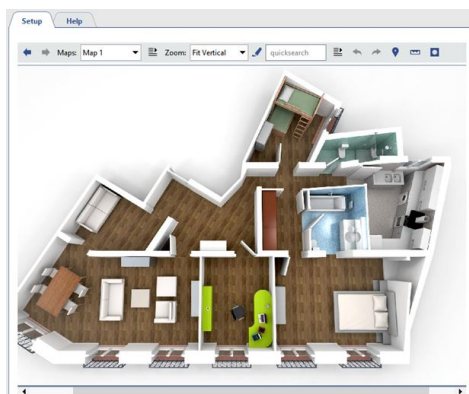
Set the image compression settings in the **Format** and **Dimensions** fields.




Choose the image file considering the following:




- The max. size of the image file is 10 MB.
- If the overall size of all uploaded maps exceeds 10 MB, the **Automatic server settings backup** function is disabled (see [Connecting server to TRASSIR Cloud](#)).

6. The uploaded map appears in the Setup window:





To blur the background press . The blurred background makes the objects and teleports stand out more distinctly on the image.

The buttons ,  and  are used to add various objects to the map. See [Adding objects to the map](#) and [Adding teleports](#).

Adding objects to the map

You can add the following interactive objects to the *created map*:

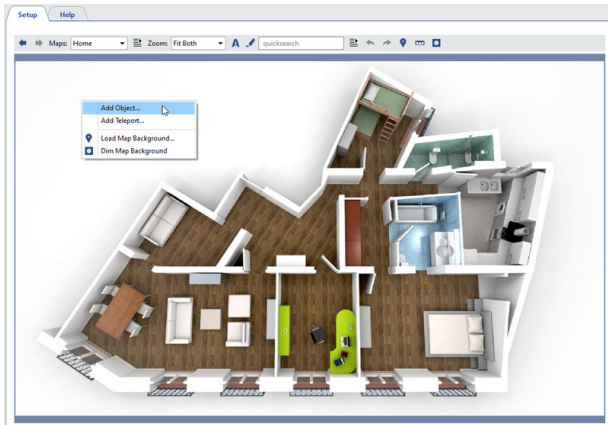
- **camera channels**;
- **Access Control devices** (including *TRASSIR ACS devices*);
- **floor areas**;
- **"Automation" module elements (scripts, rules, schedules)**;
- and other CCTV objects.



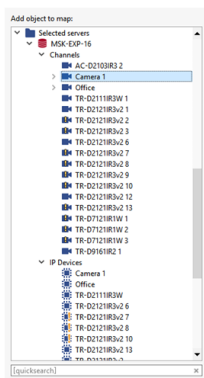
You can add the **Floor area** to the map only after its creation and calibration. Read more in *Floor mapping settings*.

Follow the next steps to add an object to the map:

1. Right-click anywhere on the map and choose **Add object** in the context menu.

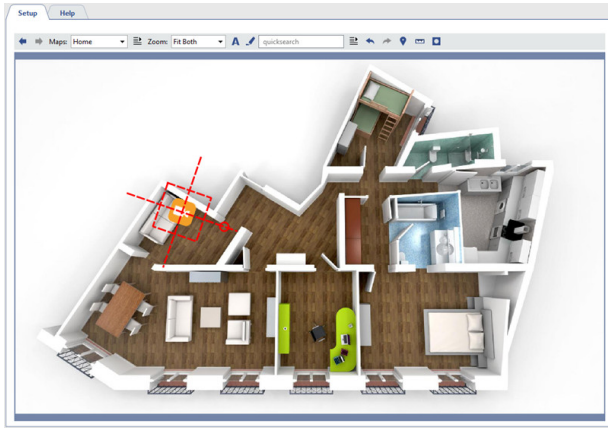


2. In the opened window, select the object to add to the map.




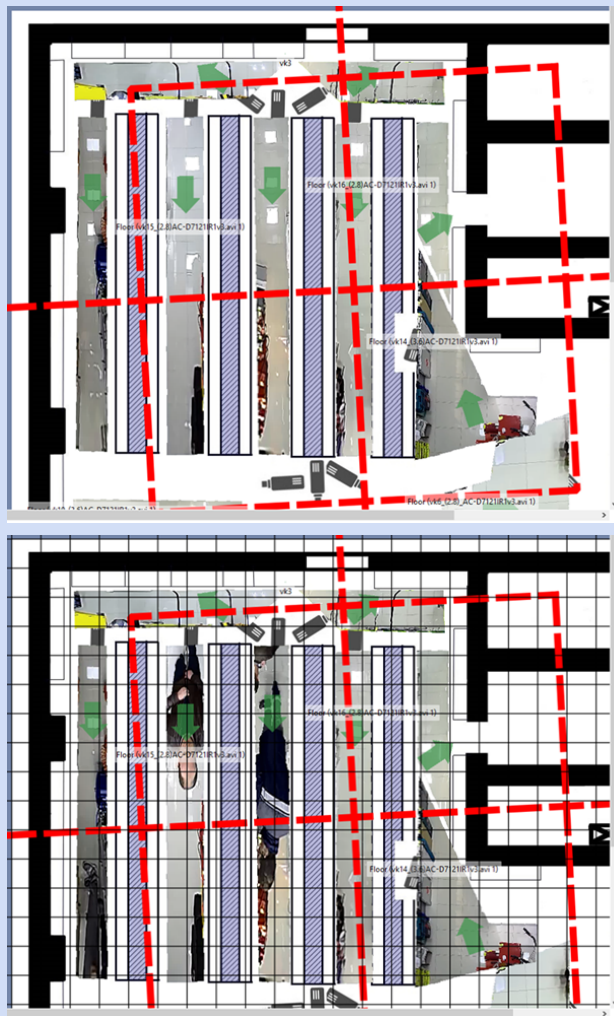
3. Place the object to the required spot on the map.

In order to rotate an object or zoom in/out, click on the red circle and change the angle or scale of the object on the map.



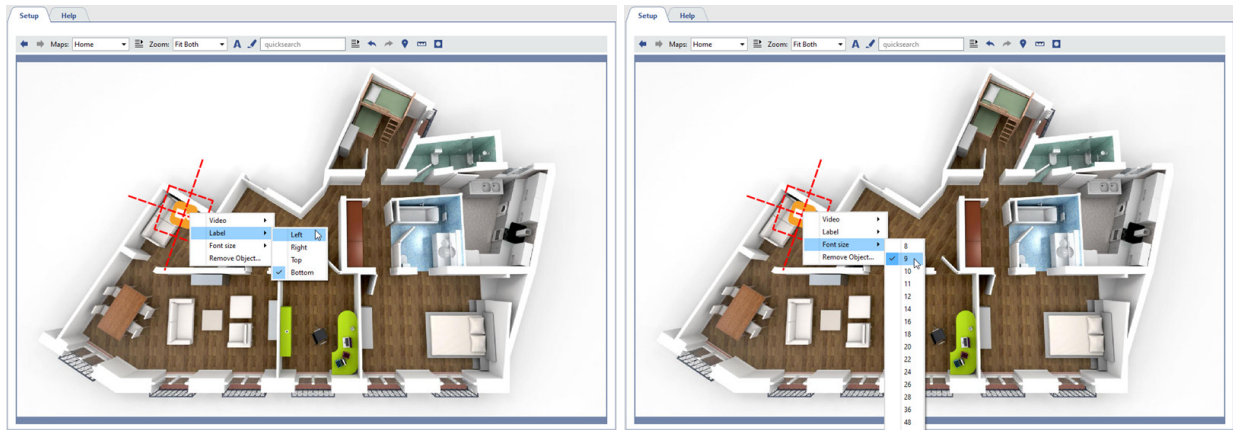
While adjusting the position of the **Floor area** object on the map, you should change the rotation angle and dimensions so that the area with the image coincides with the plan on the map.

In order to adjust the position of the **Floor area** object on the map more precisely, click  and using the grid and the **Pixels per meters** setting, adjust the image scale. The grid lines on the image are placed in intervals of 1 meter.



4. Select the display option for the label next to the object. To do this, select the object, right-click and, in the context menu that opens, select **Label** and the display option.

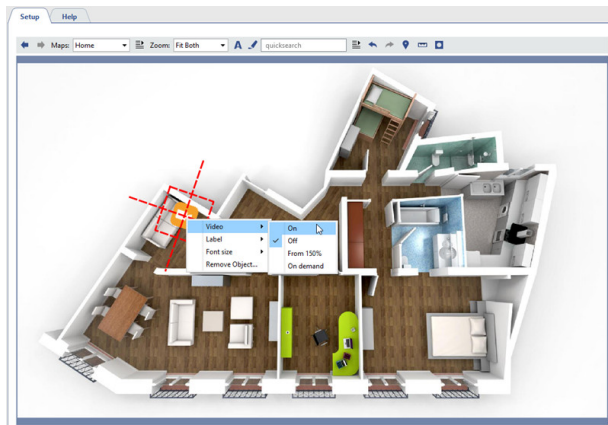
In order to set the font size of the label, select **Font size** and set the desired size.



The labels next to the objects are hidden by default. To display them, click **A**.

5. Depending on the object type, configure additional display options:

- Configure video parameters for the **Channel** object:



"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.

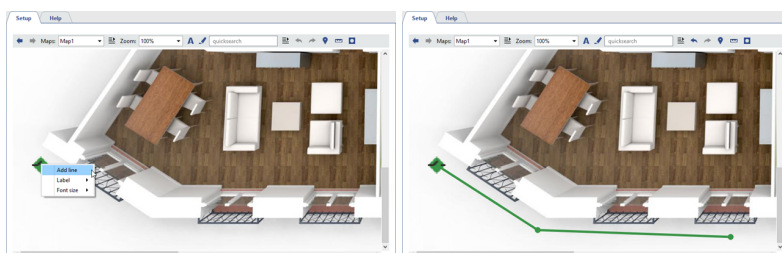
"On demand"—if videos are only need to be opened on demand by double clicking the channel icon.




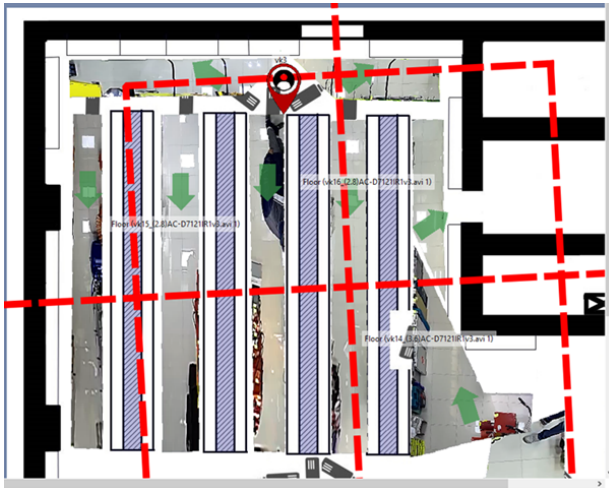
After making your selection, the video display area will be shown. If desired, you can change the area's size and location on the map.

- You can add a line on the map for the **Alarm input** object. If the alarm input state changes, the line will also change its color.

To add a line to the map, select **Add Line** and set the points through which it will pass. To finish drawing the line, put the cursor on the last point and double-click the left mouse button.



- You can change the size of the marker that shows the location of the person on the map for the **Floor area** object. To do this press , and adjust the **Person marker size**.

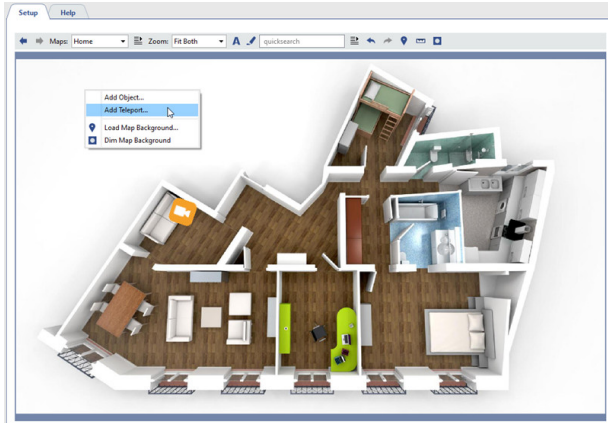


- *Creating a map*
- *Adding teleports*

Adding teleports

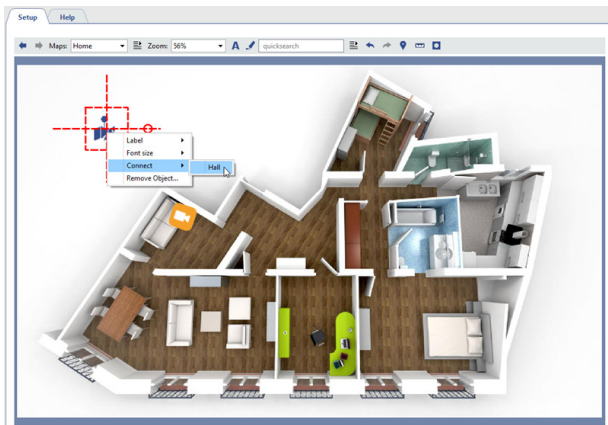
To add a teleport:

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



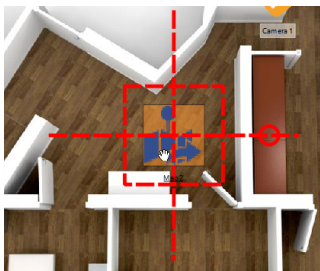
3. Link a teleport to the map that will be displayed when the teleport is selected. To do this:

- 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:

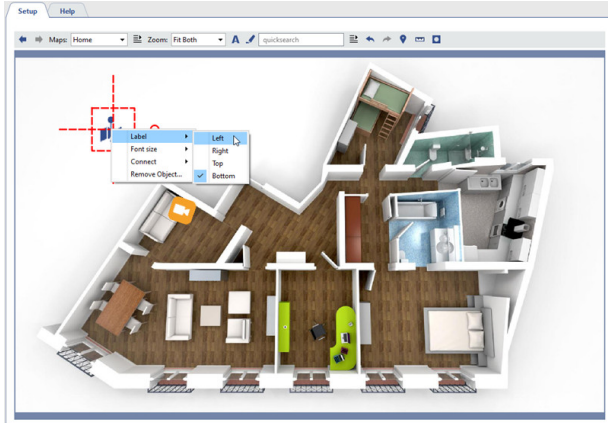
- Left-click with the mouse to select the teleport.
- Without releasing the mouse, drag the teleport to the desired location on the map.



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.

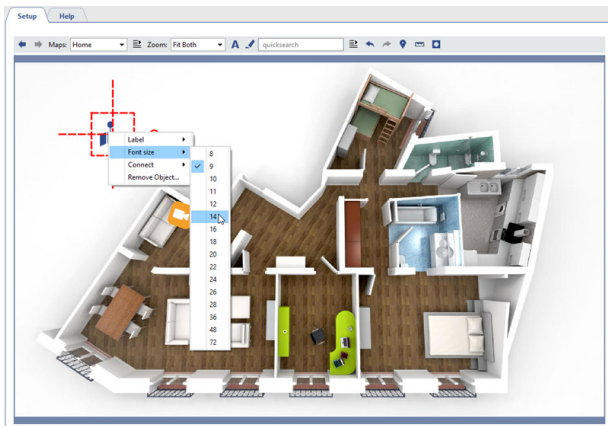


The currently selected option will be marked with a checkmark.

By default, the labels next to the objects are hidden. To display the labels, click **A**.

6. Set the font size of the text next to the teleport icon. To do this:

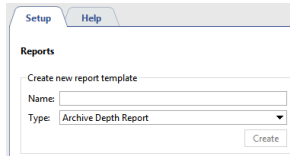
- Point the cursor at the teleport icon and right-click.
- Use **Font size** item in the opened context menu to set the required size. You can select the font size for each object, added to the map.



- *Creating a map*
- *Adding objects to the map*

Reports

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



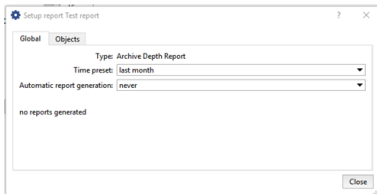
To start, you must create a report template. Enter template name, select a report type, and click **Create**. The [report template settings window](#) will open automatically.



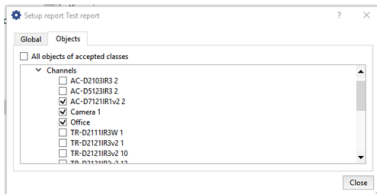
- [Report template settings](#)

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.

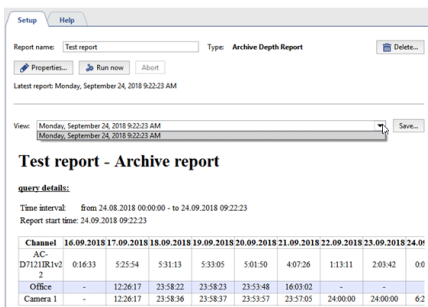


- Objects - The list of channels whose data should be used to generate the report. By default, all channels are used to create the report, but you can build a report using only the channels that interest you. To do this, clear the **All objects of accepted classes** checkbox on the **Objects** tab and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



7. Close the **Setup report** window.
8. Click **Run now**. When the reports have 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 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.

The server uses the PostgreSQL database. All necessary tables and objects are created automatically. In order to make the server work with the database, you should set up 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 'server3', '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 set to '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 'server3', 'User' is 'postgres', and 'Password' is empty. The 'Keep records for' is set to '180 days'.

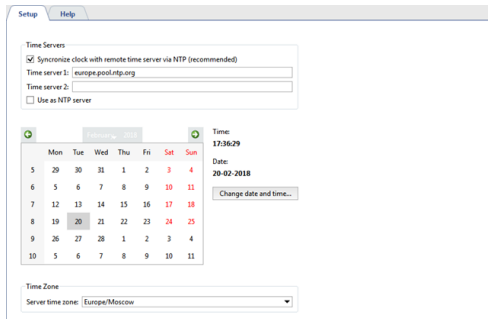


- *PostgreSQL DBMS installation*
- *Configuring the operating system to work with the PostgreSQL DBMS*
- *Starting the PostgreSQL Database Server service*
- *Allowing external connections to the PostgreSQL DBMS*

Date and time



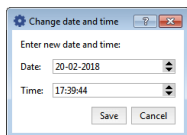
The description of this feature is intended to be used in the Linux-based TRASSIR OS



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.

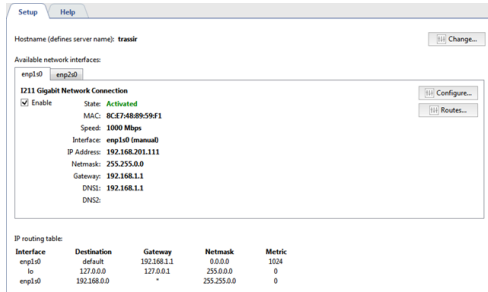


In the **Time Zone** settings group, select the time zone the video server is in.

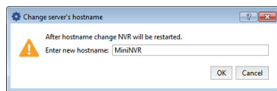
Network interfaces



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.



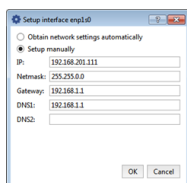
If the server name changes, TRASSIR OS asks to restart the video server in order to apply the change.

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



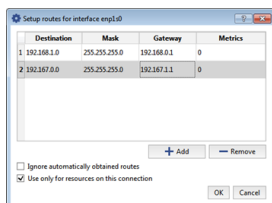
When connected to 3G / 4G modem server, connection settings tab will appear.

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.

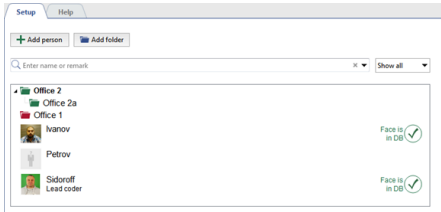
Created IP routing table will be displayed at the bottom of the tab.

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

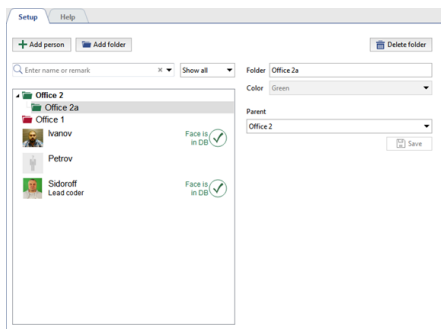
Personas is a database that contains information about people. You can create any person database structure consisting of folders and persons.



The persons' database is used in the operation of the following server 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.
- For **TRASSIR ACS** module, which has an extended set of person's parameters and its own interface for their creation and editing (see section **Personnel**).

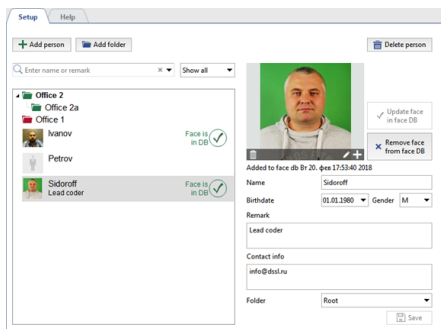
Folders creation



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



The **Add to Face Database** button converts the person's photo into a set of anthropometric data and adds the person to the **Face Database** (see section [Face database](#)).

Users

TRASSIR implements a multi-tiered rights allocation system built on user accounts. Each 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 servers.

After installing server, 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 [SDK](#). The passwords for these users are not set by default.

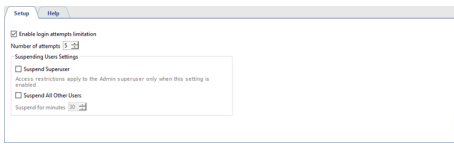
TRASSIR is distributed video surveillance system. Its architecture supports combining an arbitrary number of video servers in a single network. You can control any server through client software or a web browser. You can administer and control servers you are directly connected to as well as servers 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 server and to connect a 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.

Unauthorized access protection



One of the key steps to enhance the system security is to lock user accounts in case of unauthorized access. Set the **Enable login attempts limitation** flag and specify the **Number of attempts** to restrict access to user accounts after a certain number of invalid login attempts.

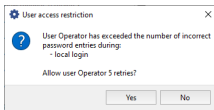
The counting of the number of login attempts is performed during any user authorization and when a certain number of attempts is reached, the corresponding flag is disabled *in user settings*:

- upon **local login**, the *authorizing on the server* is counted, and the **Enable local login** flag is disabled.
- upon **Server/Client connection**, the *server connection* is counted and the **Enable Server/Client connection** flag is disabled.
- upon **SDK connection**, the number of incorrect *SDK server connection* attempts is counted and the **Enable mobile/browser** connection is disabled.

You can enhance your video surveillance security level, if necessary, by configuring the time locking. To do this, enable the **Suspend All Other Users** flag and set the **Block time**. In this case, users who have exceeded the number of login attempts will not be able to log in until the specified time expiration.

If you need to apply the blocking setting to the Admin superuser, enable the **Suspend superuser** flag.

There are two ways to unblock regular users. The first way is to wait until the blocking time expires. After that, the user can try to log in to the system again. Second - you can use the administrator credentials to log in to the system. After that you will see a popup window with suggesting unblocking the blocked user.



The Admin user unblocking process is slightly different. In case the time blocking is used, the only way to unblock is to wait for the blocking time expiration. Upon the specified time period expiration, the Admin superuser can use his own credentials to log in to the system.

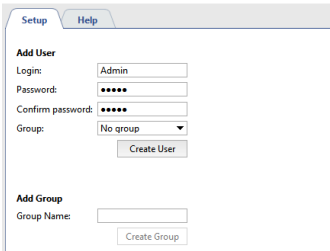


- [Adding users and user groups](#)
- [Determining access rights](#)
- [Per object rights](#)
- [Examples of user rights settings](#)
- [Audit](#)

Adding users and user groups

You can create accounts for both individual users and groups of users on the server. For each account, you can configure detailed access rights.

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 window with two tabs: 'Setup' and 'Help'. The 'Setup' tab is active. It contains two sections: 'Add User' and 'Add Group'. The 'Add User' section has fields for 'Login' (containing 'Admin'), 'Password' (masked with dots), 'Confirm password' (masked with dots), and 'Group' (a dropdown menu showing 'No group'). There is a 'Create User' button below these fields. 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*.



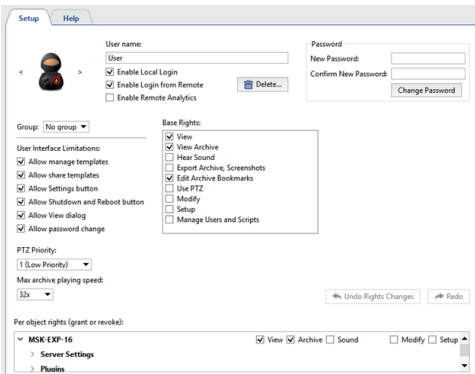
When creating a user account you can select a group to add it to. To do this, select the group's name in the **Group** field. In doing so, all the rights of the selected group will be applied to the new user.



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

Determining access rights

You can access your video surveillance system on server locally, as well as through network connection via another server, the client app, [Web-client](#), or through mobile application. The 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 Server/Client** - network connection via remote server or client.
- **Enable login from mobile/web** - connection through mobile app or Web browser, or connection via [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](#).



After changing the **Admin** user password, the **Limited Functionality Mode** will be enabled on the server. Read more about this mode in [License](#).

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** - uncheck the box to prevent user from accessing the settings window.
- **Allow Shutdown and Reboot** - if you uncheck this box, the user won't be able to shut down or turn off and reboot the server (won't be able to use these features).
- **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.
- **View video without watermark** is responsible for the ability to disable watermark display on the video (see section [Watermark](#)).
- **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.

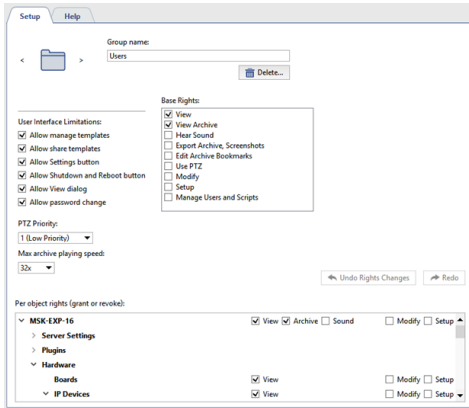


- *Adding users and user groups*
- *Per object rights*
- *Examples of user rights settings*

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](#).

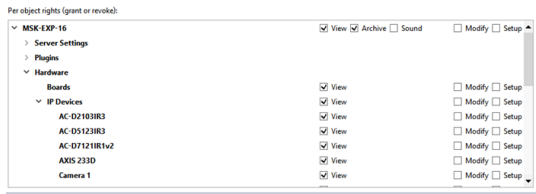
If a group account is no longer needed, then it can be deleted. To do this, open the **Users** item in the server settings, select the group, and click **Delete**. This will not delete the accounts of the users in the group.



- [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:

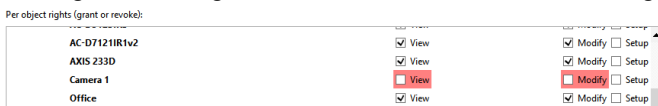
- **View** - Determines if the user can see an object in the system (if it is a device, channel, or server) and/or see specific system settings (server state, server settings, modules, and network).
- **Archive** - Determines if the user can view the archive for the selected channel. This settings is 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.



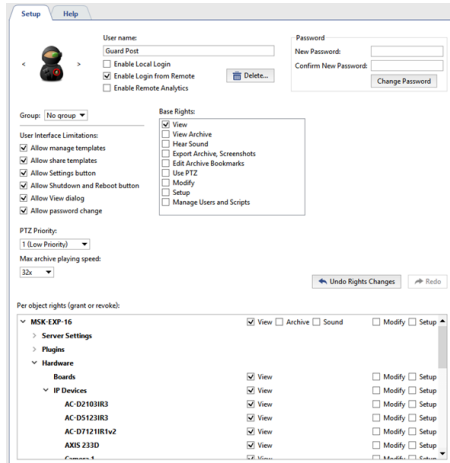
- [Adding users and user groups](#)
- [Determining access rights](#)
- [Examples of user rights settings](#)

Examples of user rights settings

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

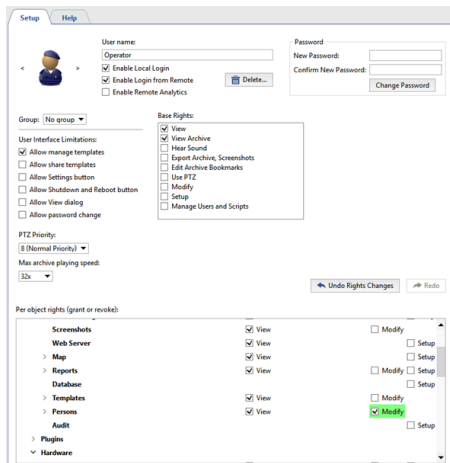
1. Account for a guard post.

- 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.

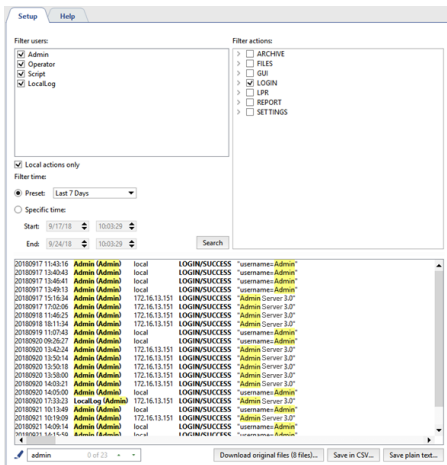
- The basic settings allow for signing into the system locally as well as over the network. Template management is also allowed.
- The **Base rights** allow **View** and **View archive**. Thus, this user can view a live video and work with an archive (only in view mode). Note that given these settings 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 allows you to monitor all user actions performed in TRASSIR. For example, manual change the archive recording mode, changing the IP-device settings, reviewing the archive by the operator, 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:

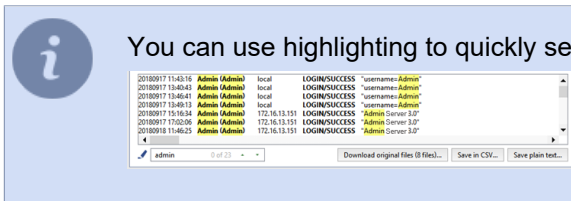
- In the **Filter users** field, select one or more users whose actions should be displayed in the log.



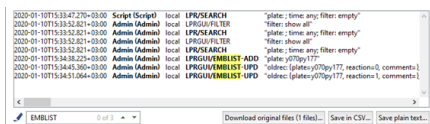
All actions that take place in TRASSIR, but are not caused by direct user actions, are stored in the log under the **LocalLog** user.

- 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.



You can use highlighting to quickly search for a specific user action.



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...**

During the operation, the software saves all user actions to the *.log, which is located in the audit of the software installation directory. A log file is created every day upon the first launch. At the same time, the older (yesterday's)

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



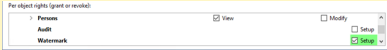
- [Users](#)
- [Adding users and user groups](#)
- [Determining access rights](#)
- [Per object rights](#)
- [Examples of user rights settings](#)

Watermark

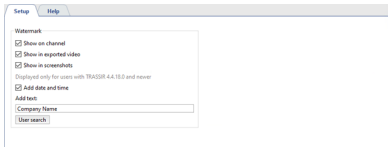
You can customize adding a watermark to be displayed on videos and screenshots in the **Settings** window on the **Server Settings** -> **Watermark** tab.



Only the **Admin** user or a user who has the **Setting** right enabled on the **Watermark** object can enable the watermark on video and customize its appearance.



For more information on user rights settings, see [Per object rights](#).



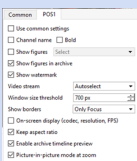
Set the corresponding flags to display the watermark:

- on live channel video and in the archive;
- on video exported from channel;
- on screenshots.

The **GUID of the user** authorized on the server or client where the video is viewed, exported, or screenshot from the channel is used as the watermark. Set the **Add date and time** flag to add the current date and time. To add the arbitrary text, enter it into the **Add Text** field.

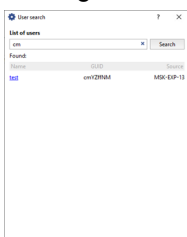


You can turn off the watermark display on channel in camera window appearance settings. To do this, open the context menu of the channel, select **View...** and clear the **Show watermark** flag (for more details see ???).



Only a user with the basic **View video without watermark** right enabled can turn off the watermark display on channel (see section [Determining access rights](#))

When detecting cases where a video or screenshot has been leaked to third parties, you can identify the username and the client/server from which the confidential information was leaked. To do this, click **User Search** and, in the window that opens, enter the **GUID of the user (Username)** or part of it that appears in the video or screenshot. After clicking the **Search** button, the user data will be displayed below.



Devices

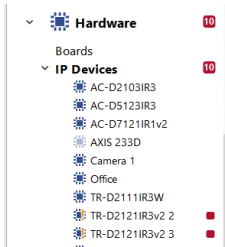
TRASSIR provides full functionality with various video capture cards and IP devices. You can always find a list of supported third-party IP devices on [our website](#).







- [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.



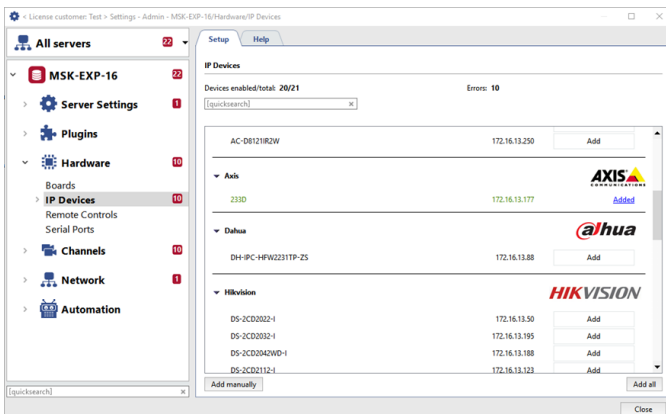
Each device in the list is identified by one of the following icons:

-  Connection OK. No error pending.
-  The connection established, but there is no audio or video stream, Open the corresponding device tab and set the **Video**, **Substream** and **Audio** flags.
-  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).

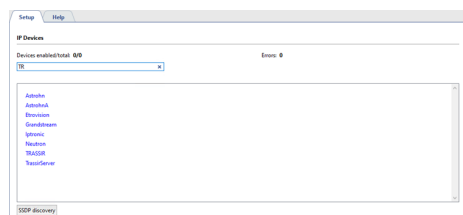
Use **Add all** button to quickly add all found devices to the system.

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

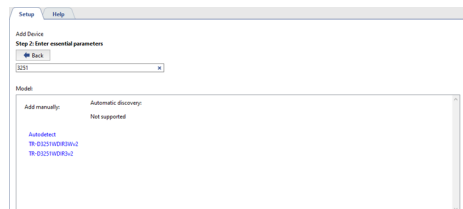


- *Adding IP devices manually*
- *Configuring device settings*
- *Channel settings*
- *Boards*

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.



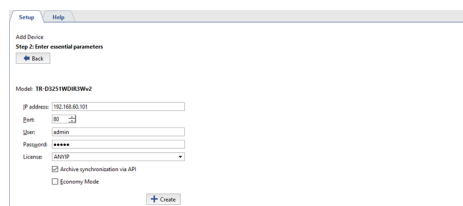
If the device you'd like to add is not on the list, you can use the **SSDP discovery** option. In this case you'll need to set up the connection parameters and the server will recognize the model of the device and connect it.



Automatic device search and **Autodetect** are not supported by all manufacturers.

In order to use the automatic search for NVR and Hikvision equipment, make sure that the UPnP service is enabled in the device WEB-interface settings. If the device is not detected after enabling this service, you will need to find it manually using the SSDP utility available for download on [our website](#).

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.
- The **License** under which this device will connect.
- **Archive synchronization via API**. Set the flag to use the method to synchronize the camera archive to the server with increased speed.
- **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).



Most of TRASSIR cameras feature **Archive synchronization via API**.

In order to activate this feature on previously connected cameras, you need to reconfigure their connection on server.

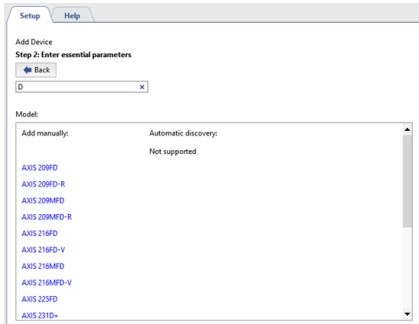
Click **Create**. The **device settings** window will open.



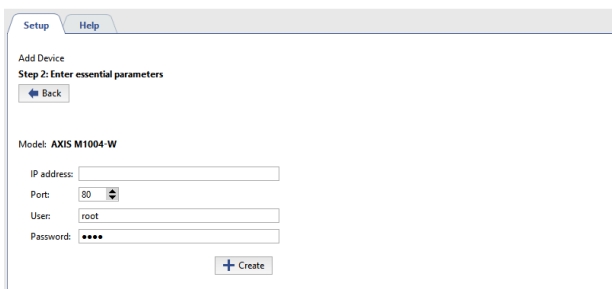
- *IP devices*
- *Adding IP devices that use the ONVIF protocol*
- *Adding IP devices using RTSP*
- *Configuring device settings*
- *Channel settings*
- *Boards*

Adding IP devices that use the ONVIF protocol

The server supports operation with IP devices via the ONVIF protocol. To add a new device, click **ONVIF** in the **IP devices** tab of the **Settings window**.



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.

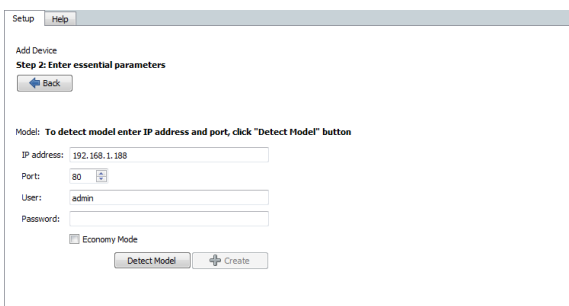



- **IP address** - The address doesn't need to be specified if the device was found automatically.
- **Port** - The number of the network port for connecting to the device (may be different from the web interface's port).
- **Username and password** - Note that the username and password entered must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



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**.



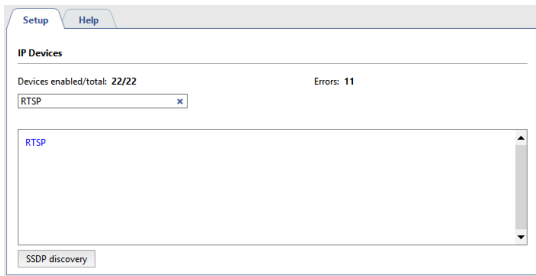
The **Model:** field will look as follows . After some time, the device model will be identified. Click the now-active **Create** button. The **device settings** window will open.



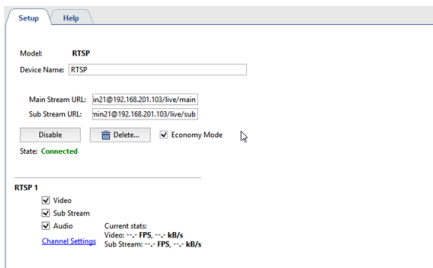
- *Adding IP devices manually*
- *Adding IP devices using RTSP*
- *Configuring device settings*
- *Channel settings*

Adding IP devices using RTSP

The server can receive RTSP stream directly from various devices and use it in your video surveillance system by writing it to an archive, processing with the help of 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.

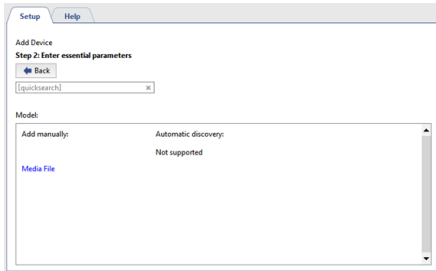


- *Adding IP devices manually*
- *Adding IP devices that use the ONVIF protocol*
- *Configuring device settings*
- *Channel settings*

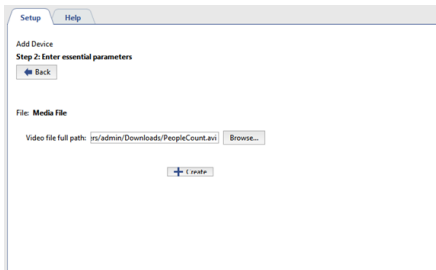
Adding video files

The server can use a video file as a channel.

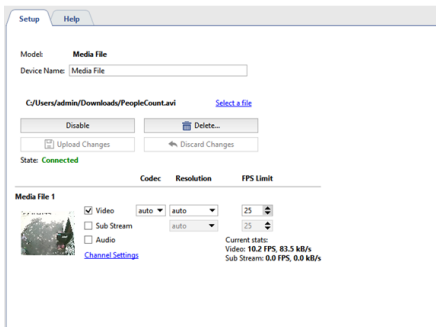
To add a video file, open **IP devices** tab. Select manual adding mode pressing **Add manually** button, and then go to **File -> Media File**.



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

The video transmitted by Fisheye-camera has a number of features: wide viewing angle and intense image deformation on the periphery. The server allows you to dewarp the image into several independent channels and each of them will be recorded into the archive with its own settings.

The screenshot shows the 'Setup' tab of a device interface. At the top, it displays the Model (TR-D9161IR2) and Device Name (TR-D9161IR2). Below this, network settings are shown: IP Address (192.168.101.62), Port (80), and User (admin). There are buttons for 'Disable', 'Delete...', 'Reboot', and 'Economy Mode'. A section for 'Allow Dewarp' is checked, with a status 'Connected' and 'HDD not formatted'. A table lists channel settings for three channels (TR-D9161IR2 1, 2, and 3). Channel 1 has settings for Video (h264), Sub Stream (CIF), Audio (G.711alaw), and a 'Current status' of Video: 24.5 FPS, 692.2 kB/s and Sub Stream: 25.1 FPS, 24.1 kB/s. Channels 2 and 3 have settings for Video (SW MPEG4), Resolution (640x480), GOP (20), and Bitrate (1024), with a 'Current status' of Video: 22.5 FPS.

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. The server allows creating 4 virtual channels 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:

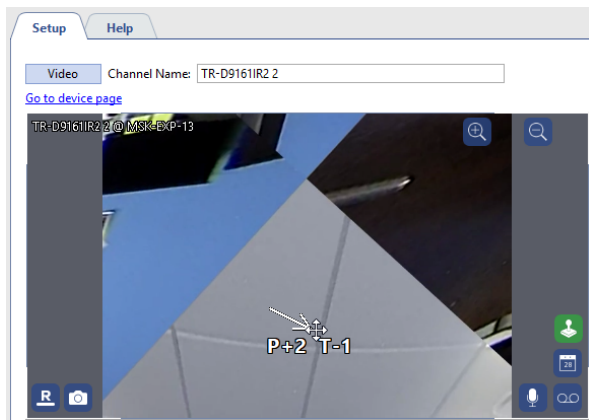
- **Codec** is compression codec used. **mpeg4** codec is used to compress virtual channel.
- **Resolution** is size of image.
- **GOP (Group of pictures)** group of pictures containing one key picture.
- **Bitrate** - video compression level.



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 the client.

The **Current stats** field displays video FPS and the speed of the channel record to the 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 operate with 2 types of the video capture plates:

- 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: TR-D8251WDR3

Device Name: TR-D8251WDR3

License: ANYIP

IP Address: 172.16.13.66 Port: 80 User: admin [Setup connection](#)

Disable Delete... Reboot ☐ Economy Mode

[Upload Changes](#) [Discard Changes](#) [Web Interface](#) [Change IP...](#) [Change Password...](#)

Firmware version: IPCAM_V4.05.38.240223 [Update firmware](#)

State: Connected
HDD absent

	Codec	Resolution	GOP	FPS Limit	Compression	Bitrate	Type	Sample Rate
TR-D8251WDR3 1	H264	5MP	20	20	Minimum	16000	Variable	
		CF	20	25	Minimum	256	Variable	
	Audio	G.711law						8000

Channel Settings

Current status:
Video: 25.0 FPS, 647.9 MB/s
Sub Stream: 23.5 FPS, 26.2 MB/s

GPIO Inputs

Name	Normal State
<input type="checkbox"/> Enable Input Input 1	Low is normal

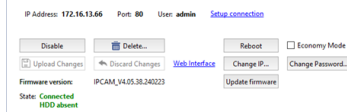
GPIO Outputs

Name	Startup State
<input type="checkbox"/> Enable Output Output 1	Store in settings

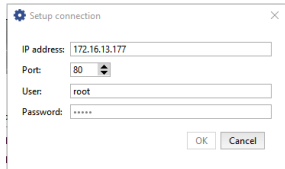
- **Model** - The device model.
- **Device name** - The name that will be displayed in the device list. By default, this is the same as the device model.
- The **License** under which this device will connect.

Connection parameters settings

The devices, connected over the network, have a number of additional settings:

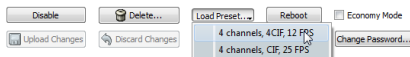


- **Network connection parameters** - IP-address, port and user name. Press **Setup Connection** to modify parameters.



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.
- Click **Delete...** to delete the device permanently 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, the server will consider it an entirely new device – all of its previous settings will be lost. If a device is deleted incorrectly or accidentally, 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.



If TRASSIR OS is used as the operating system, the web interface of the camera will open in the built-in help on the server.

- 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.

IP Address: 172.16.13.66 Port: 80 User: admin Setup connection

Disable Delete... Reboot Economy Mode

Upload Changes Discard Changes Web Interface Change IP... Change Password...

Firmware version: IPCAM_V4.05.38.240223 Update firmware

State: Connected HDD absent



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 **Firmware version**: field displays the current device firmware version.
- The **State**: field displays the current state of the connection to the device.



The **no mainstream video** and **no sub-stream video** errors may cause the detectors freezing and stop recording to the archive. Please check the device web interface settings, as well as the network status. Please make sure that the correct device model is selected.

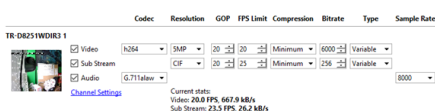
Stream settings

The devices, connected to the server, transfer 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.
- The **Additional Stream** or **Substream** is the video data of low (comparing to main 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. The substream enables the substantial decrease of load to the server and the network (in case of connecting to the server via the network using a 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).



Using H.265+ and H.264+ codecs may result in increased memory size and server load, which may negatively affect system performance and stability.

- **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.

You can configure the following audio stream parameters:

- **Codec** - the audio compression codec used.

- **Sample rate** - the selection of the audio signal transmitted by the camera sample rate. The higher value provides high-quality and detailed audio.

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.

Press **Add serial port** in order to set up PTZ device, connected to the server serial port directly. Press **Add MOXA serial port** to add the device, managed through the network converter.



The MOXA network converter connection is configured on TRASSIR OS and Astra Linux SE 1.7 server locally.

The MOXA network converter connection is configured on TRASSIR OS server locally.

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 camera using jumpers. When specifying the camera settings, 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.

In order to connect a remote control to the server, press **Add remote control**, select the **Type** and check **TCP port** or **UDP port** - port to transfer data.

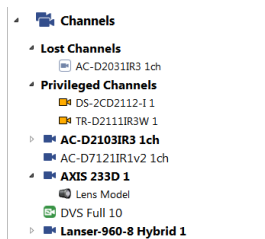


Before connecting a remote control, for example **Hikvision DS-1100KI**, the server IP-address and data transfer port should be set up.

See setting details in User's Manual of a particular remote control.

Channels

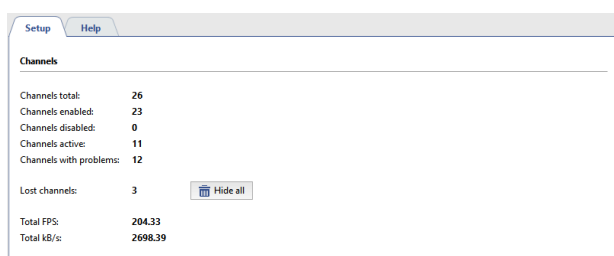
A list of all of the server's channels is always available in the **Settings** window on the **Channels** tab.



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.** The server allows recording archive from the devices, connected to another 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.

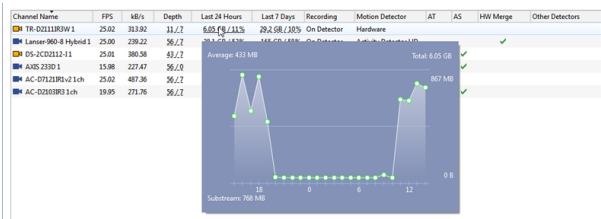
Channel Name	FPS	kB/s	Depth	Last 24 Hours	Last 7 Days	Recording	Motion Detector	AT	AS	HW Merge	Other Detectors
TR-D2111IR3W 1	25.00	317.64	31,12	6,05 GB, 131%	29,3 GB, 130%	On Detector	Hardware				
Lanzer-960-8 Hybrid 1	25.00	252.24	36,12	28,1 GB, 132%	165 GB, 158%	On Detector	Activity Detector HD				
OS-2CD2112-11	25.00	378.30	63,12	7,43 GB, 134%	9,08 GB, 134%	On Detector	Hardware				
AXIS 233D 1	16.14	247.82	36,10	6,23 GB, 133%	28,6 GB, 132%	On Detector	Activity Detector HD				
AC-D71211IR1v2 1ch	25.02	488.59	36,12	3,63 GB, 105%	28,6 GB, 132%	On Detector	Hardware				
AC-D2031IR3 1ch	19.99	243.04	36,12	963 MB, 13,2%	6,15 GB, 13,2%	On Detector	SMART				

* Forecast

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	308.36	31.7	6.05 GB / 11%	29.6 GB / 10%	On Detector	Hardware				
Laser 980-8 Hybrid 1	25.00	237.38	36.7	28.4 GB / 13%	105.0 GB / 9%	On Detector	Activity Detector H				
DS-2C02112-11	24.99	379.45	43.7	7.43 GB / 14%	9.69 GB / 34%	On Detector	Hardware				
AS05-2330 1	15.86	245.42	36.7	6.21 GB / 11%	28.6 GB / 13%	On Detector	Disable				
AC-0712183-v2 1ch	25.01	476.38	36.7	5.67 GB / 10%	38.6 GB / 13%	On Detector	Hardware				
AC-0203083 1ch	19.95	274.16	36.7	5.67 GB / 10%	38.6 GB / 13%	On Detector	Activity Detector HD				
							SMART				

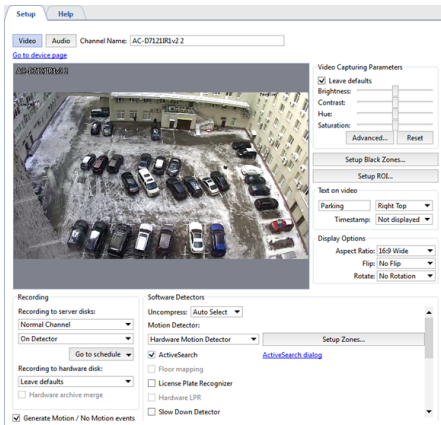


- [Channel settings](#)
- [Channel recording settings](#)
- [Motion detector settings](#)
- [Recording network channels](#)
- [Lost channels](#)

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:

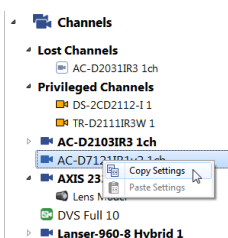
- The central part of the window has a real-time picture and you can control the camera just as you would in operator mode (for example, by using a camera's PTZ mechanism).
- **Recording**
- **Video Capturing Parameters**
- **Setup black zones**
- **Text on video (watermarks)**
- **Display options**
- **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.



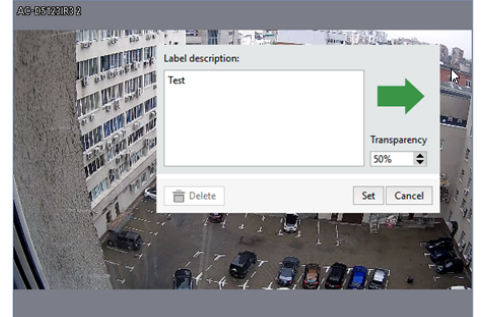
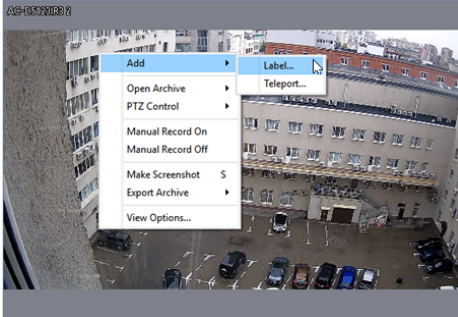
All the settings are applied "on-the-fly", and you can see all the changes in real-time.



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.




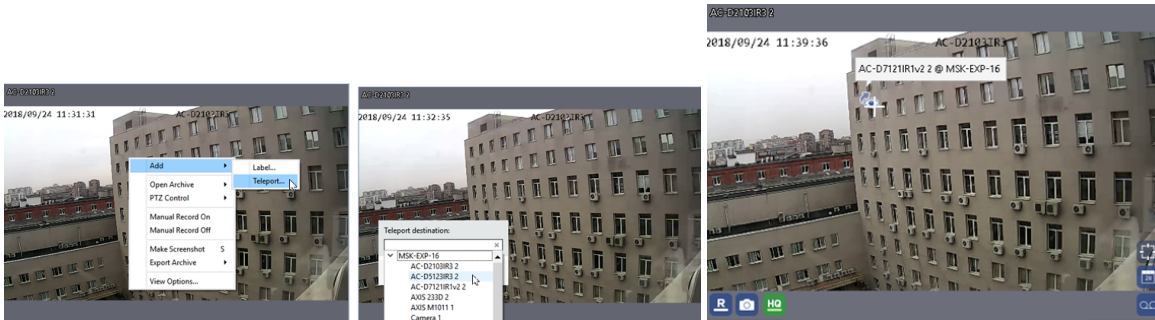
You can select the label's icon or upload your image as an icon. To do this, press **Add** and select the image.



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.



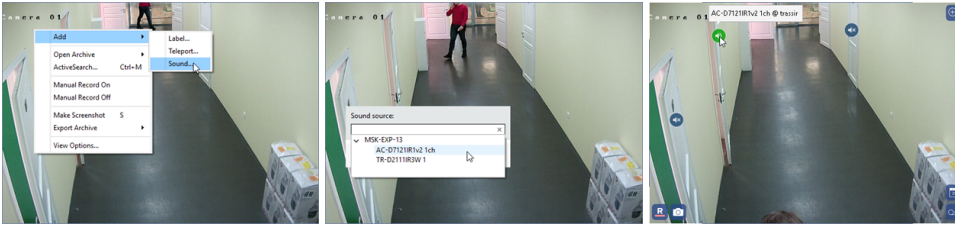
If needed, move the teleport icon to the desired location. To do this, click and drag it.

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 audio streams in one room installed, you can switch between these devices' audio streams, 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 device connection, the server sends it its own settings, including settings for the archive recording, 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 server will be restored from the device built-in drive.

The archive recorded before the flag is set will not be synchronized.

The maximum depth of the archive downloaded from the device is 72 hours. At the same time, the size of the archive downloaded from the device is limited to 24 hours.

If there is no connection to the device for an extended period (more than 3 days), upon reconnection, no more than 24 hours of data from the last 72 hours will be synchronized. The rest of the archive will only be viewable on the device.



Not all devices support working with a remote archive or the remote archive recording control feature. It is also important to consider that recorders may have limitations on the number of channels from which it is possible to download archive records at the same time. If the recorder is not able to play recordings from all channels at the same time, the synchronization of all recorder channels with the server archive will be impossible.

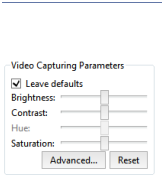


- [Archive setup on the server](#)
- [Channels](#)
- [Channel settings](#)
- [Motion detector settings](#)
- [Video capturing parameters](#)
- [Watermarks](#)
- [Black zones](#)
- [Changing image rotation and aspect ratio](#)

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 you change the sliders, the settings are sent to the device, so changing the position of the sliders may not change the picture from the camera immediately, but with some delay.

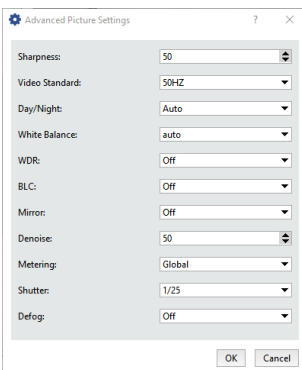


Depending on the device being used, one or more settings may be unavailable.

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](#)

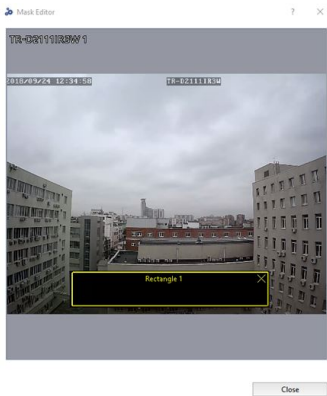
Black zones

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.



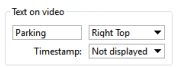
Black zones are shown over the video in both real time mode as well as in archive recording.



- [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.

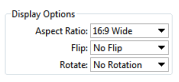


The Latin alphabet is used to display text over video; displaying text using the Cyrillic alphabet is not supported.



- [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:

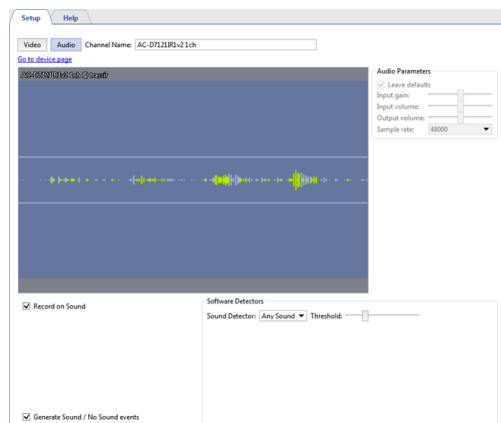
- **Aspect ratio** - Lets you select the image's aspect ratio: **Standard 4:3** or **Widescreen 16:9**;
- **Flip** - Reflects a mirror image **Horizontally** or **Vertically**;
- **Rotate** - Rotates the image by 90, 180 or 270 degrees.



- [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 a oscilloscope representation of the audio coming from the camera's microphone.

In the **Audio Parameters** group of settings, you can set the volume level and quality of the audio stream. When you move the sliders, the new settings are sent to the device, so changing the position of the sliders may not change the sound from the camera immediately, but with some delay. If the **Leave defaults** flag is set, the volume and quality of the audio stream are defined by the parameters set in IP camera's web interface.

If the audio stream of the device is of meager quality, the sound is muted or absent, choose a channel from the **Default Sound** dropdown list to play its audio stream with the video. If the channel chosen as the sound source has Archive recording enabled, the audio stream will play with the archive playback. Nevertheless, there will be no sound after the **Archive export**. Apart from that, if the channel archive chosen as the sound source contains no video, the audio stream will not be available for playback.



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.



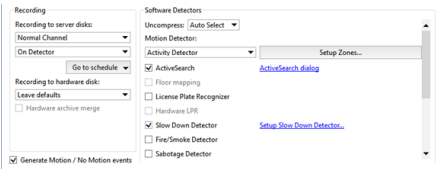
Depending on the device being used, one or more settings may be unavailable.



- *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.



We recommend selecting **Auto Select** in the **Uncompress** setting. In this case, depending on the motion detector and video analytics systems used, the optimal unpacking stream will be selected.

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** - the free software-based detector will be used for motion detection. This detector is suitable for most scenes.
- **Activity Detector HD** - the free software-based detector designed for detecting the motion of small objects in large spaces 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*
- *Camera image quality indicator CiQi*



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 server **License Plate Recognition** module. 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*

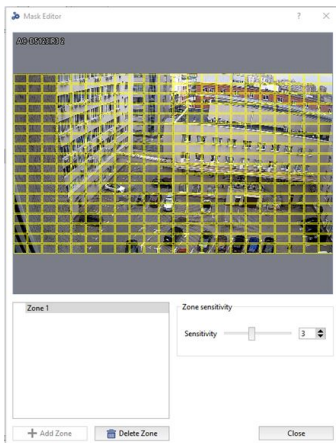
Hardware-based motion detector settings

The server can receive information from cameras' and compression cards' hardware-based detectors. This spares a substantial amount of video surveillance server resources.



Keep in mind that not all devices have a built-in hardware motion detector. The configuration of the device hardware motion detector must be performed only in the server settings, not through the device 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

In case a camera does not have a hardware-based motion detector or its quality is unsatisfactory, you can use the server free software-based detector.

The software-based detector is provided in two forms: **Activity detector** and **Activity detector HD**. The **Activity detector** suits for most scenes except large spaces; to detect the motion of small objects in large spaces, use **Activity detector HD**.

Recording Recording to server disks: Normal Channel On Detector	Software Detectors Uncompress: Auto Select Motion Detector: Activity Detector
---	---

OR

Recording Recording to server disks: Normal Channel On Detector	Software Detectors 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.

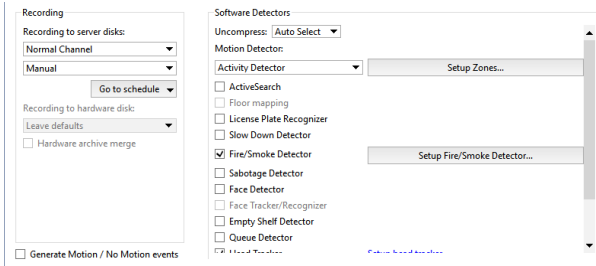
To configure the detector's sensitivity, change the value of the **Object size** slider. The sensitivity settings are specified separately for each zone. Up to five independent detection zones can be created.



- [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.



When working outdoors, the number of false alarms of the detector increases. To reduce the number of false alarms, the image in the camera field of view should be static. For this purpose, it is necessary to exclude zones with constant motion from the camera field of view.



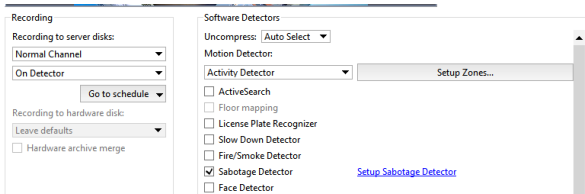
- [Channel settings](#)
- [Motion detector settings](#)

"Sabotage detector" module settings

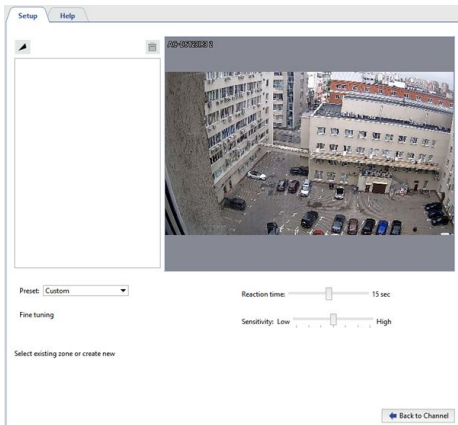
The following actions with the camera are detected as sabotage:

- **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:

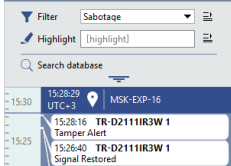
- Refrain from setting high value of this parameter as detector needs certain time to analyse the image and it will last for **Reaction time * 3**. Thus, in case response time is 20 sec., detector will need 60 sec. for analysis. That is sabotage can be detected only in 1 minute following camera activation. 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 a 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*.



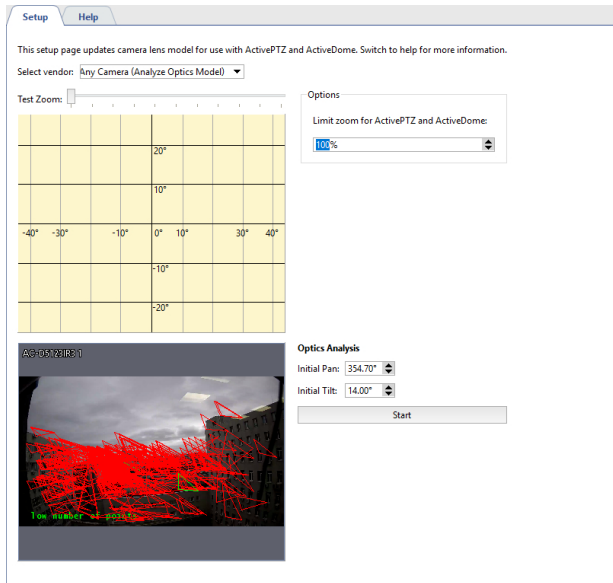
To provide the appropriate detector tracing, you can create *rule or script* which trigger on its status changing.



- *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:

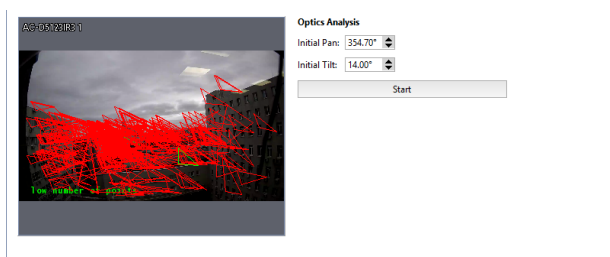
1. Select "Any camera (Analyze Optics Model)" in the "Select vendor" dropdown list.
2. Arrange the camera such that the image contains as many contrasting areas as possible.



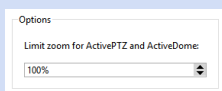
Preferably, there should not be motion and external noise (rain, snow, swaying trees) in the camera's field of view during the optics analysis.

3. Click "Start".

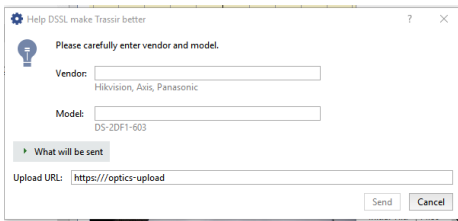
The automatic optics calibration process will start (it may take several minutes). During the calibration, the camera will aim at different points of the scene. When the calibration is complete, the coordinate grid is displayed on top of the image and a button to send the model optics appears.



The **Limit zoom for ActivePTZ and ActiveDome** additional parameter lets you manage the camera maximal zoom. The default value is **100%** (no limits). In case the **0%** value is set, the camera will rotate in the required direction without zoom.



If you want to help the development of our software, you can send the resulting calibration [to us](#). To do this, click the "Send optics model" button. A dialog box in which you can specify the manufacturer of the camera, its model, and see exactly what information will be sent, will open. Leave the "What will be sent" field default. Click the "Send" button to transfer the information.



A screenshot of a web form titled "Help DSSL make Trassir better". The form has a light blue header with a gear icon and a light blue body. It contains the following elements:

- A light blue box with a light blue lightbulb icon and the text "Please carefully enter vendor and model."
- A "Vendor:" label followed by a text input field. Below the field, the text "Hikvision, Axis, Panasonic" is displayed.
- A "Model:" label followed by a text input field. Below the field, the text "DS-2DF1-603" is displayed.
- A "What will be sent" label followed by a text input field.
- An "Upload URL:" label followed by a text input field containing the text "https://optics-upload".
- "Send" and "Cancel" buttons at the bottom right.




To test the calibration results, try to direct the camera at several points in *ActivePTZ mode*.



- *ActiveDome - Automated PTZ-camera control*

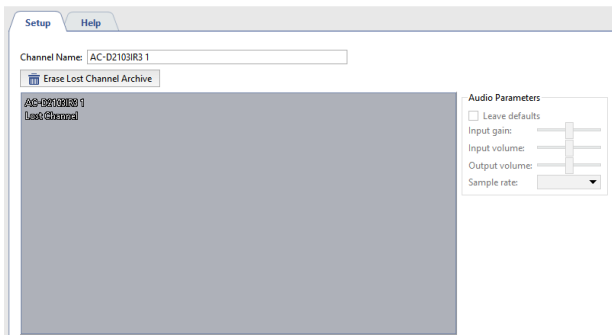
Lost channels

Lost channels is a unique feature of our software that significantly simplifies the work with an archive. If a device is deleted or disconnected, the archive recorded by the device will be accessible as lost channels. They are identified in the operator's interface by the following icon  (You can read more about the possible colors of channel icons in the [Operator's Guide](#)).

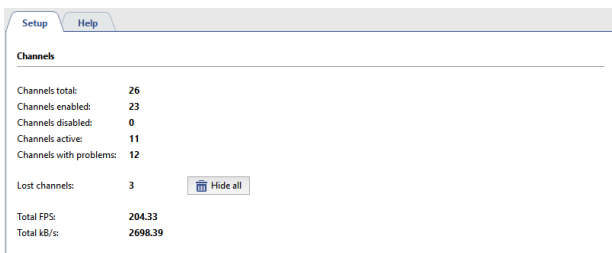
You can view and export the archive for these channels without any limitations; no additional steps or settings are necessary. And as usual, loss channels are available over the network given a client-server connection.

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 server, the list of the archive's channels will appear on the second server (read more about new disk connection in [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.



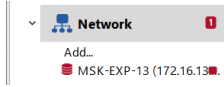
You can use both server and client versions of the software to manage lost channels. You can read more about working with the archive in the [Operator's Guide](#).



- [Archive setup on the server](#)
- [Channels](#)
- [Channel settings](#)




Network

TRASSIR is a distributed video surveillance system. Its architecture supports connecting an arbitrary number of video servers to a single network.



Each server manages specific objects: IP-equipment, video capture cards, etc. Accordingly, by setting up connections between servers, you can easily access all objects over a local network or the Internet. For example, you can select the main server and use it as a control center for all objects of the video surveillance system, or connect to all servers using the client.

You can find a list of the current connections with other servers on the **Network** tab of the **Settings** window. After the installation, the list of connections will be empty. The list will expand 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 the servers in two ways: directly by specifying the IP address or with the help of **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.



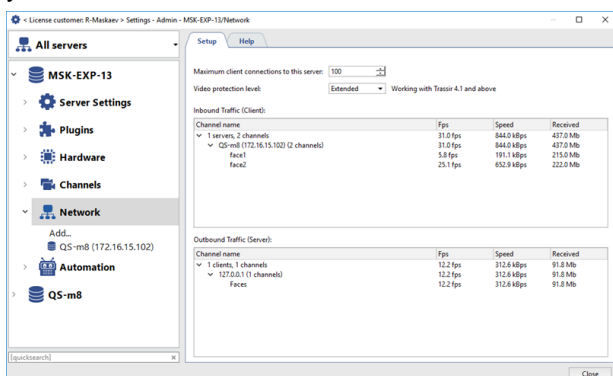
There are some cases when CloudConnect-connection will be *arranged via TRASSIR Cloud service*:

- for 10 seconds, the server cannot establish a direct CloudConnect connection with the cloud camera or server;
- errors were detected while monitoring CloudConnect connection, which does not allow a stable transfer of data between servers.



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 order to save the network bandwidth, the server streams video only from 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 limiting 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 software versions.
- **Extended** - for versions 4.1+.

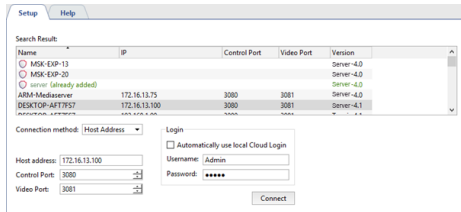


- *Connecting to a new server*
- *Changing the connection settings*

Connecting to a new server

To add a connection with another server, select **Network** -> **Add** in the system settings.

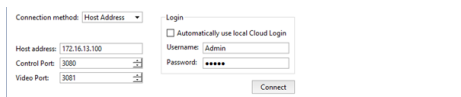
The right part of the window displays a table with a list of servers automatically found in the local network, as well as servers connected to the TRASSIR Cloud. The servers connected, found in the cloud, are highlighted with the icon . The table displays the following information: server name, IP address, 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.

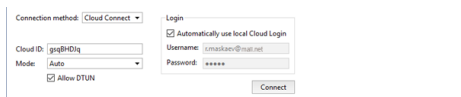
The settings can vary depending on the **Connection method**:

- 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 a 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**.



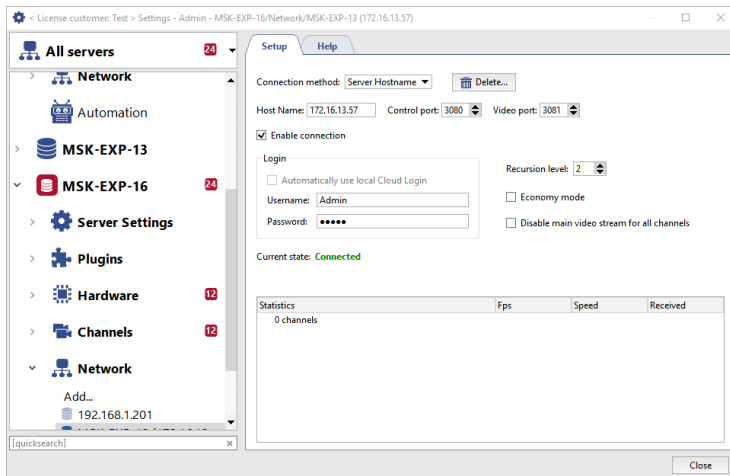
While connecting to 3.2 server version, you'll see the message **Restricted connection**, the description of which you will find in *Restrictions when connecting to servers with version 3.2*.



- **Network**
- **Changing the connection settings**
- **Connection through TRASSIR Cloud**

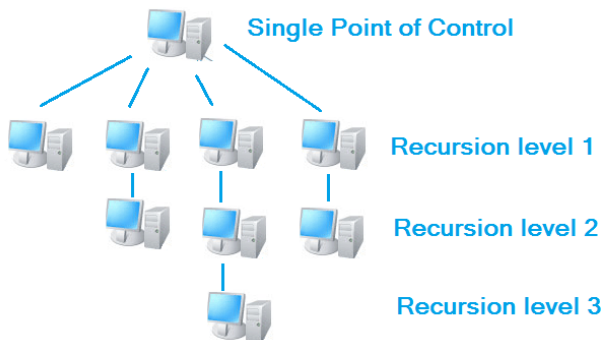
Changing the connection settings

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.

The server 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 server through an intermediate server rather than connecting directly. A **Recursion level** - 1 means that a connection will be made only the server to which you are directly connecting. A **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.



Take care when building complex video surveillance systems, where one server is used as a gateway or intermediate server to which other servers and clients are connected. If more than 5 servers are connected to such a gateway server, including servers connected by recursion, we cannot guarantee stable operation of the gateway server.

In this case, you should use **TRASSIR CMS** server as a gate.

Economy mode - A special connection mode that reduces network traffic. In this mode, the server transmits the minimum amount of information, including service information.

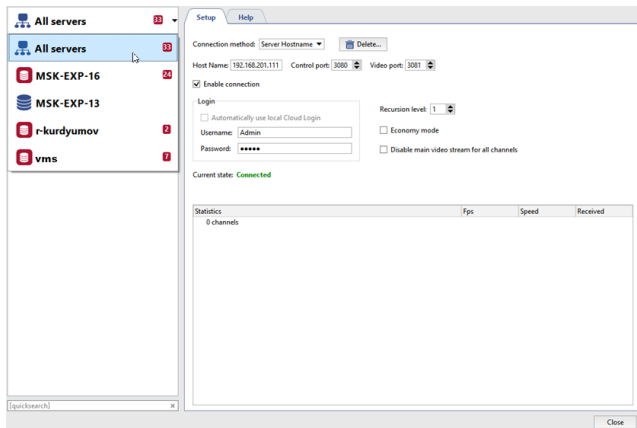
Disallow main video stream - Blocks the reception of the mainstream from all channels. When viewing a camera's feed, the substream will always be displayed, regardless of other server settings; and if there is no substream – the number of frames displayed per second will drop to between one and two.

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-2CD2012-I1	0.0 fps	0.0 kbps	0.0 Kb
DS-2CD854FWD-E1	25.3 fps	542.5 kbps	24.5 Mb
DS-2CD854FWD-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.



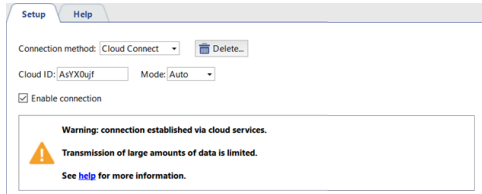
- [Network](#)
- [Connecting to a new server](#)

Connection through TRASSIR Cloud

CloudConnect-connection will be arranged via TRASSIR Cloud service:

- if the server fails to establish a direct CloudConnect connection with the cloud camera or server within 10 seconds;
- if errors are detected during the CloudConnect connection monitoring that do not allow a stable transfer of data.

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* - 3 minutes.
- *Archive review* - 3 minutes.
- *Archive export* maximum length is 180 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 when connecting to servers with version 3.2

- The event log does not show the archive of channels connected to servers with version 3.2 *on the same timeline*.
- The *tabs* are not displayed in archive of channels connected to servers with 3.2 version.
- 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*. The **Automation** greatly simplifies the work of an operator by configuring responses to interesting- and/or alarm events. You can customize 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, 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.



For the correct operation of rules and scripts, the names of IP devices, channels and detector zones must be unique.

Scripts

Scripts are a strong point of TRASSIR. Scripts allow you to automate typical operations, simplify the operator's work, and make integrations. In addition, scripts are fun!

Scripts are written in the **Python** language.

- Python is the easiest language to learn, a [syntax language](#). Also, the Python is a general-purpose language, which is not limited to a predefined set of functions. You can do anything you want with it, that is, read files and communicate with people over the network. You can find more information on python.org.
- The script can [read and change settings](#) of servers, [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 the language's syntax. If you need a more complete description of the language, you should use python.org.



The indentation is a part of the language. The 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()))
```

The 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

The server has its own built-in script editor, which consists of the following functional areas:

- Script management area

Enter the script name to be displayed in settings into the **Script name** field.

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>>?MS</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.

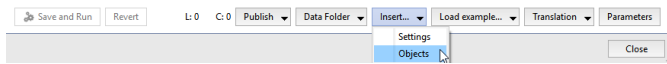
To save the script to a file, click the **Publish** button and select the desired option: in encrypted form - **To file...** or as is **To file (unencoded)...**



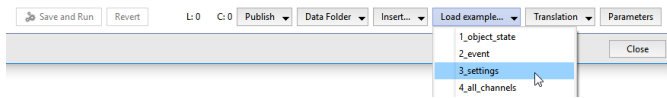
When saved in encrypted form, the text of the script displayed in the editor is encrypted. This feature will help you to protect your intellectual property and to prevent unauthorized changes to the script.

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.

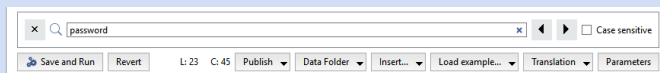


The built-in script editor supports creation of multilingual scripts. You can create a script that can display the interface in the same language as the server or in another language you need. The language file is created using the **Qt Linguist** program. You can add a new language file, edit an existing one, update or select a script language by clicking **Translation** and selecting the required action.

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:

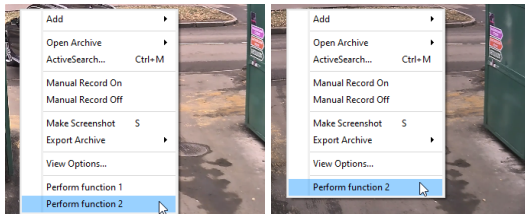
```
def f():
    message("Hello world!")
activate_on_shortcut("F9", f)
```

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)
```

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)
```

Working with the settings makes it possible to change the server configuration significantly. As an example, use the script for converting 2.x to 3.x software settings.



- *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])
```

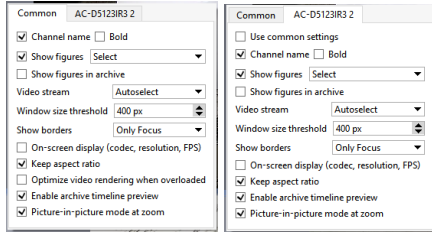
[csv_channels] - list pf channels separated by commas;

[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

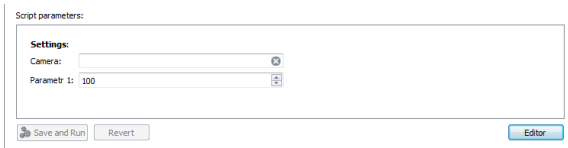
To create a parameter block in a script and/or add additional resources to a script, insert the following block at the beginning of the code:

```
"""
<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** - field for selecting a channel from the channels connected to the server

```
<parameter>
  <type>channel</type>
  <id>channel_id</id>
  <name>Camera</name>
  <value></value>
</parameter>
```

- **objects** - server objects selection field

```
<parameter>
  <type>objects</type>
  <id>objects_id</id>
```

```
<name>Objects</name>
<value></value>
</parameter>
```

- **server** - server selection field

```
<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

ActivePOS events

ActivePOS events received by the script are represented by objects that have the following fields:

Field	Value
<i>article</i>	Article number
<i>associated_channel</i>	Video channel associated with POS terminal
<i>barcode</i>	Item barcode
<i>cashier_name</i>	Name of the cashier
<i>discount</i>	Total discount on check
<i>discount_card</i>	Discount card number
<i>flags</i>	Event flags
<i>location</i>	Location
<i>op_id</i>	Internal receipt number (may contain the actual receipt number)
<i>pos_terminal</i>	POS GUID
<i>pos_terminal_name</i>	POS name
<i>position</i>	Item in the receipt
<i>price</i>	Item price
<i>price_per_unit</i>	Price per unit
<i>quantity</i>	Item quantity
<i>text</i>	Text (item name, bonus card number, message, etc.)
<i>ts_in_receipt</i>	Time of the event generation on the terminal
<i>ts_received</i>	Time of event receipt by the server
<i>type</i>	Event type
<i>weight</i>	Item weight

The `activate_on_pos_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. To find the required moment in the video archive, use the reception time of the event.

To search for events from POS terminals in the database, use the **search_pos_events()** function. The function accepts 4 parameters:

- callable object, which will be called for each event found;
- the lower limit of the time interval in which the events will be searched for;
- the upper limit of the time interval in which the events will be searched for;
- filter.

As a filter, you need to transmit a dictionary, in which you can use the following keys:

Key	Value	Default value
cashiers	Names of cashiers in whose receipts you need to find the events	[]
events	Types of events to find	[]
receipt_number	Numbers of receipts in the receipts of which you need to find the events	[]
terminals	Terminals, in the receipts from which you want to find the events	[]
text	Text containing in events (event_text, event_article, event_barcode) that you need to find	[]

```
import time
from pos_utils import *

filter = {
    "receipt_number": "1234567",
    "text": [StringFilter("Milk", SearchFlags.STARTS_WITH)],
    "cashiers": ("Ivanov I",)
}
search_pos_events(lambda event: alert(event.text), time.time() - 24 * 60 * 60, time.time(), filter)
```

This example will find all events (maximum: 500) in the checks with the number "1234567" created by the cashier "Ivanov I", in the event_text, event_article or event_barcode fields containing the text beginning with the string "Milk" and received in the last 24 hours. The text of each event will be displayed in a separate pop-up window.

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 the string to upper case (all capital letters). For this conversion to work, the string must be in Unicode (utf-8).

ActivePOS incidents

Incidents generated by ActivePOS detectors and received by the script are represented by objects with the following fields:

Field	Value
<i>associated_channel</i>	Video channel associated with POS terminal
<i>cashier_name</i>	Name of the cashier
<i>comment</i>	Commentary on incident
<i>custom_columns</i>	Additional information
<i>detector</i>	GUID of the detector that created the incident
<i>expert</i>	Name of the operator who processed the incident
<i>expert_estimate</i>	Damage assessment
<i>id</i>	Unique incident ID
<i>operator</i>	Name of the operator who created the incident
<i>related_ts</i>	Times of the events that triggered the detector
<i>review_duration</i>	Duration of incident processing
<i>review_ts</i>	End time of incident processing
<i>server</i>	Server GUID
<i>status</i>	Incident status (0 - new, 1 - confirmed, 2 - rejected)
<i>terminal_guid</i>	POS GUID
<i>terminal_name</i>	POS name
<i>ts_created</i>	Incident creation time
<i>type_description</i>	Incident description
<i>type_id</i>	GUID of the incident type
<i>type_name</i>	Incident name

The **activate_on_pos_incidents()** function is used to get messages about new incidents. The function accepts two parameters:

- Detector GUID;
- callable object, which will be called for each received ActivePos incident created by the detector with the given GUID.



If you send an empty string as GUID, the callable object will be called for any new incident.

```
activate_on_pos_incidents("", lambda incident: alert(incident.type_name))
```

The **search_pos_incidents()** function can be used to search for incidents in the database. The function accepts 4 parameters:

- callable object, which will be called for each ActivePos incident found;
- the lower limit of the time interval in which the incidents will be searched for;
- the upper limit of the time interval in which the incidents will be searched for;
- filter.

As a filter, you need to transmit a dictionary, in which you can use the following keys:

Key	Value	Default value
cashiers	The cashiers in whose receipts you need to find incidents	[]
detectors_names	The names of the detectors that generated the incidents or the types of incidents to find	[]
experts	The operators who confirmed or rejected the incidents to be found	[]
flags	The bitmask of incident search flags: <ul style="list-style-type: none"> • FILTER_CONFIRMED - search for confirmed incidents only; • FILTER_DECLINED - search for declined incidents only; • FILTER_NEW - search only for unreviewed incidents; • FILTER_NONEMPTY_ESTIMATE - search for incidents with non-zero damage assessment. 	0
incidents_ids	Types of incidents to find	[]
limit	Maximum number of requested incidents	-1
terminals	The terminals, in the receipts from which you need to find the incidents	[]

```
import time
from pos_utils import IncidentFlag

filter = {
    "flags": IncidentFlag.FILTER_CONFIRMED | IncidentFlag.FILTER_NONEMPTY_ESTIMATE,
    "limit": 20,
}
search_pos_incidents(lambda incident: alert(incident.type_name), time.time() - 24 * 60 * 60 * 2, time.time(),
    filter)
```

This example will analyze all the receipts stored in the database for the last 2 days, then find the last 20 confirmed incidents with a non-zero damage estimate among them, and display the name of each type of incident in a pop-up window.

The **pos_process_archive()** function can be used to start the processing of the event archive by a particular detector. The function has 3 arguments:

- Detector GUID;
- the lower limit of the time interval of the event archive;
- the upper limit of the time interval of the event archive.

```
import time

pos_process_archive("T1RuoVF7", time.time() - 24 * 60 * 60 * 2, time.time())
```

This example will start processing checks for the last 48 hours by a detector with a GUID equal to "T1RuoVF7".

The **pos_incident_create()** function can be used to create a new incident from a script. The function uses 4 mandatory arguments:

- The GUID of the terminal that will be associated with the created incident;
- name of the created incident type;
- name of the cashier;

- the function to which the result of the incident creation operation will be sent in case of an error.

```
pos_incident_create("ZyPx6vF0", "Cancel position without the administrator", "Ivanov I", lambda err:
    alert(err.msg))
```

This example will create an incident with the "Cancel position without the administrator" type, associated with the terminal, the GUID of which is "ZyPx6vF0", and the cashier "Ivanov I".

In order to transfer or restore the detector configurations, you can use the **pos_import_detector()** function. This function accepts data in xml format containing the detector configuration.

```
with open("pos_detectors.xml") as detectors_config:
    pos_import_detector(detectors_config.read())
```

This example will delete the current detector configuration and restore it from the pos_detectors.xml file.

ActivePOS reports

The **generate_pos_report()** function can be used to generate ActivePOS reports. The function has 4 arguments:

- report type;
- the lower limit of the time interval in which the data for the report will be searched;
- the upper limit of the time interval in which the data for the report will be searched;
- the function to which the object containing the report will be sent.

```
import time
from pos_utils import ReportType

def report_ready(res):
    with open("pos_report.ods", "w") as report:
        report.write(res.zipped_report)

generate_pos_report(ReportType.VIOLATIONS_REPORT, str(int((time.time() - 24 * 60 * 60 * 10) * 1e6)),
    str(int(time.time() * 1e6)), report_ready)
```

This example generates a "Violation Report" for the last 10 days and saves it to the file pos_report.ods.



The module pos_utils.py contains a description of the **StringFilter**, SearchFlags, **ReportType** and **IncidentFlag** classes, and is located in the **pyredist** folder.



The time is in microseconds in **UNIX time** format based on the timezone configured on server.



- [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 for easy configuration of rules in the video surveillance system. It allows you to set the desired reaction to a particular event in the system in a few clicks, without having to dig deep into the *scripts* 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 necessary number of schedules on server, and then automate the server's operation by applying schedules using rules to server objects.

To create a new schedule:

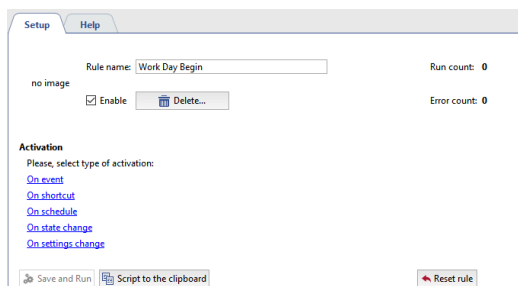
1. Open the **Settings** window.
2. Select **Automation**.
3. Click the **Create new schedule...** link.
4. Name a schedule.
5. Set the **Snap to 30 minutes** checkbox if you want the schedule divided into 30-minute zones. If this checkbox is cleared, the schedule will not be divided and the actual zone 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.

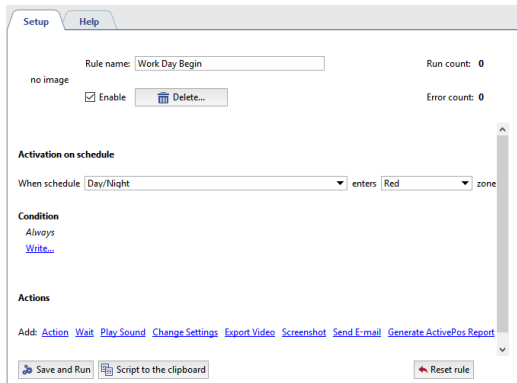
To use a schedule:

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.

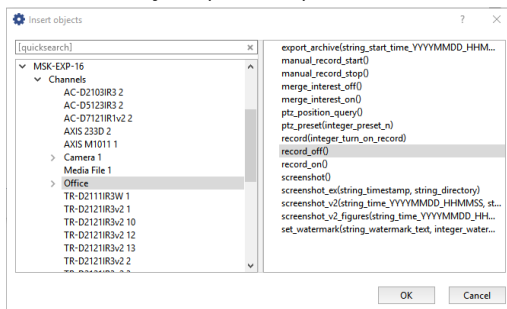


5. Select the previously created schedule from the **When schedule** list and select the zone that, when entered, should trigger execution of the action.

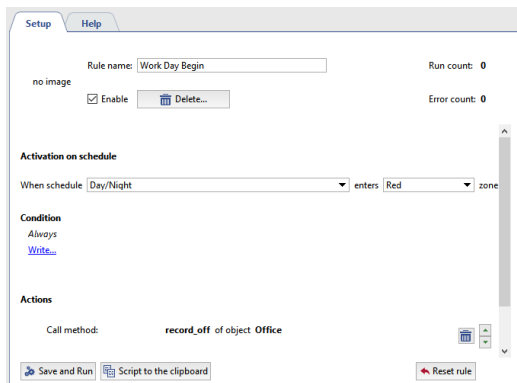
6. If necessary, specify condition for the execution of the rule, or leave the default value (the rule will always be executed when the schedule enters the specified zone).
7. In the list of possible actions, click the **Call method** link.



8. Select an object (camera) and action to be executed (record_off).

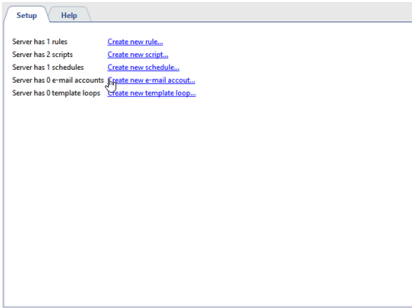


9. Verify that the rule has been correctly constructed and click **Save and run**. The rule will be active in the system, and recording will be disabled for the Lancam-CD812 camera when the schedule enters the specified zone.



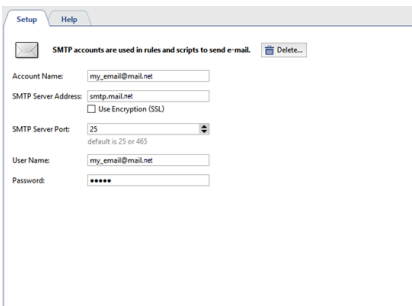
Adding an email account

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.net, the SMTP server is "smtp.mail.net".
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.net account, the username matches the full email address, e.g. "my_email@mail.net" 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](#)

Template loop

In order to create a new template loop, open the settings, select **Automation** and click **New template loop**.

Specify the following parameters in the window that opens:

1. **Loop name** - set any name you like.
2. **Monitor number** - select the number of the monitor on which the template loop view will be displayed.
3. **Activation on shortcut** - press any key or combination of keys to start the loop.
4. **Loop order** use **Add template** and **Add channel** buttons to add templates or channels that will be displayed in this loop. Use arrow keys to change the template and channel display order.
5. Set the display time for each template or channel, in seconds.
6. Set the **Enable** flag to display the customized loop on the monitor upon pressing hotkeys.

Check correctness of the specified settings and press **Save and Run**.



- [Rules](#)
- [Scripts](#)
- [Schedules](#)
- [Examples of the rules and scripts](#)

Examples of the rules and scripts

This section provides examples of the most popular rules and scripts. With their help, you can use real examples to understand the principles of automation and configure automation in your video surveillance system. Each example is accompanied by a description, as well as examples describing the possibilities of applying a rule/script.

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.net", ["addressee@mail.net"],\
    "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; channel name: Camera 1; 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:\VMS\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:\VMS\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.net

To: addressee@mail.net

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.net

To: addressee@mail.net

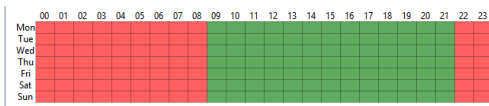
Subject: Health turns good

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.

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.



2. 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.
3. Then click on **Filter** and in the **Object** window check alarm input box, in our case it is "Emergency exit(door)".
4. 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.
5. 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: Input High to Low

Objects: All objects Filter... Gate 1

Condition

`object("Night").state("color") == "Red"`

+ Add condition

Actions

Call method: `set_output_high` of object Siren

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: Input Low to High

Objects: [All objects](#) Filter... Gate 1

Condition

`object("Night").state("color") == "Red"`

[Add condition](#)

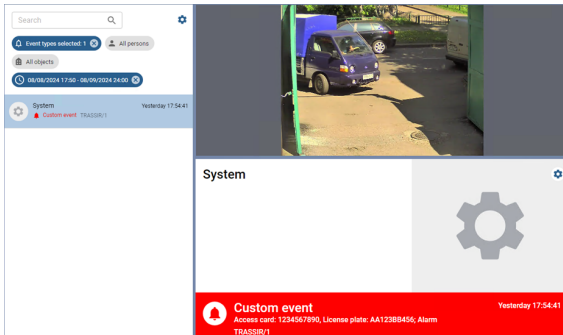
Actions

Wait (seconds): 5 sec

Call method: `set_output_low` of object Siren

Creating and displaying user messages in Access Control log

In this example, we will consider a rule that creates a custom event and displays it in the TRASSIR ACS log



1. **Create a new rule** and select **Activation on shortcut** activation type. Press the key that will execute the rule in the window that opens, in the **On keyboard** field.
2. Next, press **Action**, in the window that opens select **Access Control** section and the **Access point**. In the right window, select **emit_custom_event(string_title, string_color, string_person_guid, string_details_json)** string. Press **OK**. After that, it will be possible to specify the custom event parameters in the rule.

Activation on shortcut

On Keyboard: F2 On Release: On Panel: User function 102

Conditions

Always

Actions

Call method: `emit_custom_event` of object TRASSIR/1

title: "Custom event"
 color: "#FF0000"
 person_guid: ""
 details_json: '{"card_id": "1234567890", "plate": "AA123BB456", "comment": "Alarm"}'

[Add](#) [Action](#) [Help](#) [This window](#) [Change settings](#) [Export table](#) [Screenshot](#) [Send E-mail](#) [Generate Activation Report](#)

3. Specify the following parameters for the custom event:

- Enter the title of the custom event into the **title** field.
- In the **color** field, enter the color of the event (in HEX format). All TRASSIR ACS events created by this rule will be colored with it.
- Enter the GUID of the TRASSIR ACS# person, on whose behalf the custom events will be displayed, into the **person guid** field.
The process for obtaining the server object's GUID is described in the TRASSIR SDK in section [Working with objects](#).
To display the event on behalf of the system, type "" (empty quotes).
- In the **details json** field, enter the event parameters (in JSON format, in single quotes) that will be displayed in the custom event as additional information. You can use the person properties as parameters:
For example,

```
'{"card_id": "1234567890", "plate": "AA123BB456", "comment": "Alarm"}'
```

Where,

card_id - card number;

plate - license plate number;

comment - optional comment.



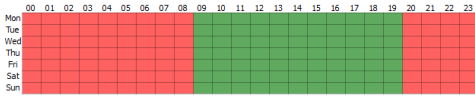
If the TRASSIR ACS person's GUID is entered in the *person guid* field, then the **card_id** and the **plate** properties must contain the person's card number and the license plate number as entered in this *person's parameters*.

If the *person guid* field is empty, any values can be specified.

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():
```

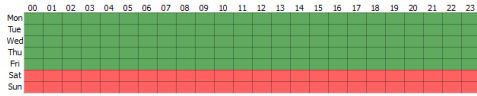
```
set_fps_on_all_devices(12)

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:\VMS\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:\VMS\Screenshots\Low_quality")
    elif event.flags & LPR_WHITELIST :
        obj(event.channel).screenshot_ex("", r"C:\VMS\Screenshots\Whitelist")
    elif event.flags & LPR_BLACKLIST :
        obj(event.channel).screenshot_ex("", r"C:\VMS\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:\VMS\Screenshots\Low_quality" folder

```
if event.quality == 0 :
    obj(event.channel).screenshot_ex\
```

```
("", r"C:\VMS\Screenshots\Low_quality")
```

- If the recognized number is on the whitelist, a screenshot will be captured and placed in the "C:\VMS\Screenshots\Whitelist" folder

```
elif event.flags & LPR_WHITELIST :
    obj(event.channel).screenshot_ex\
    ("", r"C:\VMS\Screenshots\Whitelist")
```

- If the recognized number is on the blacklist, a screenshot will be captured and placed in the "C:\VMS\Screenshots\Blacklist" folder

```
elif event.flags & LPR_BLACKLIST :
    obj(event.channel).screenshot_ex\
    ("", r"C:\VMS\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:\VMS\Screenshots\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)
```

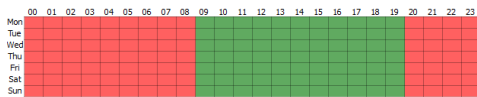
2. The function shot(event) defines a condition whereby if the event is a cashier signing in, then a screenshot from the associated channel is saved to "C:\VMS\Screenshots\Cashiers".

```
def shot(event):
    if event.type == "POS_CASHIER_REGISTRATION":
        obj(event.associated_channel).screenshot_ex\
        ("", r"C:\VMS\Screenshots\Cashiers")
```

Placing a warning flag on a receipt when alcohol is sold at night

Each store has certain scenarios of events that are alarming and require verification. ActivePOS allows you to mark such events with alarm bookmarks and add arbitrary comments. After that, you can sample these events for further analysis. In this example, we will consider a script that marks the sale of alcohol at night as an alarm 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:\VMS\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:\VMS\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
timeout(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()))
```

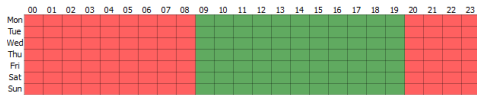
4. The 'export_wait' function determines if an archive export is currently underway from a previous instance of the script; if it is not, then action0_2 is executed.

```
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.

-
- 258

Modeling 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.

259

```
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 expand the basic server functionality by configuring the following additional modules:

- *ActiveDome* is a module for automated control of PTZ cameras.
- *ActivePOS* is a module for monitoring point-of-sale operations.
- *AutoTRASSIR/AutoPass* 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.
- *Camera image quality indicator* is a module that allows you to analyze the quality of the camera image and report visibility impairment.



The availability of any of the modules described is determined by your license.

ActiveDome - Automated PTZ-camera control

ActiveDome is a module for PTZ cameras robotic control. It can be used to provide instant positioning of PTZ camera on the desired object. The object tracking can be performed in *two modes*: manual or automatic.

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. Install and configure cameras to be used in the 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.
- Object tracking both manually and automatically using *Neuro Detector*.



- *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 for the PTZ camera is transmitted from *Neural Detector*. At the same, the modules transmit coordinates of objects to the ActiveDome, taking into account their future displacement during the rotation of the camera. They can also distinguish objects from each other and remember their history (the path traveled), which allows you to point the camera to them in turn to record a detailed image of each. The video camera switches between the objects accompanying them for a time, which is called the "redirection interval" and is configured in *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](#)

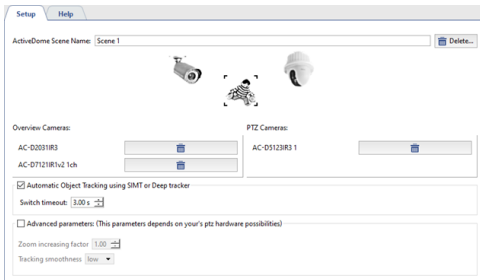
Creating an ActiveDome scene

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.

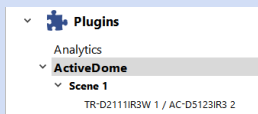


An inventory of available PTZ cameras is generated from the list of PTZ devices that have been bound to an appropriate [serial port](#). Additionally, you can use SpeedDome PTZ IP-cameras. IP cameras are added and configured just like other [IP devices](#).

- 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](#).



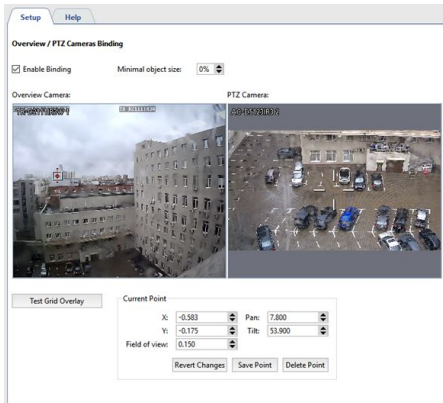
A list of all created scenes is shown in the settings tree.



- [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.

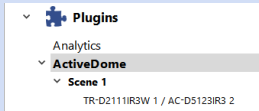
Example of a correctly configured grid:



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. Cash registers and video surveillance server are combined into 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 necessary, the server administrator sets up filters for suspicious events, the occurrence of which requires additional attention by monitoring personnel.



- [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
- Frontol software
- R-Keeper
- dStore POS of MICROS company
- SuperMag UKM 4 cash desk system
- SHTRIH-LIGHTPOS POS-system
- IBS GAS software package
- Set Retail cash program
- 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



Not all counting machines can work directly with the server, some require a signal converter that works on **RS-485** interface. Contact technical support for detailed advice on the operation of each device.

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 the POS terminals, you need to specify the IP address, port and protocol in the trading system software. Check the documentation from the vendors of the cash register software for each of the supported trading systems settings.



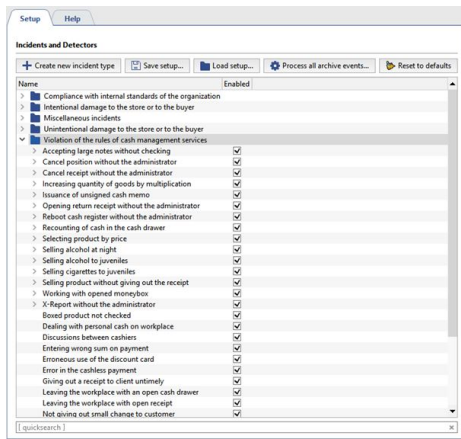
- *ActivePOS - Point-of-sale operations monitoring*
- *ActivePOS features*
- *ActivePOS incidents and detectors*
- *Configuring POS terminals*
- *Configuring R-Keeper POS terminals*
- *DSSL XML for ActivePOS*
- *Using ActivePOS in scripts*

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.

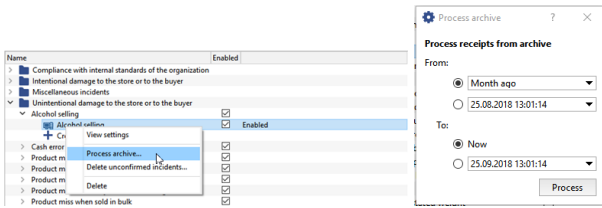
You can use the following types of incidents:

- **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 during the operation any detector has been deactivated and the staff activities analysis has not been performed, you can activate it at any time and process the archive of receipt which has been already saved with it. To do this, mark the required detector in the list and select **Archive processing...** item in context menu. Specify the period of time, the receipts of which should be processed by this detector in the opened window and press **Process**.



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

You can create an unlimited number of the incident type and detectors to detect them. In order to create an incident press **Create new incident type** button or select **Create new incident type...** item in the context menu. Enter the **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.

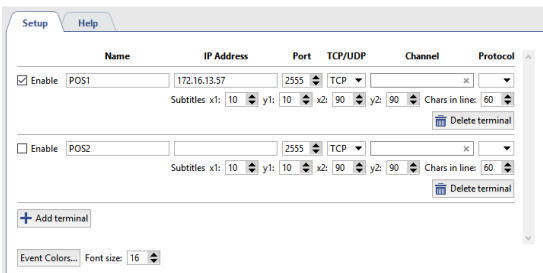
Now if a cashier will register discount card sales and hand out gift to the client, we will see it in the incident report (see section ??? in "Operator's Manual").



ActivePOS incidents and detectors

Configuring POS terminals

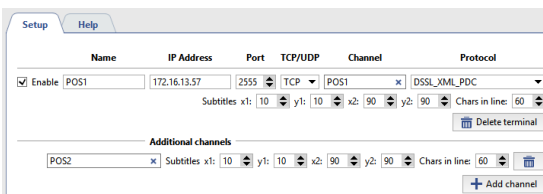
In order to add POS-terminal click **ActivePOS** -> **Terminals** menu items and press **Add POS** button.



Specify the following in the point-of-sale terminal's settings window:

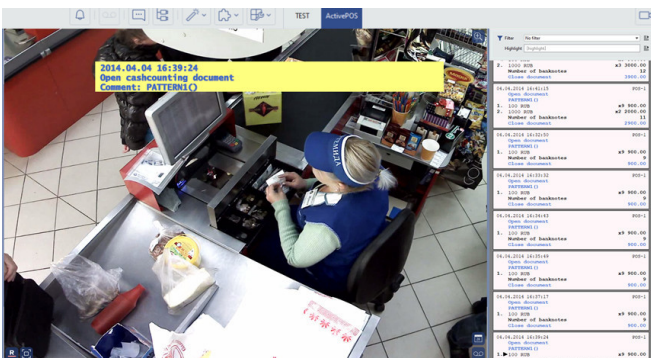
- **Name** - The terminal's display name in the system.
- **IP address** - The address of the server providing information about transactions.
- **Port** - The server port.
- **TCP/UDP** - The transport protocol.
- **Channel** - The camera to which the point-of-sale terminal will be bound.
- **Protocol** - 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**.



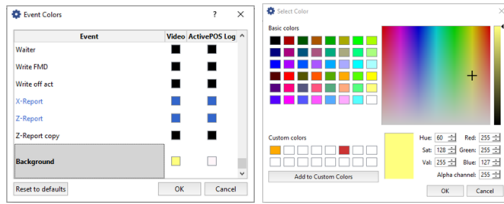
The number of additional channels is determined by corresponding software license.

If the settings are correct, the events generated by the POS terminal will be displayed in the operator interface in the Event Log of POS terminals and on the selected channel.



You can select the color and font of the events generated by POS terminals, in the event log and on video, if necessary. To do this:

- Set the font high in the **Font size** field. In order to choose the event colors, press **Event colors...**
- In the opened window, select the color of the event by clicking on the corresponding color icon. The colors for similar events can be changed by dragging the color icon from one event to another.



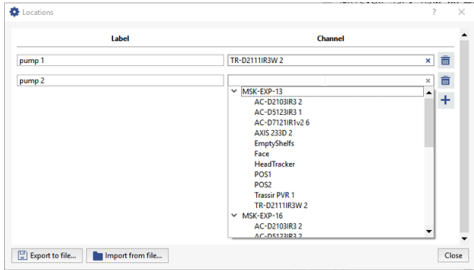
When defining the background color of ActivePOS events, use **Alpha channel** field to set the background transparency level: from **0(fully transparent background)** to **255(opaque background)**.

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 on fuel dispensers. Using special identifiers transmitted to the server along with payment data, you will bind payment receipt with certain video channel. Thus, the image of each fuel dispenser will be overlaid with information about the payment for fuel dispensed only through it.

To do this press **Location settings...** button and establish matching of **Identifiers** and **Video channel**.



You can use **Export to file...** and **Import from file...** buttons to transfer location settings from one server to another one.



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.

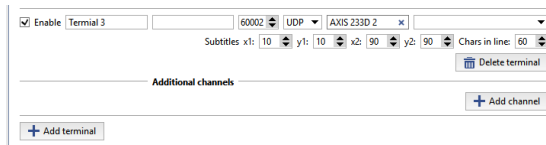
The server handles this peculiarity with an automation script that receives R-Keeper transactions, analyzes their contents, and redirects them to the appropriate ActivePOS terminal.

Configuration of the server for the R-Keeper protocol consists of three steps:

1. Terminal configuration

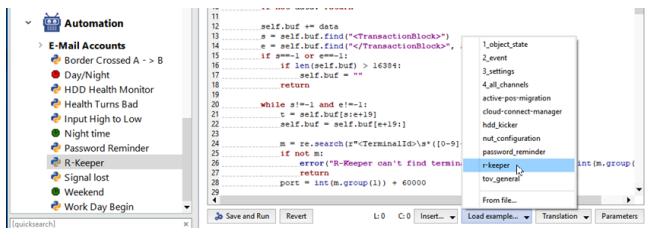
R-Keeper POS-terminals must be configured as follows:

- **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:



The server awaits for the data on port 4444, by default; you can change this port number by editing the following lines, if necessary:

```
cont = Container()
cont.server = EchoServer('127.0.0.1', 4444)
cont.server_thread = ServerThread()
cont.server_thread.quit_flag = 0
cont.server_thread.start()
```

3. Editing the configuration file

For correct processing of the R-Keeper transactions, you should edit **pos-rkeeper.ini**, which is located in the server 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



You can find the configuration example in pos-rkeeper.sample.ini in the server 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.



The ranges of different events must not overlap for correct operation.
A configuration file string beginning with ";" is a comment and is not analyzed.

There is no need to restart the server to check the modified settings, just turn off and on the adjustable ActivePOS terminal.



- *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_POSITION_SUB_ADD</i>	Adding an additional item
<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_NOT_FOUND</i>	Item not found
<i>POSNG_POSITION_SCAN_OUT_OF_RECEIPT</i>	Position not on receipt was scanned
<i>POSNG_POSITION_IMIT_ADD_BY_SCANNER</i>	Scanning of the items without adding the item to the receipt
<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
<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_SYSTEM_SHOW_PRODUCT_PRICE</i>	Check price
<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_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

Event type (<i>event_type</i>)	Description
<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
<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_POSITION_RETURN</i>	Return of goods
<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
<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

Event type (<i>event_type</i>)	Description
<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_RECEIPT_NUMBER</i>	Receipt number
<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_SETTING_PRICES_AT_FILLING_STATIONS</i>	Setting prices for gas stations
<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

Event type (<i>event_type</i>)	Description
<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_STORE_MODE</i>	Entering the store mode
<i>POSNG_EXIT_STORE_MODE</i>	Exiting the store mode
<i>POSNG_SUMMARY RECEIPT</i>	Opening the single-check window
<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_INPUT_OF_FUEL_QUANTITY_LITRES</i>	Entering the fuel quantity (liters)
<i>POSNG_INPUT_OF_FUEL_QUANTITY_RUBLES</i>	Entering the fuel quantity (rubles)
<i>POSNG_FUELING_TO_FULL_TANK</i>	Refuel to full tank
<i>POSNG_SELECT_TYPE_OF_FUEL</i>	Selecting the fuel type
<i>POSNG_ADD_FUEL_WITH_FUEL_BUTTON</i>	Adding fuel with the [+Fuel] button
<i>POSNG_ADD_CAR_WASHING_WITH_CAR_WASH_BUTTON</i>	Adding car wash by [+Car wash] button
<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

Event type (<i>event_type</i>)	Description
<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
<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_CHANGE_TYPE_OF_PAYMENT</i>	Changing the payment type
<i>POSNG_MIXING_TYPE_OF_PAYMENT</i>	Mixed payment type
<i>POSNG_OTHER_TYPES_OF_PAYMENT</i>	Other payment types
<i>POSNG_POST_PAYMENT_MODE</i>	Post-payment mode
<i>POSNG_PREPAYMENT_MODE</i>	Prepayment mode
<i>POSNG_CANCEL_PAYMENT_WITH_BONUS_CARD</i>	Cancellation of bonus card payment
<i>POSNG_PAYMENT_WITH_EXTERNAL_SYSTEM</i>	Payment via integrated systems
<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
<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
<i>POSNG_PAYMENT_FUEL_THEFT</i>	Fuel theft

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

Event type (<i>event_type</i>)	Description
<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_EXIT</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_CANCEL_BONUS_CARD</i>	Cancellation of bonus card use
<i>POSNG_BONUS_CARD_BALANCE_REQUEST</i>	Bonus card balance inquiry
<i>POSNG_BONUS_CARD_ACTIVATE</i>	Bonus card activation
<i>POSNG_BONUS_CARD_DEPOSITION</i>	Deposit to bonus card
<i>POSNG_BONUS_CARD_BONUS_DEPOSITION</i>	Adding bonuses to the bonus card

Event type (<i>event_type</i>)	Description
<i>POSNG_BONUS_CARD_UNREGISTER</i>	Bonus card registration
<i>POSNG_BONUS_CARD_BALANCE_DETAILED_REQUEST</i>	Detailed bonus card balance inquiry
<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
<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

Event type (<i>event_type</i>)	Description
POSNG_REPORT_BY_BANK_OPERATIONS	Bank operations report printed
POSNG_REPORT_BY_SHIFT	Shift report printed
POSNG_REPORT_WRITE_OFF_ACT	Write-off report printed

Service events

Event type (<i>event_type</i>)	Description
POSNG_COMMENT	Comments
POSNG_ACTIVITY	Operator activity
POSNG_ACTION	Action taken
POSNG_FRAUD	Incident event generated from a script
POSNG_ERROR	Error
POSNG_ERROR_PRINTER	Printer error
POSNG_ERROR_BANK_PAYMENT	Bank (payment) error
POSNG_ERROR_NOT_A_NUMBER	Non-numeric value entered
POSNG_ERROR_NUMBER_TOO_LARGE	Number entered is too large
POSNG_BANK_CHECK_RESULTS	Bank reconciliation
POSNG_BANK_DAY_FINAL_RESULT_REQUEST	Daily bank totals requested
POSNG_BANK_DAY_CLOSE	Bank day closed
POSNG_ERROR_SYSTEM	System error

Gas Station

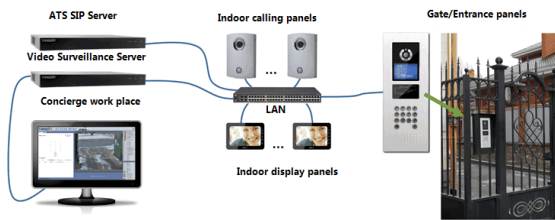
Event type (<i>event_type</i>)	Description
POSNG_START_OF_TANK_UP	Starting refueling at the fuel dispenser
POSNG_END_OF_TANK_UP	End of refueling at the fuel dispenser
POSNG_FUELING_NOZZLE_REMOVED	The fueling nozzle is removed
POSNG_FUELING_NOZZLE_HANGED	The fueling nozzle is hung up
POSNG_PAUSE_OF_FUELING	Pause / Stop refueling
POSNG_START_OF_FUEL_DISCHARGE	Start of fuel dumping
POSNG_END_OF_FUEL_DISCHARGE	End of fuel dumping
POSNG_SELECT_OF_GASOLINE_STATION	Selecting petrol pump in the interface
POSNG_CANCEL_SELECTION_OF_GASOLINE_STATION	Deselecting petrol pump in the interface
POSNG_RECONCILIATION_WITH_FUEL_TERMINAL	Checking results with the fuel terminal



- [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 door phone system into a unified complex.



The list of available features depends on the module and is defined 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	+	+	
A full scale SipPhone in the operator 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

The screenshot shows the 'Setup' window with two tabs: 'AMI' and 'Call archiver'. Both are marked as 'Connected'. The 'AMI' section includes fields for 'Current state', 'Connection Options' (AMI host: localhost, AMI port: 5038, AMI user: admin, AMI password: ****), and 'Monitoring phones'. The 'Call archiver' section includes fields for 'Current state', 'Connection Options' (Driver: MySQL, Host: localhost, Port: 3306, Database name: asteriskcdrdb, User: Gringo, Password: ****, Audio files URL: http://localhost, FTP user: FTPuser, FTP password: ****, Max depth: 3), and 'Setup associations...'.

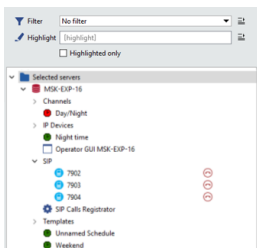
AMI (Asterisk Management Interface) is an Asterisk(API) server control interface. With it TRASSIR makes connection to Asterisk server via TCP, initiate instructions execution, receives the result of their execution and receives current status of SIP-phones.

Enter the following parameters to connect to Asterisk:

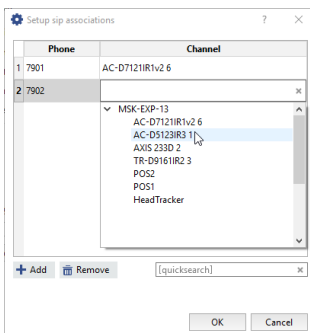
- **AMI server** - server ip-address or DNS-name.
- **AMI port** - network port of server (by default: 5038).
- **AMI user** and **AMI password** - server account name and password.

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).



You can output video from the camera to operator's display when calling to the phone. It requires **Set up associations...**, that is, to indicate the SIP-phone number and the corresponding video channel.



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, the below described settings should be configured. After that, the 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, an account for each server should be created on the Asterisk server, which will be used by the operator 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.



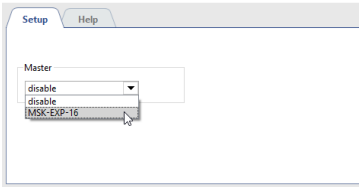
Selecting a server as **Master TRASSIR** will be possible only after the connection to it. See detailed description of connection to server procedure in the section [Connecting to a new server](#).



- [IP-video intercom](#)
- [Connection to Asterisk server](#)

SipPhone on the client settings

In order to use the SIP-telephony module, you need to adjust the below described settings.



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/AutoPass - Automated license plate recognition

AutoTRASSIR module is designed for automatic recognition of license plates caught in the video camera field of view. It can be used in a video surveillance system to monitor vehicle entry/exit from the territory of industrial areas, parking lots, checkpoints, etc.



The 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 is identical.

The server uses several AutoTRASSIR module versions, that have a set of features:

The **AutoTRASSIR (LPR1)** and **AutoTRASSIR (LPR3)** modules run only **locally** on all servers.

The **AutoTRASSIR (LPR5)** plugin runs:

- **local** for **NeuroStation** and **QuattroStation** server with TRASSIR OS;
- **remotely** on all 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**.
The **AutoTRASSIR (LPR5)** module can use TRASSIR OS server of **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**.

HSC AutoPass is a vehicle detection module using state-of-the-art recognition algorithms, including license plate and vehicle type recognition. The module is used to detect vehicles, including special vehicles (ambulance, fire department, police, etc.).



HSC AutoPass supports only cameras with in-built LPR module and can be launched only on certain servers. View the list of supported equipment on [our website](#).

In addition, the server means can provide interaction with other systems (for example, access control systems, video and audio control) and equipment (barriers, operational units, etc.).

AutoTRASSIR features:

- **License plate reading by templates and without them**

The module can recognize license plates of the following countries: Russia, Ukraine, Turkey, Taiwan, Moldova, Kyrgyzstan, Kazakhstan, Spain, Georgia, Belarus, China, etc. The operation of the recognition templates depends on the selected AutoTRASSIR plugin version:

LPR5 - with the help of the server 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 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.

HSC AutoPass features:

- **License plate reading by templates and without them**

The module can recognize license plates of the following countries: Russia.

- **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/AutoPass general settings*](#)

Selecting, installing, and configuring cameras to work with the AutoTRASSIR/AutoPass 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/AutoPass module. We recommend that you read the Administrator's Guide very carefully.

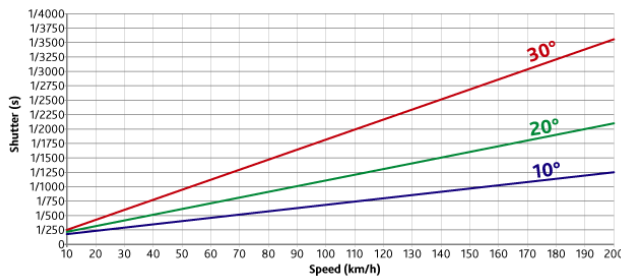
Camera requirements:

- AutoTRASSIR (LPR5) module supports video from any surveillance camera.
- HSC AutoPass supports only TRASSIR cameras with in-built LPR module.
- We recommend to use AutoTRASSIR (LPR1) or AutoTRASSIR (LPR3) module on grayscale videos featuring greater resolution and sensitivity (in comparison with color videos, the processed color videos are converted to grayscale during the detection).
- An analogue camera used with the AutoTRASSIR module must feature 500 TVL (television lines) or greater resolution.

Image quality requirements:

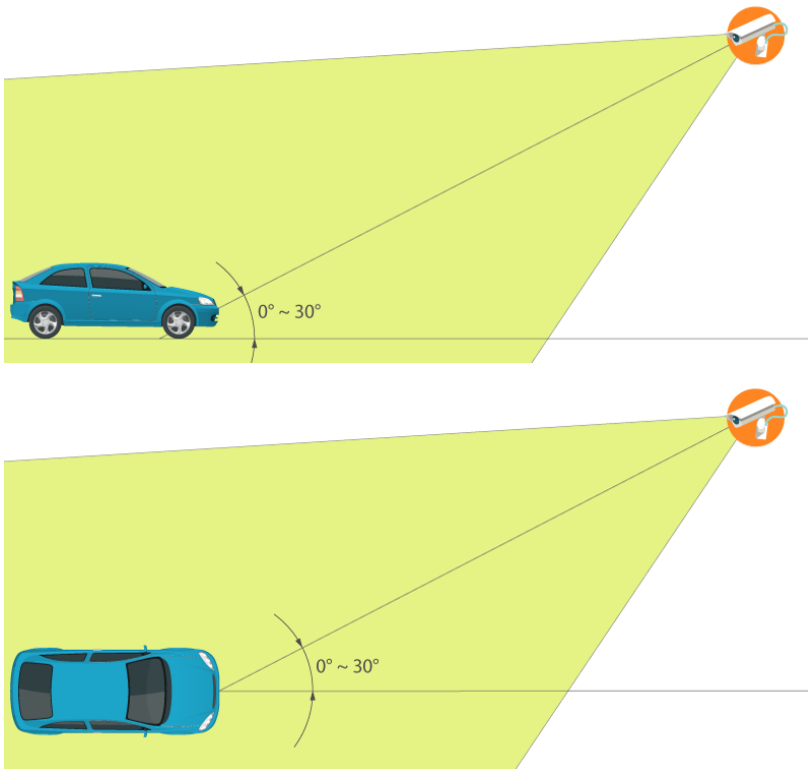
- The primary problem affecting image quality during license plate recognition is motion blur. To avoid motion blur, the shutter speed (the time each frame is exposed) must be very small.

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. To work with the AutoTRASSIR module, the camera must support the manual shutter function! 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).

Camera angle requirements:



- AutoTRASSIR (LPR5) and HSC AutoPass modules support camera angle (up to 30°) to the vehicle movement direction. The greater the angle, the lower the recognition quality.
- The AutoTRASSIR (LPR5) module supports camera angle (up to 30°) to the vehicle movement direction. The greater the angle, the lower the recognition quality.
- The camera used with AutoTRASSIR (LPR1) and AutoTRASSIR (LPR3) modules must be installed in a way that the license plate surface appears at the right angle to the visual axis of the camera to exclude recognition errors.



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.

License plate in frame position requirements:

- AutoTRASSIR (LPR5) and HSC AutoPass allow for the horizontal deflection of up to 5° of the license plate without the recognition quality degradation. The 5°-10° deflection of the license plate can cause errors in the recognition of certain characters.
- AutoTRASSIR (LPR5) allows for the horizontal deflection of up to 5° of the license plate without the recognition quality degradation. The 5°-10° deflection of the license plate can cause errors in the recognition of certain characters.
- AutoTRASSIR (LPR1) and AutoTRASSIR (LPR3) modules require the license plate to be positioned horizontally in the frame.



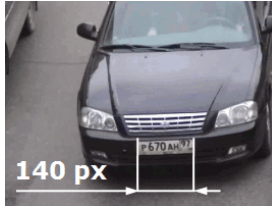
If swing barriers are used to control entrances/exits, we recommend installing the camera in such a way that the swing barrier does not reach the bottom of the screen. Otherwise, the swing barrier may cause false positives.

Lighting conditions requirements:

- Verify that there is sufficient brightness during nighttime conditions. To do this, record a small video. License plate numbers should be easily recognized during playback. If the license plates on the image are too noisy or dark, the brightness 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 at night the camera will be overexposed by the headlights of passing vehicles.

Other camera settings and image requirements:

- The superposition of any information onto the image (date, camera name, etc.) must be disabled.
- Autofocus must be disabled.
- The focal distance must ensure that the license plate of the vehicle is about 120 to 140 pixels horizontally on the processed video.



- [*AutoTRASSIR/AutoPass - Automated license plate recognition*](#)
- [*Setup AutoTRASSIR module on a channel*](#)

AutoTRASSIR/AutoPass general settings

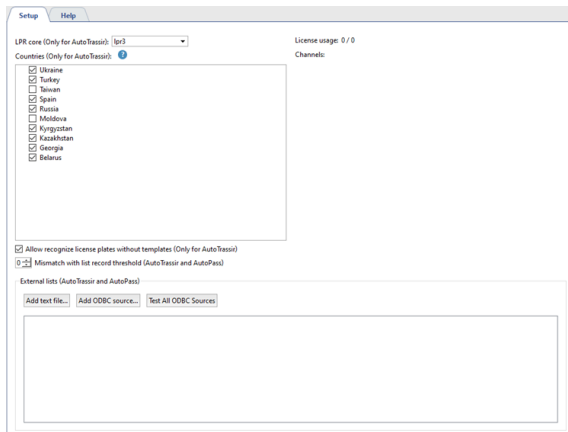


Before the AutoTRASSIR configuration, we strongly recommend you to read the section [AutoTRASSIR/AutoPass - Automated license plate recognition](#).

For the license plate recognition system to operate correctly, the camera must include certain features and be installed and set in a proper way. Please familiarize yourself with [Selecting, installing, and configuring cameras to work with the AutoTRASSIR/AutoPass module](#).

Before using the AutoTRASSIR module, be sure you have correctly configured your [database connection](#).

Main parameters of the AutoTRASSIR/AutoPass module are displayed on the **Plugins** -> **AutoTRASSIR/AutoPass** tab of the **Settings** window.



- **Only for the AutoTRASSIR module:**

In the **LPR core** configuration, select the version of AutoTRASSIR.



After changing the version of the module, the server must be rebooted.

- **Only for the AutoTRASSIR module:**

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.

The recognition template for the **HSC AutoPass** module is chosen during its setting (see [Setup HSC AutoPass module on a channel](#)).



AutoTRASSIR/AutoPass 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 the 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.

- **Only for the AutoTRASSIR module:**

The **Licenses usage** field shows the number of currently connected channels out of the maximum allowed (which is limited by your license).

- **Only for the AutoTRASSIR module:**

The **Channels** section displays the list of channels for which AutoTRASSIR has been activated.

- **For AutoTRASSIR and HSC AutoPass modules:**

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.

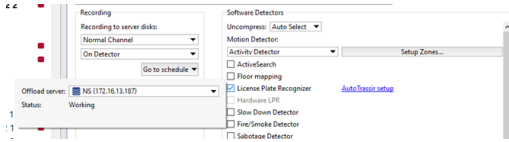
In case AutoTRASSIR makes a mistake in 1 symbol when recognizing a license plate and recognizes **a221co177** or **m221co77** instead of **m221co177** number, due to 1 symbol mismatch, the mistakenly recognized number will match with the number from the whitelist.

- **For AutoTRASSIR and HSC AutoPass modules:**

The **External lists** area displays a list of all of the *external lists connected to AutoTRASSIR*.

AutoTRASSIR module standard setting workflow

1. Install and configure cameras that will be used for license plate number recognition.
2. Go to the **Channels** node of the settings tree, select the desired channel from the list, and check **License Plate Recognizer** for the channel in the **Software 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**.

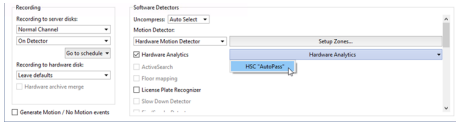
4. Verify that the AutoTRASSIR module is properly functioning by [creating a simple template](#).
5. Configure "black", "white" or "info" plate lists:
 - Using [internal lists](#).
 - You can also connect external lists, stored in external text files or databases.



The settings for connecting external lists of license plate numbers differs for **Windows** and **TRASSIR OS**.

HSC AutoPass standard setting workflow

1. Install and configure cameras that will be used for license plate number recognition.
2. Go to the **Channels** node of the settings tree, select the desired channel from the list, and check **Hardware Analytics** for the channel in the **Software Detectors** area.
Press **Hardware Analytics** and choose **HSC AutoPass**.



3. Configure the module operation on the chosen channel (see [Setup HSC AutoPass module on a channel](#)).
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**.



- [Setup AutoTRASSIR module on a channel](#)
- [Creating an AutoTRASSIR/AutoPass 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 on Windows](#)
- [Connection of the external number lists in TRASSIR OS](#)

Setup AutoTRASSIR module on a channel



Before beginning this configuration process, be sure that the camera to work with AutoTRASSIR/ AutoPass 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/AutoPass**. For a detailed description, see section *AutoTRASSIR/AutoPass general settings*.

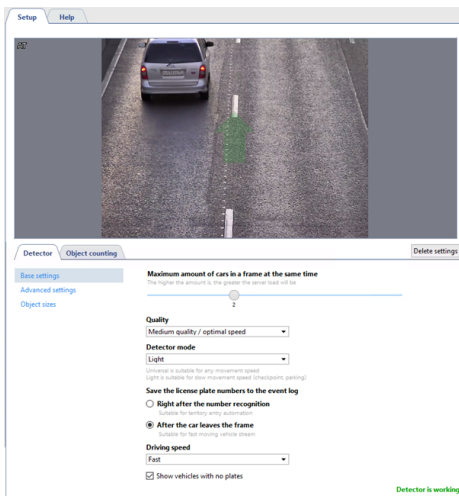
HSC AutoPass module setup is described in *Setup HSC AutoPass module on a channel*.



- *AutoTRASSIR/AutoPass - 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 on Windows*
- *Connection of the external number lists 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** is the maximal number of cars that the detector will simultaneously detect in a frame. As a rule, the value is selected depending on number of lanes in a frame. The higher the value is, the higher is the load on the analytics server.
- **Quality** - determines the quality performance of the detector:
Best quality / low speed for recognizing license plates in the distance. The image of higher quality is used in this mode, which significantly increases the load on the analytics server.
Medium quality / optimal speed for recognizing license plates at medium and close distances. This mode makes the best use of the analytics server resources and can use an image of medium quality for detection.



The value of the **Quality** should match the **License plate recognition** neural detector settings on the analytics server.

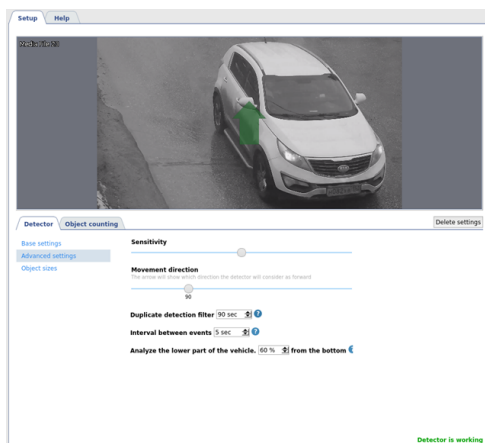
Read more about the server analytics configuration in [Analytics](#).

- The **Detector mode** is selected in dependence on the scene in which the license plates are recognized:
Simplified - this mode is suitable for scenes when the vehicle moves at low speed (at the barrier, in the parking lot, etc.).
Universal - this mode is suitable for all speed modes and provides high quality of license plate recognition, but at the same time, it significantly increases the load on the analytics server.
- **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.
- Set the **Show vehicles with no plate** flag to display events with unrecognized license plate number in the AutoTRASSIR log.

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 allows you to eliminate repeated detections of the same license number if it has been previously recognized. 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 **Interval between events** parameter allows repeated detections while the vehicle is continuously in the frame. This may be useful in case the license plate number was previously recognized incorrectly. An event will be sent only if the newly recognized license plate number is different. 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.

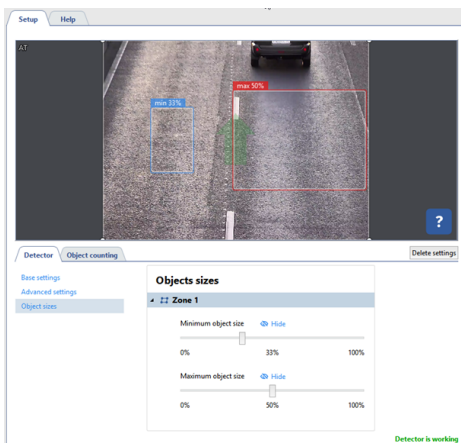




In the AutoTRASSIR log the movement in the direction of the green arrow is indicated by up arrow and the oncoming direction - by the down arrow. You can read more about recognized license plate number review in the [License plate recognition](#) and [Filtering current license plates](#) sections of the Operator's Guide.

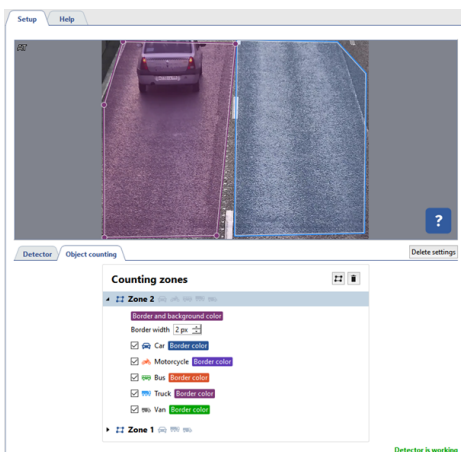
Plate	Time	Channel
15 15 15	11:51:05	AT
15 15 15	11:51:04	Highway
15 15 15	11:51:04	AT
NO PLATE	11:51:04	AT
15 15 15	11:51:03	Highway
15 15 15	11:51:03	AT
NO PLATE	11:51:02	AT
15 15 15	11:51:02	LPR test
15 15 15	11:51:02	AT
NO PLATE	11:51:01	AT
15 15 15	11:51:01	Highway

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.

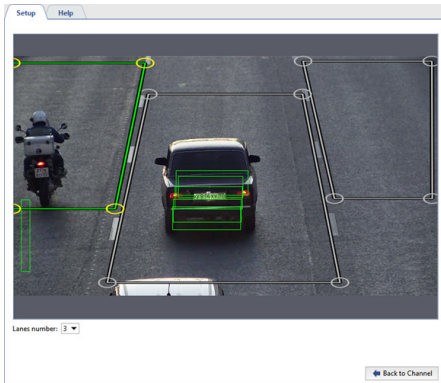
You can check the setting correctness in the [operator's interface](#).



- *AutoTRASSIR/AutoPass 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.



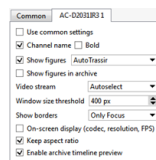
The standard commonly accepted lane width of a roadway is 3,5 meters. If the camera captures the roadway width which is 8 meters (that is not only the roadway, but the entire actual width of the image in meters). In this case you should select the closest to 8 meters value, which is 2 lanes.

- **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.

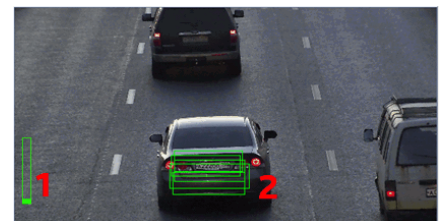


It is necessary to take into account depth of field and number of frames shot by the camera during the passage of the car inside the zone when selecting areas of recognition. Number of frames shot by the camera will directly depend on the speed of the car. It must be remembered as well that not all frames 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.

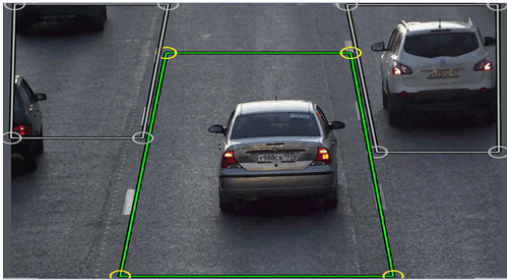
2. **Frame recognition quality** - is a rectangular indicator that displays recognition quality. Each rectangle is a separate frame used for license plate number recognition. Depending on whether or not the frame was suitable for recognition, the color of the rectangle will change from green (a "good" frame) to red (a "bad" frame).

Examples of module configuration:

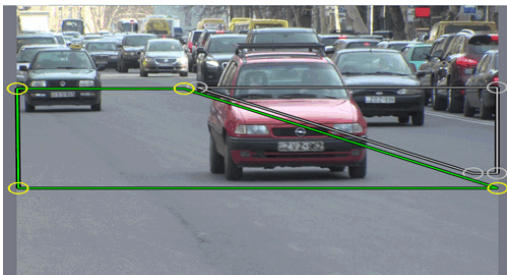
- To recognize license plate numbers of entering and leaving through the gate cars, you can select only the gate area. Cars passing on the road will be ignored in this case.



- You should draw a separate zone on each lane of the multilane roadways.



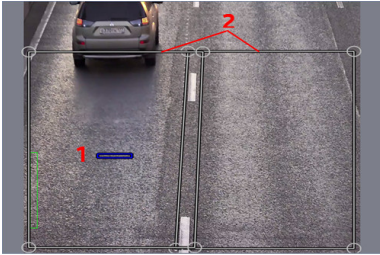
- In this example the camera has been installed so that the depth of field (the area of the image with the best image quality) covers only a small area in the middle of the frame. This is the same area that is relevant and useful for license plate recognition. There is no point in performing license 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/AutoPass 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**!



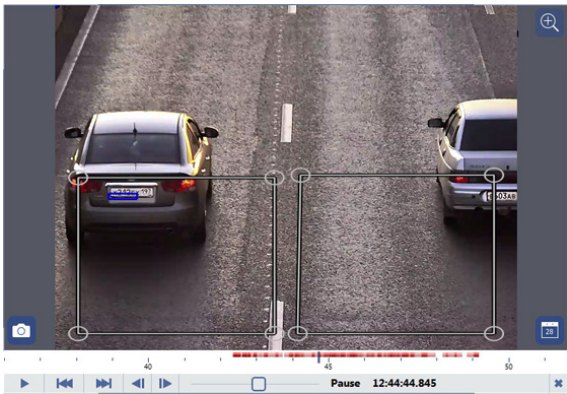
At this stage of the configuration it is not necessary to precisely determine the dimensions of the recognition zones. The recognition zones will be configured in step 6.

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.

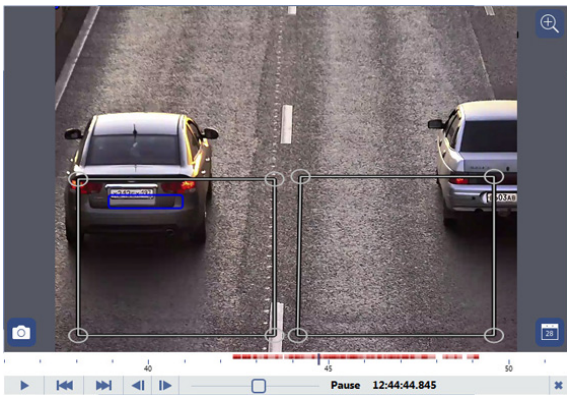


In the **Detector resolution** dropdown list, select **Preset**. The picture's resolution will be reduced in the best way possible, with minimal loss of quality and minimal additional load on the server's CPU.

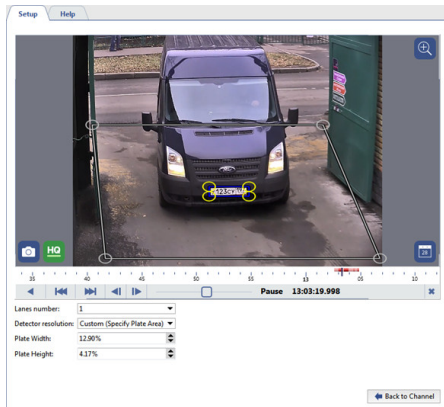


This situation may occur if a high-resolution camera is used to monitor a very narrow section of road. For example, if a 3-MP camera is used to monitor a single lane. Note that in this case the **expected license plate size** depends on the value of the **Lanes number** parameter.

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:

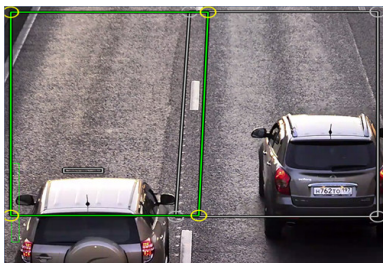
- associate a vehicle's passing with a specific lane (monitoring selected lanes for fixed-route vehicles, detecting vehicles passing on a walkway, etc.);
- save server resources by analyzing only the truly interesting and relevant areas of the image, minimizing the number of false activations of the detector.

For example:

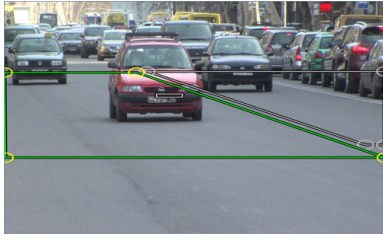
- To recognize the license plates of vehicles entering and exiting through a gate, you can assign only the area with the gate. In doing so, vehicles passing by on the road will be ignored.



- You should draw a separate zone on each lane of the multilane roadways.

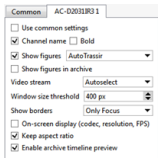


- In this example the camera has been installed so that the depth of field (the area of the image with the best image quality) covers only a small area in the middle of the frame. This is the same area that is relevant and useful for license plate recognition. There is no point in performing license 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.

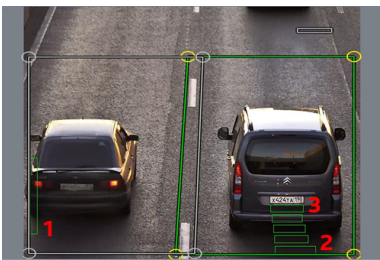


Upon setting the depth of field and assigning recognition zones, it should be born in mind how many frames the camera will be able to capture in the time period the vehicle passes through the zone. The number of frames the camera takes depends directly on the vehicle's speed. Additionally, note that 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:



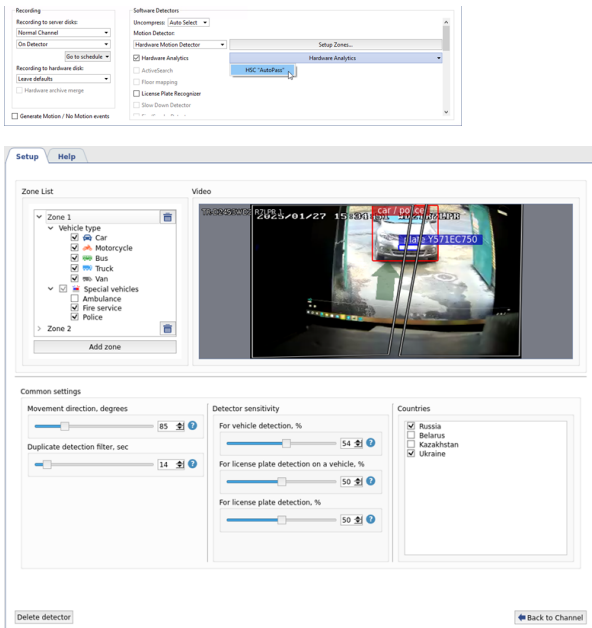
1. **Processing queue** - This indicator reflects the state of the queue for processing license plate numbers. If the vertical bar fills up and turns red, then AutoTRASSIR begins to drop frames. The processing queue will fill if the server's CPU is heavily loaded and unable to process the frames.
2. **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/AutoPass general settings](#)
- [AutoTRASSIR settings \(LPR3\)](#)
- [AutoTRASSIR \(LPR5\) setup](#)

Setup HSC AutoPass module on a channel

To activate the plugin, go to the *Channel settings* and in the *Software detectors* area select *Hardware Analytics*. Press *Hardware Analytics* and choose *HSC AutoPass*.



In the window that opens, configure the module operation settings:

- In the **Zones list** settings group, create up to 5 zones for vehicle detection. To do that, press **Add zone** and select an area on the video frame. In the zone settings, select **Vehicle types** and **Special vehicles** to trigger the detector in the zone.
- In the **Movement direction, degrees** parameter, set the traffic flow direction to be defined as the direct movement by the detector. The direction is indicated by the green arrow on video and the slider shows the value in degrees. The **Duplicate detection filter, sec** parameter allows you to eliminate repeated detections of the same license number if it has been previously recognized. 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.
- Select a value for the **Detector sensitivity** parameter:
 - For vehicle detection, %** is the detector confidence level for the presence of a vehicle in the video.
 - For license plate detection on a vehicle, %** is the detector confidence level for the presence of a license plate on the detected vehicle.
 - For license plate detection, %** is the detector confidence level that the detected license plate is really a vehicle license plate.
- In the **Countries** list select country templates for the license plates to be recognized.



When the detector is configured properly, the recognized license plates and types of vehicles are shown in the operator interface in the **AutoTRASSIR/AutoPass Log**.

Plate	Time	Channel	Vehicle type	Special vehicles
453ATAT	16:08:37	TR-02453W02R...	Car	Fire service
A1818E	16:07:27	TR-02453W02R...	Car	Police
A1818E	16:07:22	TR-02453W02R...	Car	Police
NO PLATE	16:07:07	TR-02453W02R...	Car	Police
V571EC75D	15:53:31	TR-02453W02R...	Car	Ambulance
X337AD777	15:53:15	TR-02453W02R...	Car	Police
X337AD777	15:53:00	TR-02453W02R...	Car	Police
B663KT777	15:51:50	TR-02453W02R...	Car	Police
Y123CY197	15:51:03	TR-02453W02R...	Car	Police

For a detailed view of the recognized license plates, see [License plate recognition](#) and [Filtering current license plates](#) sections of the Operator's Guide.



- [Motion detector settings](#)
- [Channel settings](#)

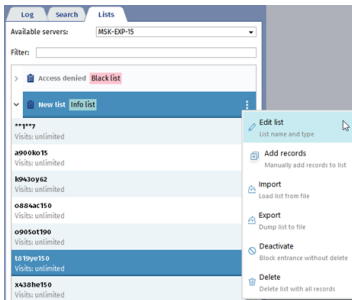
Maintaining internal lists of license plate numbers

The AutoTRASSIR/AutoPass plugin can use the internal license plate lists, which are stored in its own database. If a license plate stored in the internal list is recognized, the module will build up a message in accordance with the settings specified for this license plate.



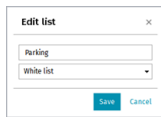
In order to start working with AutoTRASSIR/AutoPass internal license plate number lists, you should create *a simple AutoTRASSIR/AutoPass template*

An operator can create and edit license plate number lists in the **Lists** tab in the **AutoTRASSIR/AutoPass 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**.

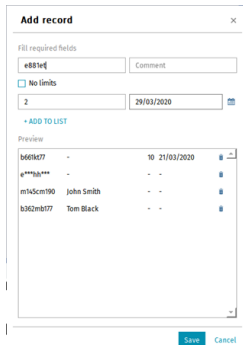


The list editing menu lets you:

- **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 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:

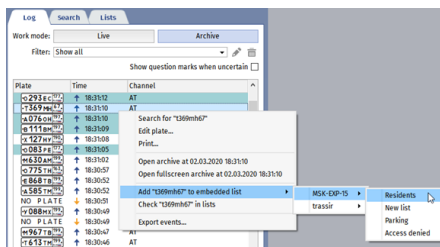
```
"License plate";"Comment";"Visits count";"Expiration date"
"b663kt777";"John Smith";;
"m145cm190";"Peter Still";;
"o362tk197";"Ian Johns";10;29/02/2020
```

- **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.

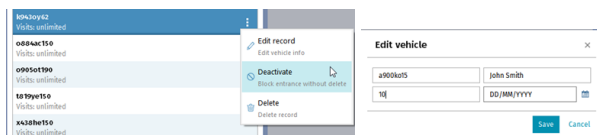


The **Audit** module allows to track the changes of the internal license plate list. See details in [Audit](#).

Besides manual addition or import from the file, the numbers can be added to the list with the help of scripts or from AutoTRASSIR/AutoPass 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 [Connection of the external number lists in TRASSIR OS](#).



- [AutoTRASSIR/AutoPass general settings](#)
- [AutoTRASSIR/AutoPass - Automated license plate recognition](#)
- [Selecting, installing, and configuring cameras to work with the AutoTRASSIR/AutoPass module](#)
- [Setup AutoTRASSIR module on a channel](#)
- [Creating an AutoTRASSIR/AutoPass 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/AutoPass** 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 on server.
- **Enable** - This checkbox determines if this source of license plate numbers should be processed by the AutoTRASSIR/AutoPass 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
ml45cm190 Tony Shot
o191hk190 Ian West
```

- **Encoding** - The text file's encoding.
 - **Plate letters in file** - A value from the dropdown list. Choose "Latin" , 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.

Plate	Comment
y070py177	Petrov
o362nk197	Ivanov
m145cm190	Kozlov
o191hk190	Sidorov

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** to save connection to the external list on server.

External lists
Office

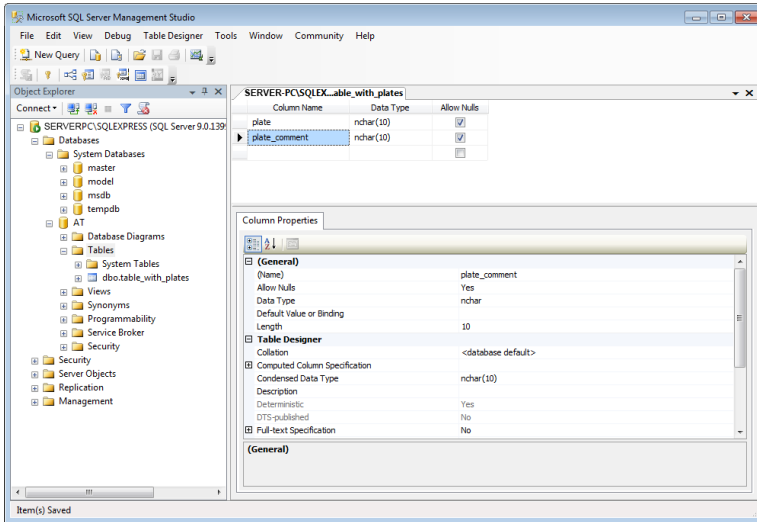


- *AutoTRASSIR/AutoPass general settings*
- *AutoTRASSIR/AutoPass - Automated license plate recognition*
- *Selecting, installing, and configuring cameras to work with the AutoTRASSIR/AutoPass module*
- *Setup AutoTRASSIR module on a channel*
- *Creating an AutoTRASSIR/AutoPass template*
- *Maintaining internal lists of license plate numbers*

Creating an external ODBC data source for AutoTRASSIR

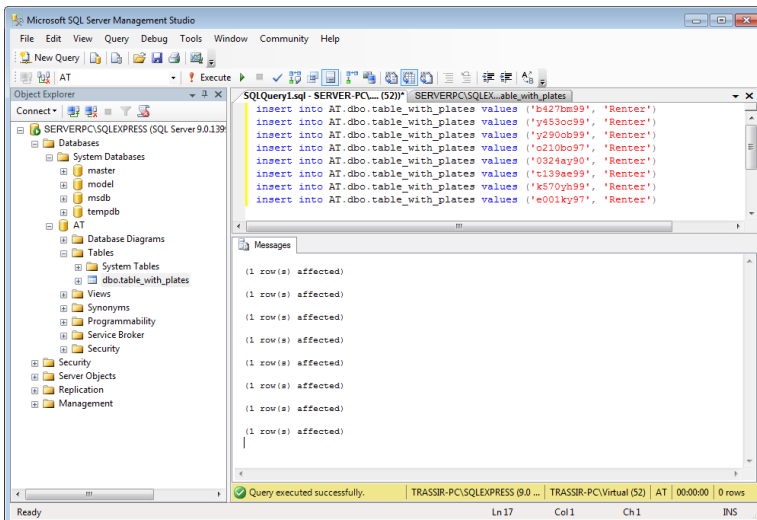
Let us consider the creation of an external ODBC data source using an MSSQL database.

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:

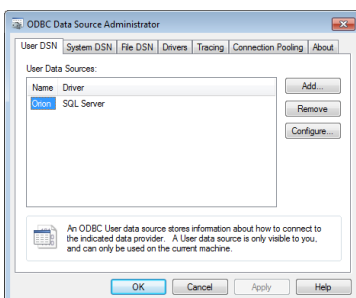


In our example we are only using two columns that contain the license plate number and a description of its owner. You can create tables with any number of columns and amounts of information. For example, you might include the vehicle's time of passage or its color.

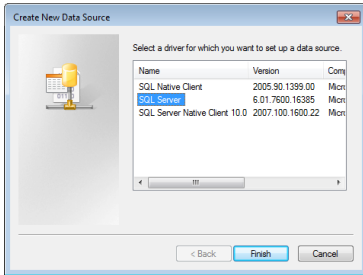
Next, use an SQL query to fill the table:



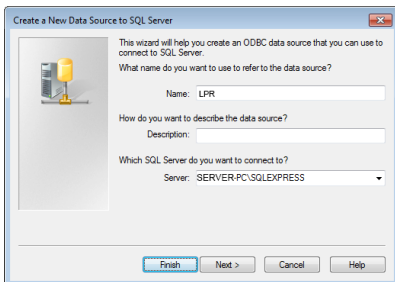
Now let's create the ODBC data source. To do this, launch the **ODBC Data Source Administrator** (**Start -> Control Panel -> Administrative Tools -> Data Sources (ODBC)**)



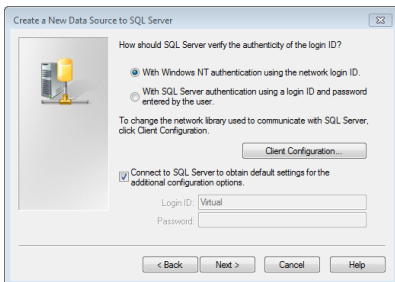
Click the **Add** button and select a driver in the window that opens. In our case, we will use **SQL Server**. To begin the configuration, click **Finish**



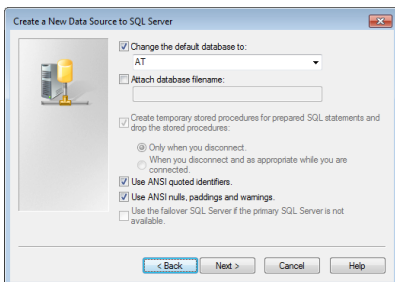
After that, the wizard will prompt you to enter the name of the data source, which will be used subsequently for the connection configuration, and the path to the SQL server. Enter the required information and click **Next >** to continue.



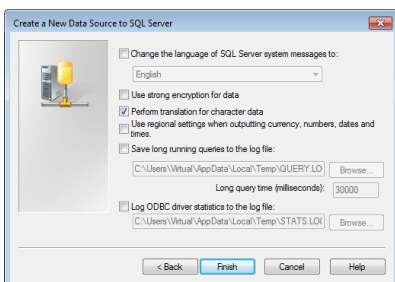
In the next step, the wizard will prompt you to select a user authentication option. In our case, we will leave the settings unchanged and click **Next >** to continue.



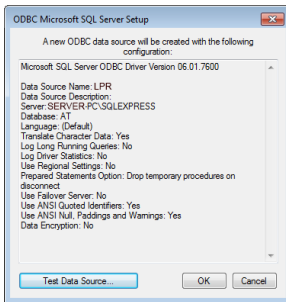
In the next step of the configuration, set the **Use database by default** checkbox and select the previously created **AT** database. Leave the remaining settings unchanged. To continue the configuration, click **Next >**.



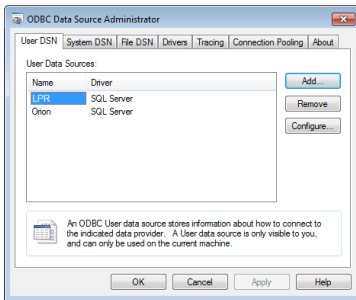
Similarly, leave the ODBC data source's other parameters unchanged.



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/AutoPass.



- *Connecting external lists of license plate numbers on Windows*
- *Connection of the external number lists in TRASSIR OS*

Connecting external lists of license plate numbers on 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/AutoPass** 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 on server.
- **Enable** - This checkbox determines if the source should be used by the AutoTRASSIR/AutoPass 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", 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** to save connection to the external list on server.



- [AutoTRASSIR/AutoPass general settings](#)
- [Creating an external ODBC data source for AutoTRASSIR](#)

Connection of the external number lists 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/AutoPass** 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 on server.
- **Enable** - This checkbox determines if the source should be used by the AutoTRASSIR/AutoPass 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", 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** to save connection to the external list on server.



- [AutoTRASSIR/AutoPass general settings](#)
- [Creating an external ODBC data source for AutoTRASSIR](#)

Creating an AutoTRASSIR/AutoPass template

You can verify that the AutoTRASSIR/AutoPass 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  .
3. Click  Add AutoTrassir .
4. Drag the camera signal being processed by the AutoTRASSIR/AutoPass module from the list of channels to an available space.
5. Click  Save As... .

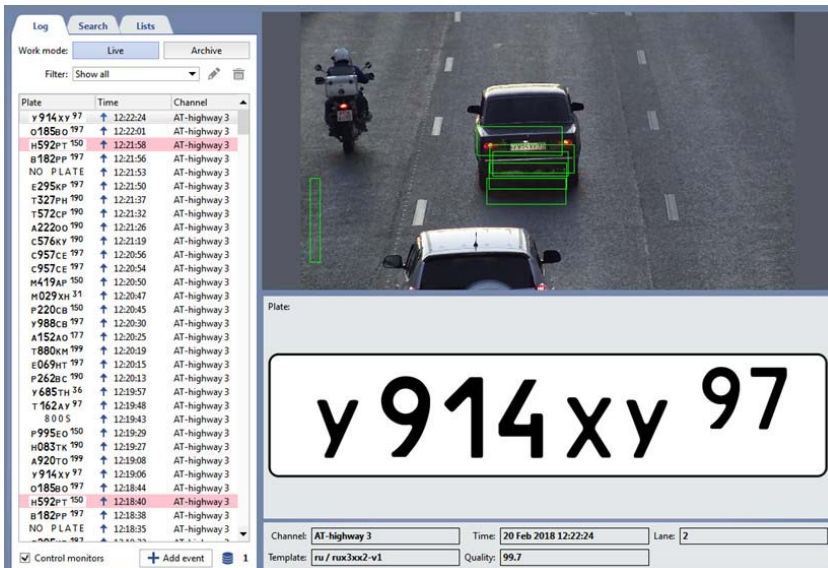
Save template under name:

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/AutoPass log.



The screenshot shows the AutoTRASSIR/AutoPass interface. On the left is a log table with columns for Plate, Time, and Channel. The log contains several entries, with the last one highlighted in red. On the right is a video monitor showing a car with a license plate. Below the video monitor is a large display showing the recognized license plate number: y 914 xy 97. At the bottom of the interface, there are fields for Channel (AT-highway 3), Time (20 Feb 2018 12:22:24), Lane (2), Template (ru / rus30x2-v1), and Quality (99.7).

Plate	Time	Channel
y 914 xy 97	12:22:24	AT-highway 3
o185o 197	12:22:01	AT-highway 3
h592p 150	12:21:58	AT-highway 3
h182p 197	12:21:56	AT-highway 3
NO PLATE	12:21:53	AT-highway 3
e295p 197	12:21:50	AT-highway 3
t327p 190	12:21:37	AT-highway 3
t572c 190	12:21:32	AT-highway 3
a222o 190	12:21:26	AT-highway 3
c576x 190	12:21:19	AT-highway 3
c957c 197	12:20:56	AT-highway 3
c957c 197	12:20:54	AT-highway 3
h419p 150	12:20:50	AT-highway 3
h029x 11	12:20:47	AT-highway 3
p220c 150	12:20:45	AT-highway 3
y988c 197	12:20:30	AT-highway 3
a152a 177	12:20:25	AT-highway 3
t880h 199	12:20:19	AT-highway 3
e069h 197	12:20:15	AT-highway 3
p262c 190	12:20:13	AT-highway 3
y685t 16	12:19:57	AT-highway 3
t162a 197	12:19:48	AT-highway 3
800 S	12:19:43	AT-highway 3
p995e 150	12:19:29	AT-highway 3
h083x 190	12:19:27	AT-highway 3
x920o 199	12:19:08	AT-highway 3
y914 xy 97	12:19:06	AT-highway 3
o185o 197	12:18:44	AT-highway 3
h592p 150	12:18:40	AT-highway 3
h182p 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, verify:

- AutoTRASSIR/AutoPass module settings (see [Setup AutoTRASSIR module on a channel](#) or [Setup HSC AutoPass module on a channel](#)).
- AutoTRASSIR/AutoPass module settings (see [Setup AutoTRASSIR module on a channel](#)).
- Database connection settings (see [Database connection settings](#)).

You can read more about working with the template editor and the AutoTRASSIR/AutoPass module in the Operator's Guide (???)



- *AutoTRASSIR/AutoPass general settings*
- *AutoTRASSIR/AutoPass - Automated license plate recognition*
- *Selecting, installing, and configuring cameras to work with the AutoTRASSIR/AutoPass module*
- *Setup AutoTRASSIR module on a channel*
- *Maintaining internal lists of license plate numbers*
- *Connecting external lists of license plate numbers on Windows*
- *Connection of the external number lists in TRASSIR OS*

SIMT software-based detector

The purpose of a SIMT detector 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:

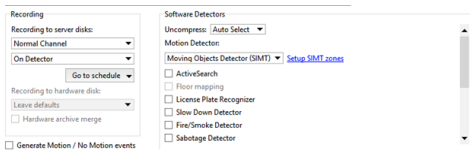
- high tolerance of precipitation, interference, and noise;
- detection of the speed, direction of the motion, distance covered, and the sizes of actually moving objects;
- monitoring of intersections with object borders;
- monitoring of the presence of objects in a zone;
- automated PTZ camera control (in conjunction with the [ActiveDome](#) module);



- [SIMT detector settings](#)
- [ActiveDome - Automated PTZ-camera control](#)


SIMT detector settings

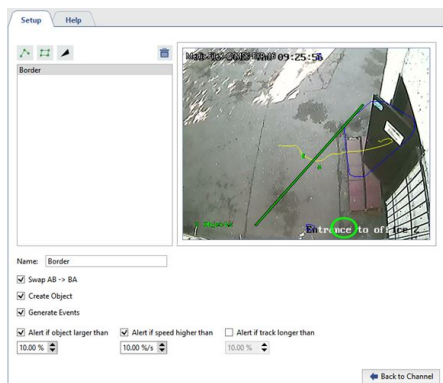
To configure the SIMT detector, in the **Motion detector** settings group in the **Software Detectors** area of the **Channel settings** window, select **Moving object detector (SIMT)** and click **Setup SIMT zones**. A window for configuring the SIMT detector's borders and zones will open.




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:

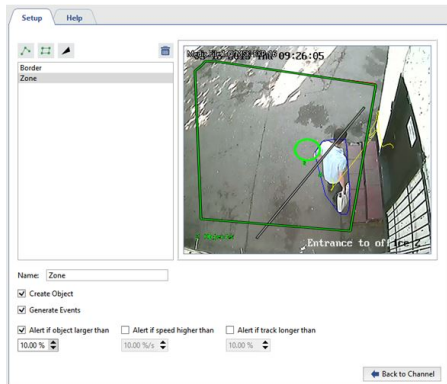
- Click the ;
- Then left-click with the mouse to specify the vertices of a polygonal line;
- Click **Finish**;
- Give the detection zone a name;
- Set the **Swap AB -> BA** checkbox in order to make zones A and B switch places;
- Set the **Create object** checkbox if you need to create an object for this border in the 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:

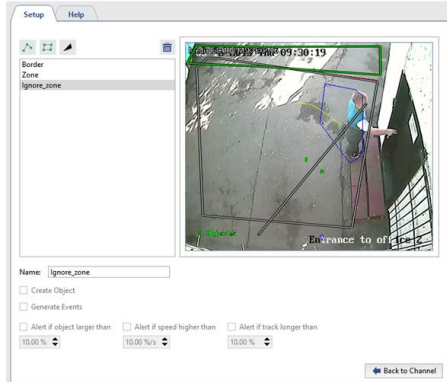
- Click the ;
- Consecutively left-click with the mouse to specify the vertices of the polygon;
- Click **Finish**;
- Give the detection zone a name;
- Set the **Create object** checkbox if you need to create an object for this zone in the object tree. A zone object may be used, for example, when setting 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:

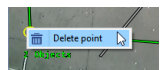
- Click the ;
- Consecutively left-click with the mouse to specify the vertices of the polygon;
- Click **Finish**;
- Give the ignore zone a name.



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.

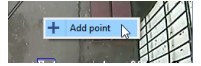


If a vertex is unnecessary you can delete it. To do this:

- 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:

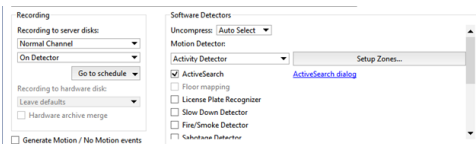
- super fast search across the entire archive;
- motion search in the specific zone with the preset parameters;
- versatility using set parameters (speed of motion, object size, duration of motion, exact time);
- archive viewing in the search window;
- easy interactive search and the possibility of the 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 about working with the ActiveSearch module in the Operator's Guide (???).



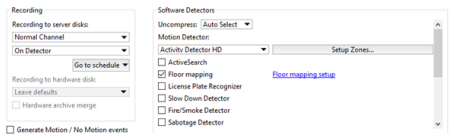
- [Motion detector settings](#)
- [Channel settings](#)

Floor mapping settings

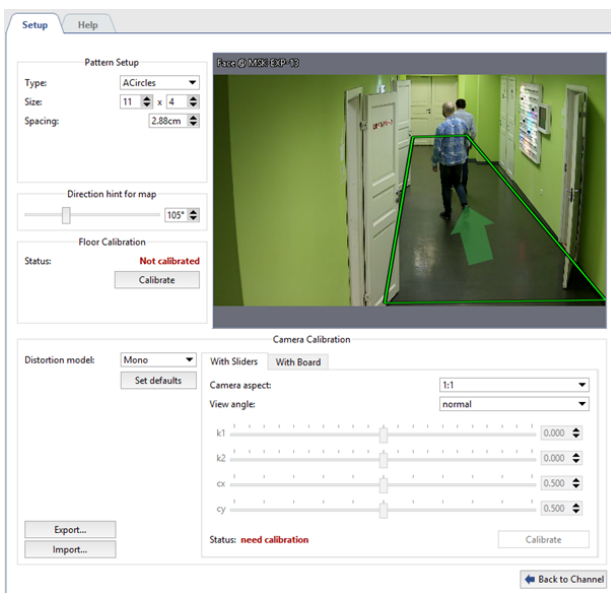


Floor mapping is designed for transferring image from camera to the floor surface. It is required for showing people movement on *map*, detected by *Neuro detector*. It is also required for building *heatmap*.

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. Print it in 1:1 scale in A2 format or bigger sheet.

Check the scale of the received template using the ruler.



Settings

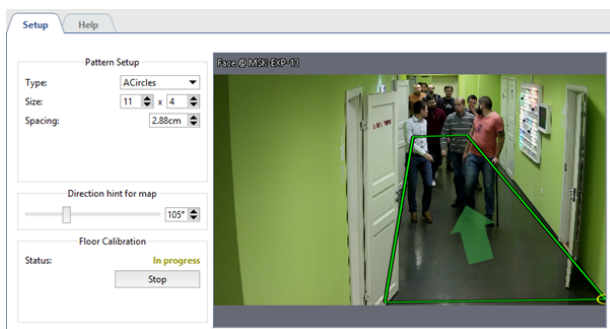
1. Make the module preset

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:

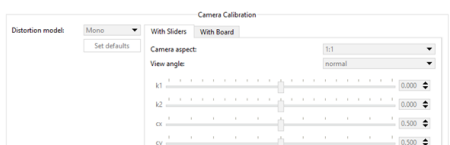
- camera installation location;
- camera tilting angle;
- focal distance of the lens.

3. Camera calibration

To start with select the **Distortion model** installed on the camera: **Mono** or **Fisheye**.

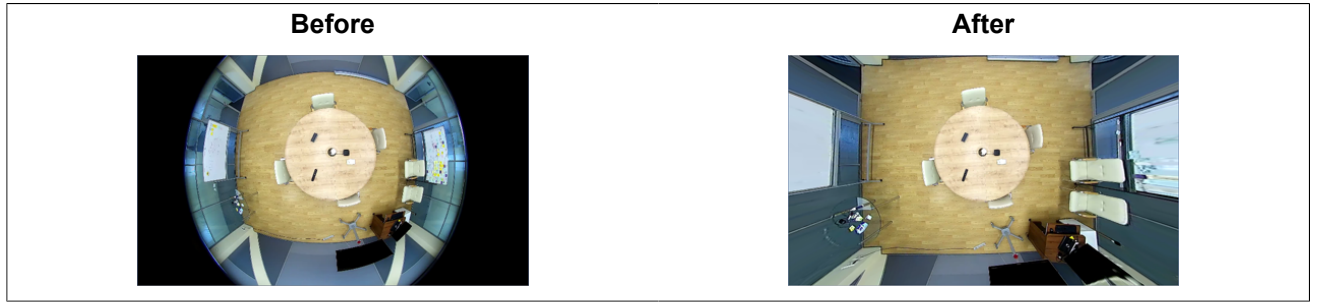
Further calibration of camera can be done in two ways:

• With sliders

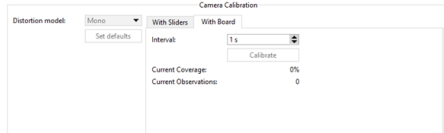


On the **"With sliders"** tab in **Camera aspect** and **View angle** fields select height-to-width aspect of maximum resolution and lens vision's horizontal angle.

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

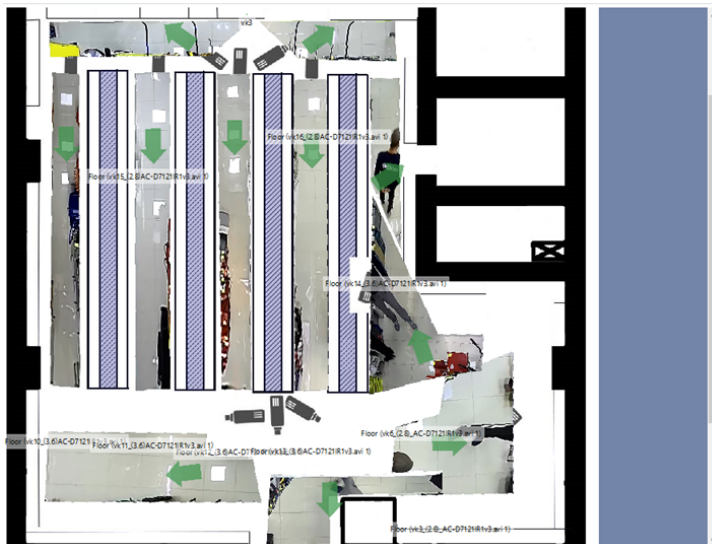
Modify the position of the rectangle points in such a way to make the marked area to enframe all visible surface of the floor. If necessary, add the desired number of points using the context menu.

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 settings*
- *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 the server 4.x. 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:

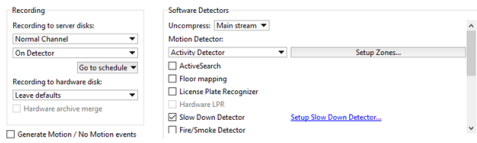
- [*Common Slow Down detector settings*](#)
- [*Configuration of the Advanced Slow Down detector*](#)



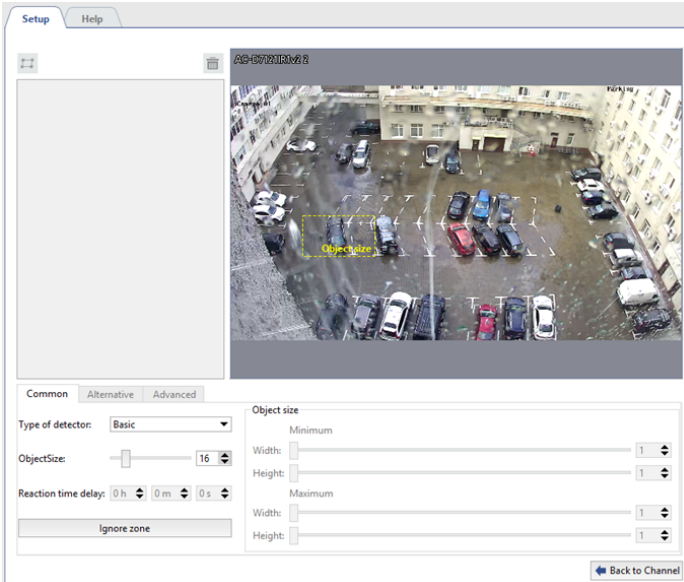
- [*Channel settings*](#)
- [*Motion detector settings*](#)

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.

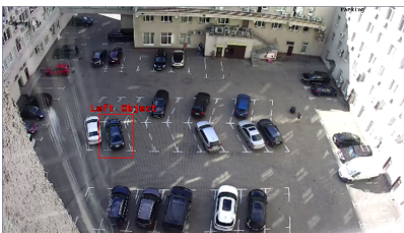


By default, the detector monitors appearance of abandoned objects across the entire image area. If necessary, you can decrease this area. To do that, click **Ignore zone** button and holding the right button select image areas the detector should ignore.

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.



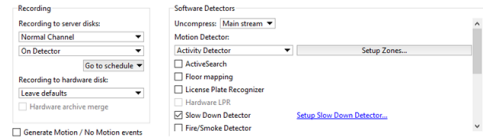
To monitor changes in the detector's operation, enable displaying of figures on the channel **Slow Down detector** (see section ???).



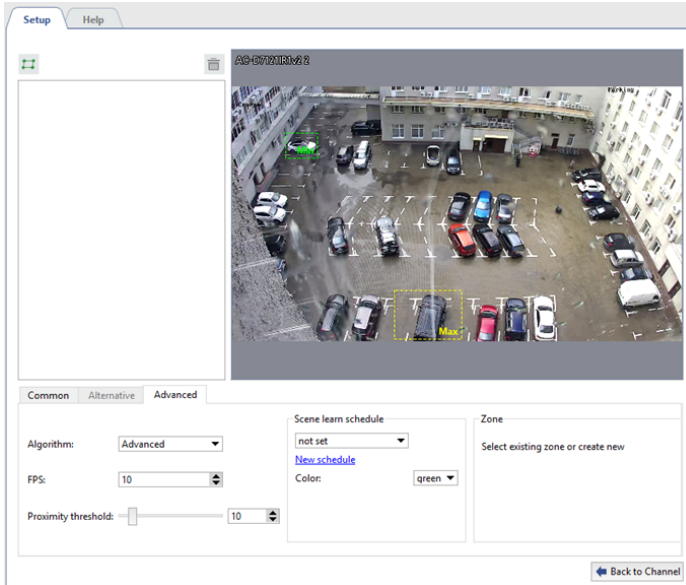
- [Channel settings](#)
- [Motion detector settings](#)
- [Slow Down Detector](#)

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.

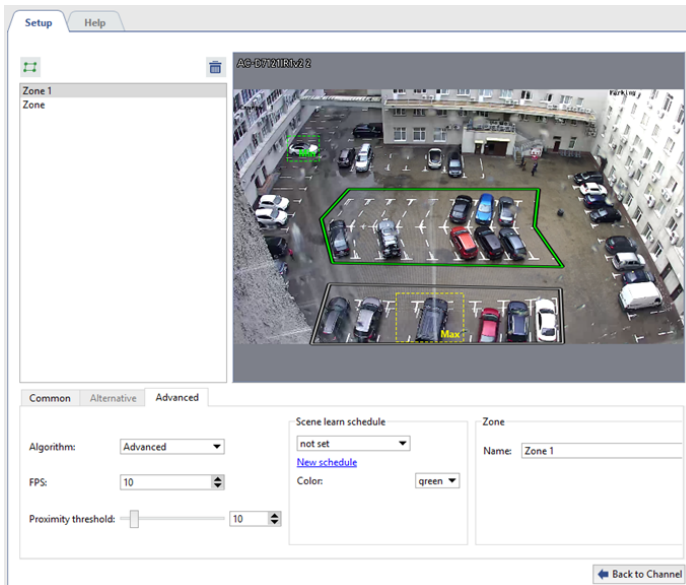


Next, using **ObjectSize** setting, you can determine a **minimum** and **maximum** size of the object, the detector will respond to. Rectangles on the image will help to evaluate its size. The detector will trigger if the abandoned object is bigger than the green box, but smaller than the yellow box.

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: **Face Recognizer** and **Face Recognizer 2.0** built into TRASSIR. Both versions can work with the face database, located both **locally** (on the server with the module) and **remotely** (on any server that is connected to the server with the module). Read more about the face database location in [Face recognizer basic settings](#).



Features of the module remote mode operation settings:

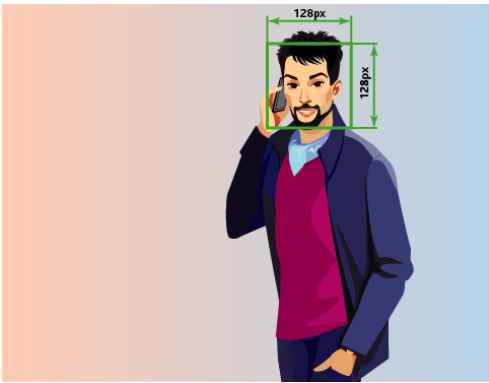
- The server with cameras that recognize faces must be connected to the server with TRASSIR OS, which will be used as **Analytics Server**.
The TRASSIR OS server of **NeuroStation** version can be used as analytics server.
Read more about server connection in [Connecting to a new server](#).
- Check 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

- **Human face detection**
The module searches for a face in the camera video and highlights it. It is possible to detect a face on a video taken from any angle, including faces in profile.
- **Face tracking**
The module supports tracking and single face monitoring (Face Recognizer) or multiple faces in a stream (Face Recognizer 2.0).
- **Face identification and quality assessment**
Comparing the found face with the one saved in face database and determining the degree of matching.
- **Identifying gender and age by face**
- **Recognizing specific attributes of a person's appearance**
In addition to gender and age, the module can recognize and search by individual appearance attributes, such as hair color, the presence of glasses or headgear, etc.
- **Ability to recognize the usage of photo in frame**
Identification of the use of a photo instead of a live face in the frame by comparing various characteristics of a person's face with a static image.
- **Using module in Access Control**

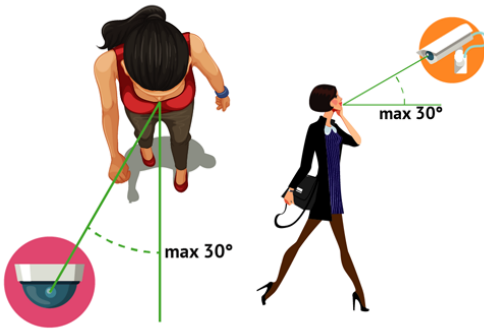
Recommendations on choosing and setting up a camera

- 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.



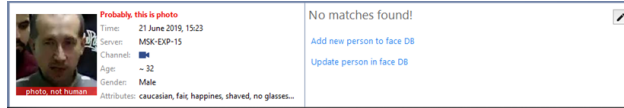
Be careful, increasing the number of streams will increase the server load.

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 **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	view content

Face database can be stored both locally and on any 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.



The face database local cash is used for face recognition. That's why in case of the face database server connection loss, the face detection continues. The 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
TR-02111R3W.1	<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*



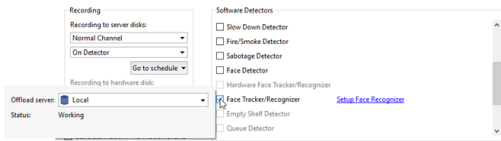
For a detailed description of the operator interface, see [Face recognizer](#) section of Operator manual.



- [Face recognizer](#)
- [Face recognizer settings for the channel](#)
- [Face recognizer 2.0 settings for the channel](#)
- [Face database](#)

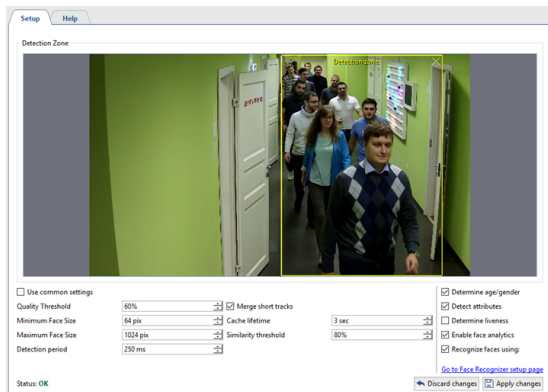
Face recognizer settings for the channel

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.

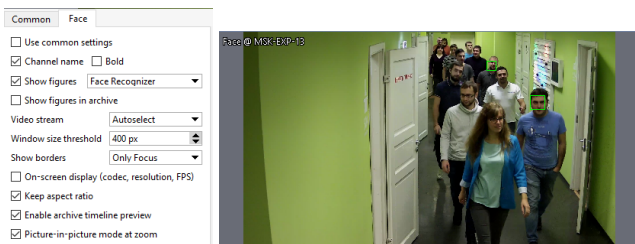


- If common detection parameters are not suitable for the detector operation on this channel, then clear the **Use common settings** checkbox and change them.

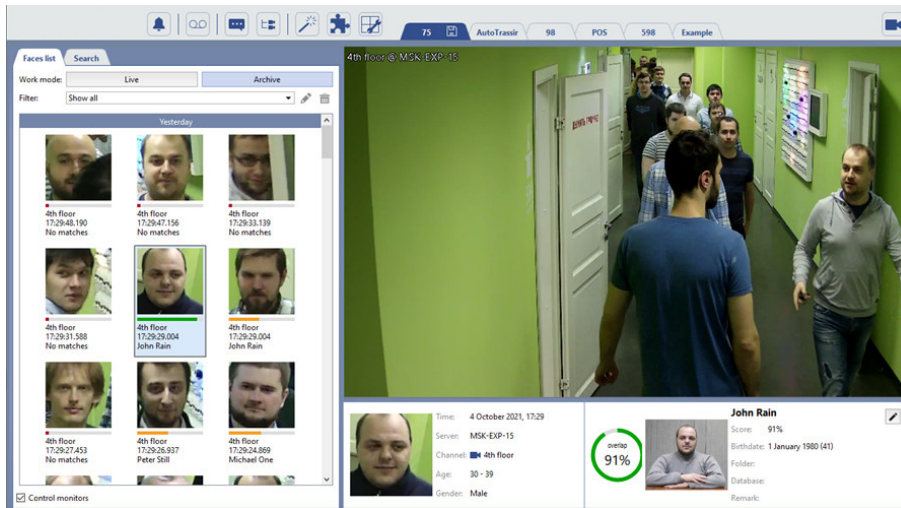


Clicking the **Go to Face Recognizer setup page** link you will go to the global settings of the detector. Description of the detection parameters can be found in the section *Face recognizer basic settings*.

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:



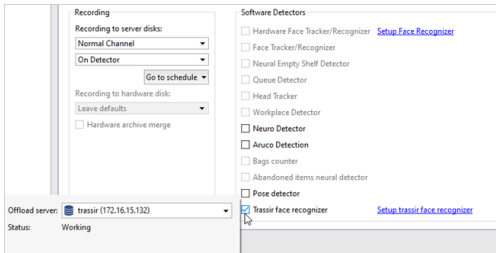
The full operation of the module can be seen in the operator interface. To do this, you can *create a simple template*.



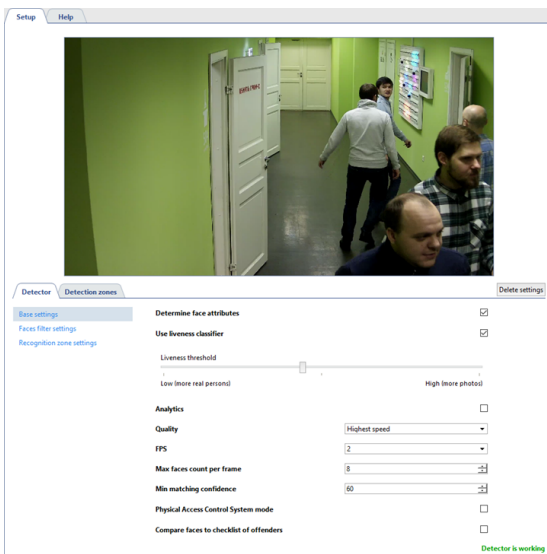
- *Face recognizer*
- *Face recognizer basic settings*
- *Channel settings*
- *Motion detector settings*

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.



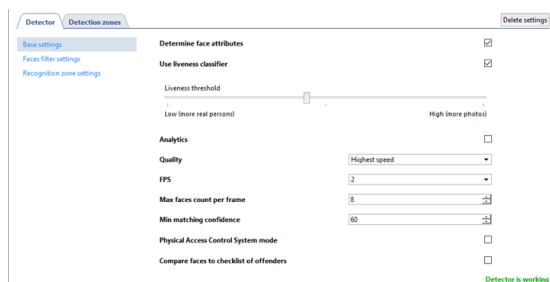
You can check the correctness of the detection settings, by enabling the figure display. To do this, right-click on the image and select the **View options...** item in the drop-down menu. Set the **Show figures** flag and select **Face recognizer** item in the drop-down menu. The recognized faces will 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:



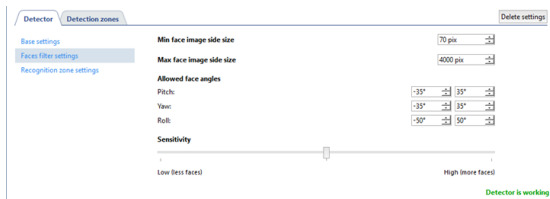
- Determine face attributes** - set the flag to display gender and age when a person is recognized.

- Set the **Use liveness classifier** flag and specify the **Liveness threshold** to allow the detector to distinguish between a real person and a photo or image of a person. The higher the threshold is, the higher is the facial liveness value will be used, by which the detector will determine whether a person or a photo is in the frame.
- **Analytics** -set the flag to let the detector analyze the gender and age of the person in the frame.
- **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.

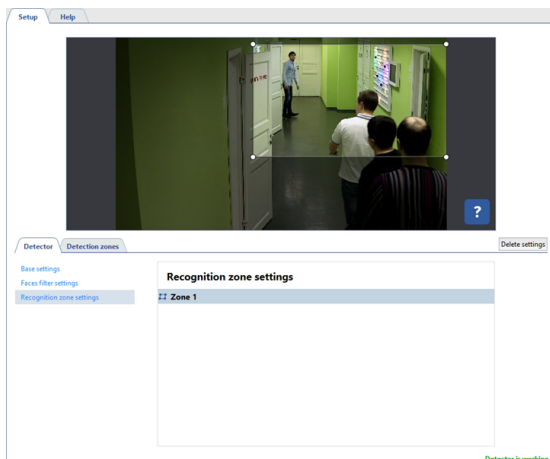


To ensure the detector correct operation, you should select the same quality in the analytics server settings as in the detector settings.

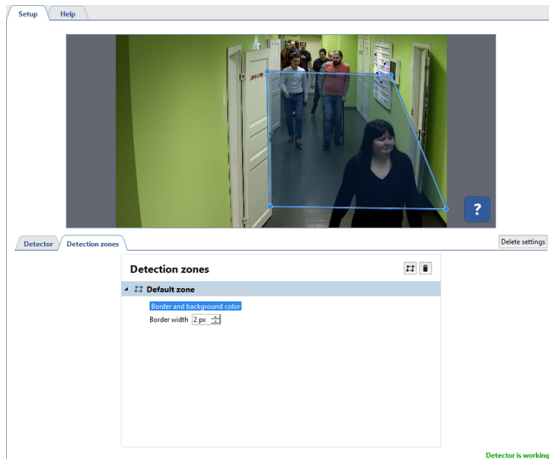
- **FPS** - frame rate.
- **Max faces count per frame** - set the maximum number of faces that the detector can recognize in one frame. If the number of faces exceeds the selected value, the detection frames around them will be gray, and such faces will be displayed as unrecognized in the operator interface.
- **Min matching confidence** - set the degree of correspondence between the detected person and the person in face database.
- Set the **Physical Access Control System mode** flag and select the **Viewing time** to use the detector in Access Control.
- 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.



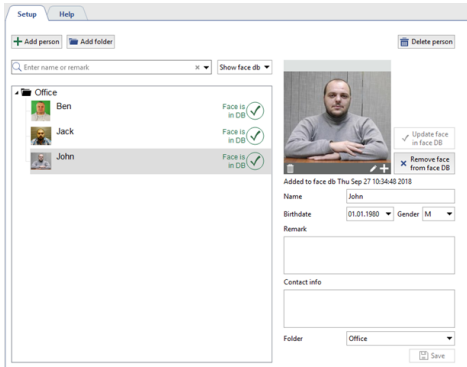
In order to create a new **counting zone**, press **⌘** and set its vertices on the image. Place the cursor to the zone starting point and left-click or press **CTRL+ENTER** to complete the zone drawing.



- [Face recognizer](#)
- [Face recognizer basic settings](#)
- [Channel settings](#)
- [Motion detector settings](#)

Face database

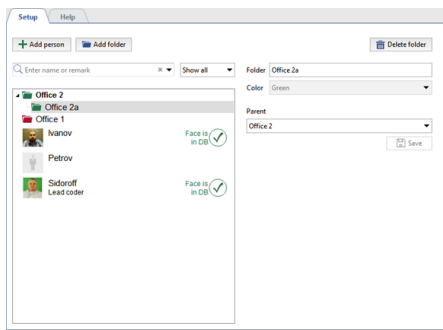
Face database is a part of *Persons database*, which includes people and their anthropometric data. Face database is used for comparison with faces that *Face Tracker/Recognizer* module detects on camera image.



The server 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.
- The face database size is determined by the license.

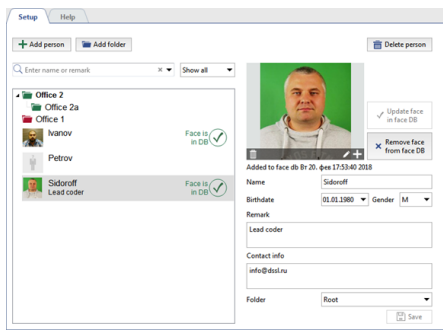
Folders creation



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.

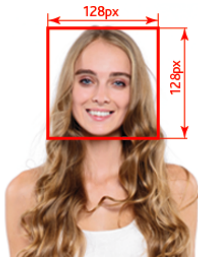
Creating and adding persons to the face database



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

- Click **Add Photo** and select the photo of the person. You can upload multiple photos. Consider *photo recommendations* when making your selection.
- Enter the person's name into the **Name** field.
- Select **Birthdate**.
- Select **Gender**.
- Enter **Remark** and **Contact info**.
- Select the **Folder** where the person will be located.
- Press **Add to Face DB**. The person will be added to the **Face database** and marked with the corresponding icon. After that, the photos of the person will be converted into a set of anthropometric data, which will be stored in the database and used to identify the person by *Face Recognizer* module.

Recommendations to the photos used for recognition



All photos, stored in the **Face database** are used by the server for recognition. The probability of recognizing a person caught in a camera depends on the quality of the uploaded photos. 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

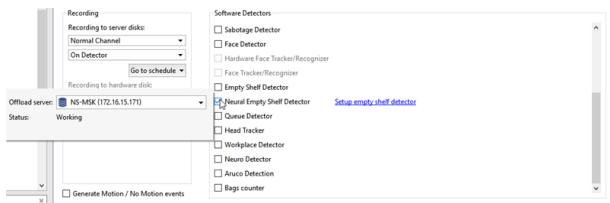
The **Neural Empty Shelf Detector** is intended to build up video surveillance systems which require the detailed analysis with the help of the neural networks. As a result, the video surveillance operator will monitor the shop shelves state in real time.



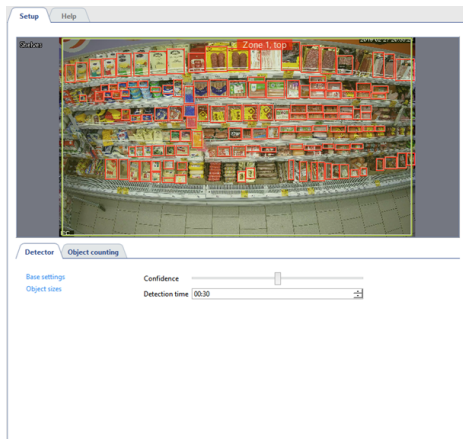
Neural empty shelf detector features:

- The module works with **NeuroStation** video recorders or on any video recorders of 4.x version, connected to **NeuroStation** server and using it as **Server Analytics**. Read more on 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.



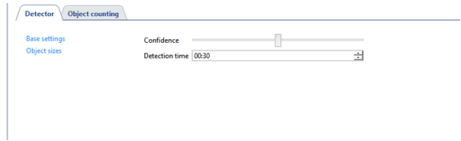
Press **Setup empty shelf detector** to open the settings window.



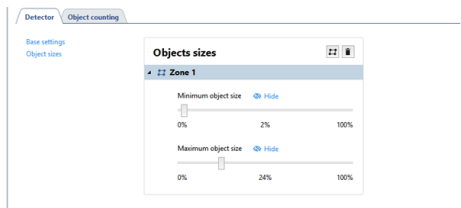
Detector

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**.

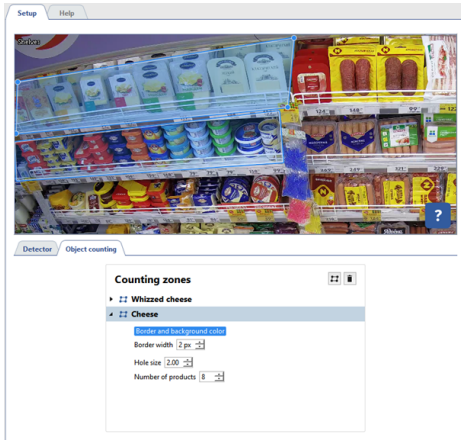


- You can create the zones in which empty space on the shelves will be swept in the **Object sizes** settings group. Set the biggest and the smallest sizes of the detected objects with the help of **Minimum object size** and **Maximum object size** settings.



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 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.

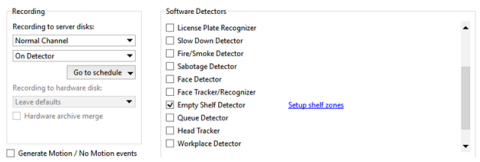


- [Motion detector settings](#)
- [Channel settings](#)


Empty Shelf Detector

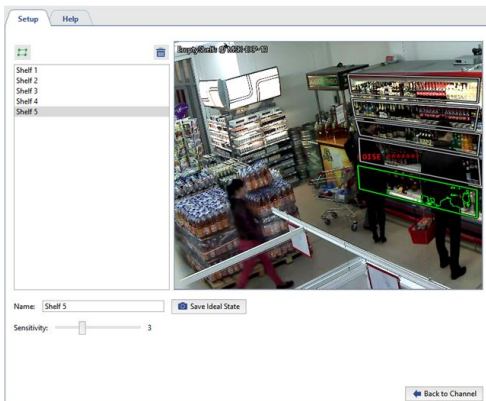
The shelf detector is intended to track the good availability on the shop shelves. It compares the current state of the specified shooting area with the previously saved image and notify the operator of the changes.







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.

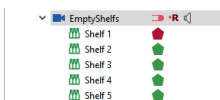


In the window that opens you can create detector zones - the areas which will be monitored by the detector:

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).



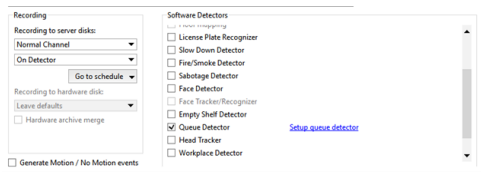
- The size of the head on the image should be of 40 pixels at least and should not exceed 25% of the entire frame size.
- The size of the head at the image limiting points should not alter more than twice.



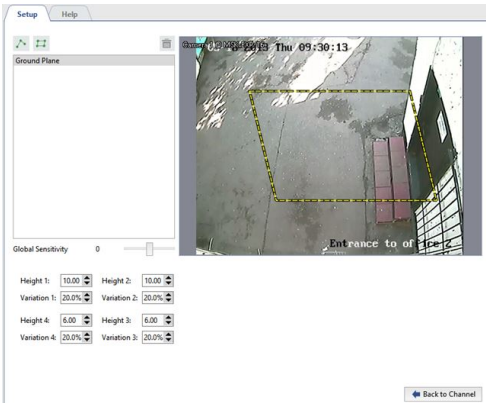
- [Channel settings](#)
- [Motion detector settings](#)
- ["Queue detector" module settings](#)
- [Workplace detector module settings](#)

"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.

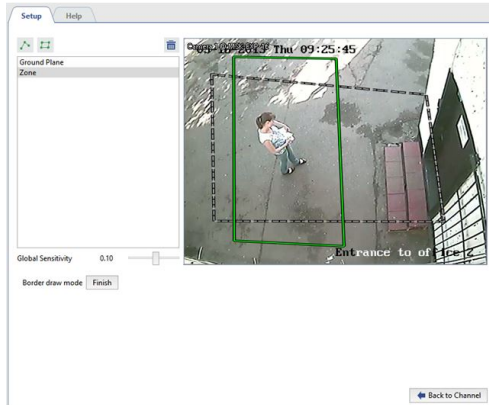
If the counter is configured correctly, the heads of people within the frame will be highlighted with a blue square.




Queue detector can be used to count the number of people:

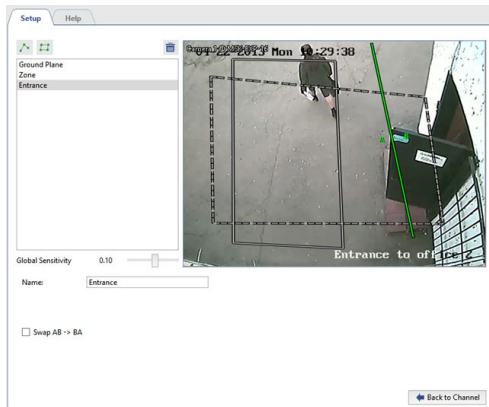
- within a selected area.







To do this, click the  button and specify an area within the Ground Plane.

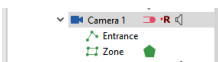


- intersecting a border line from either direction.

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  →  →  →  →  → .



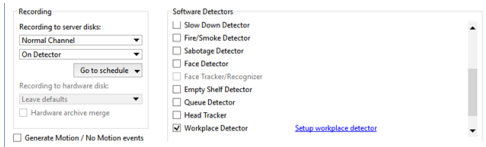
To track the detector's state in a timely fashion, you can create a *rule or script* that will activate when the state changes.



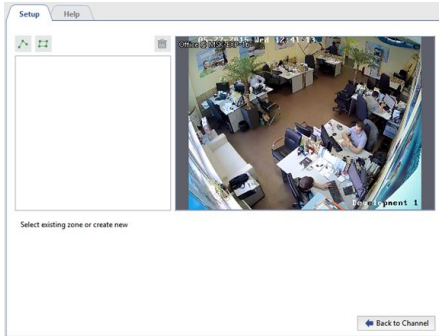
- [Channel settings](#)
- [Motion detector settings](#)

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.

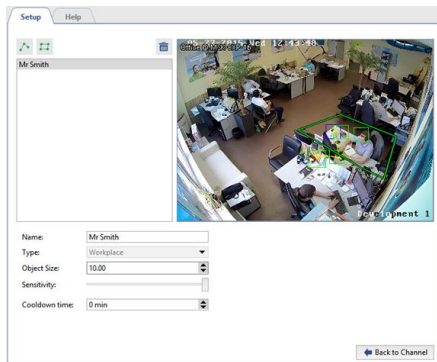
1. Press the button .
2. Set the vertex of the polygon by pressing the left mouse button sequentially. Upon completion press **Finish** button.
3. Set the zone name, i.e. employee's name or the name of the workplace.

After that the parameters where the detector will be activated should be defined for each zone:

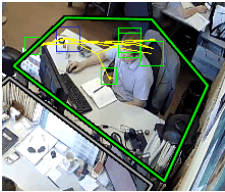
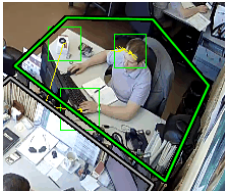
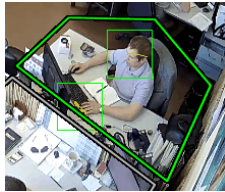
- **Object size** - the size of the head of the monitored objects.
- **Sensitivity** - the level of the detector's sensitivity.
- **Cooldown period** - the duration of motion absence in the zone.

Setting procedure

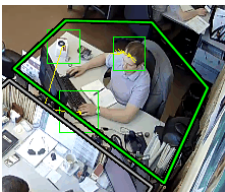
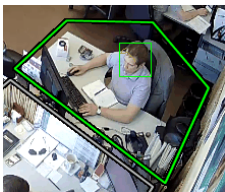
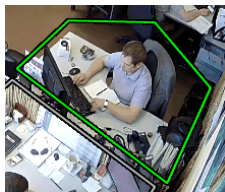
1. Move the **Sensitivity** slider right to adjust the detector's sensitivity above average. You'll see false triggering of the detector on the display in the shape of several squares.





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 triggering.

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.







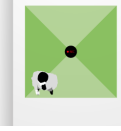
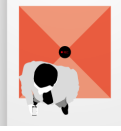
- [Channel settings](#)
- [Motion detector settings](#)

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](#)

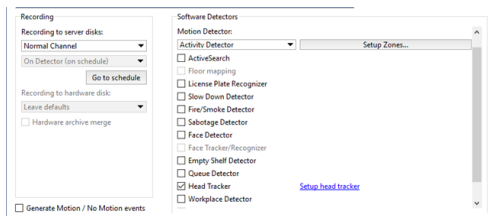
"Head Tracker" module settings

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.




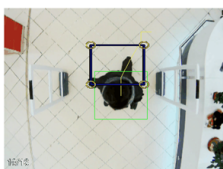
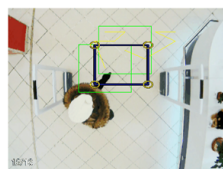
Set up the module:

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.
		



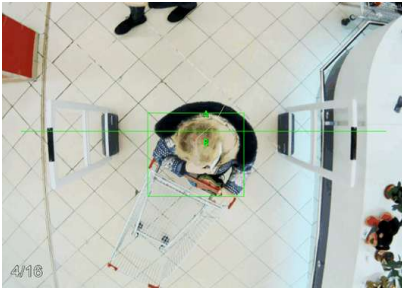
If the optimal result fails to appear under the given parameters, select **an alternative** detection method and repeat the settings.

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.



Neuro Detector features:

- The module works with **NeuroStation** video recorders or on any video recorders of 4.x version, connected to **NeuroStation** server and using it as **Server Analytics**. Read more on server connection in [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.

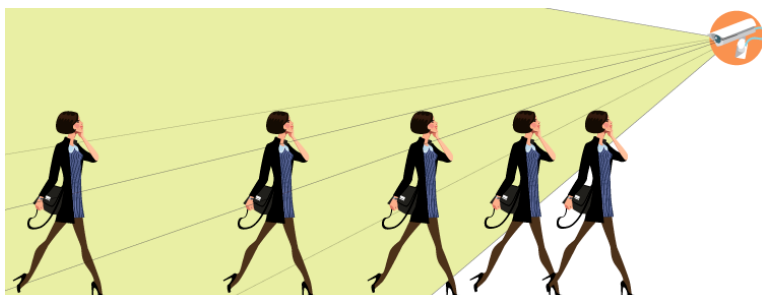
Recommendations on the camera selection, its location and shooting area lighting:

- 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:

In order to detect objects on video, the module can analyze video stream of any resolution and bitrate. The server will decode the image to the format 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.



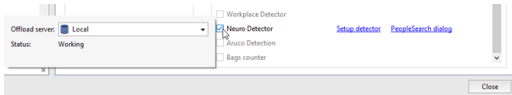
- [Channel settings](#)
- [Motion detector settings](#)
- [Neuro Detector settings](#)
- [Selection of the neural detector version and creation of classes](#)

Neuro Detector settings

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.

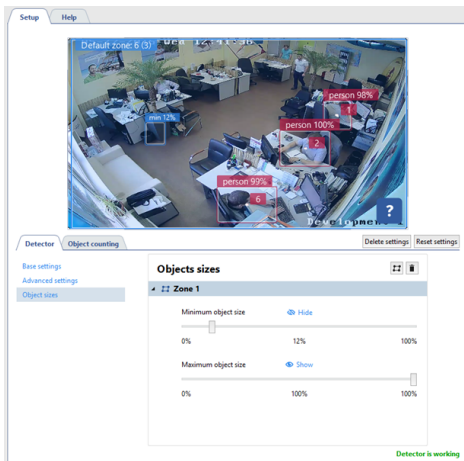


In case the module is activated on the **NeuroStation**, video recorder, in the **Server** settings select the **locally** value. Otherwise, select **NeuroStation** server name.



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.

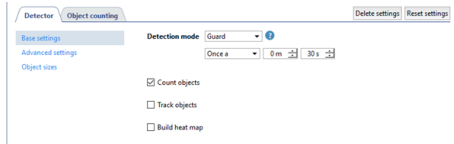


Enable showing the **People/Object detector** figure on the channel before configuring the detector settings and to track the changes in the detector's operation (read more in ???).

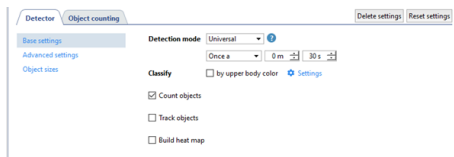
Detector

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.



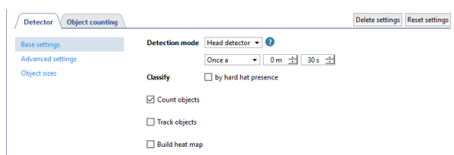
If you need to identify people wearing the same color of clothing among all detected objects on video, set the **by upper body color** flag and press **Settings** to choose the required classes.

i

To create classes which will be used by the detector, go to the **Server settings** -> **Plugins** -> **Neuro detector**.

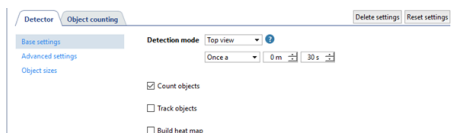
Read more about creating classes in [Selection of the neural detector version and creation of classes](#).

- **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.

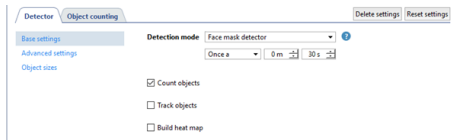
- The **Top view** detects people the same as the **Head detector**. It is designed for scenes with complex angles (i.e. when a camera shots from above or installed at the 75 degree or greater angle).



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.

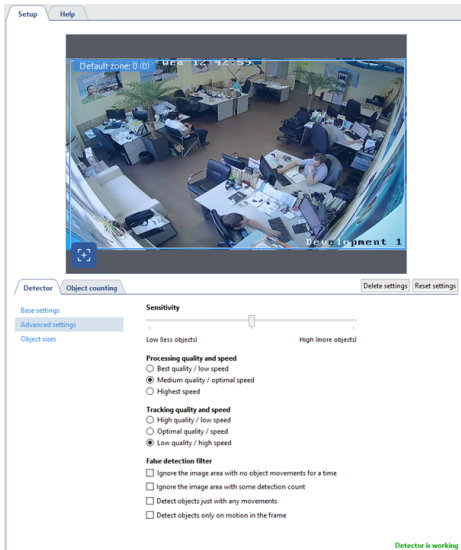


The operation of the detector depends on the **Mode** selected in the *analytics server settings*:

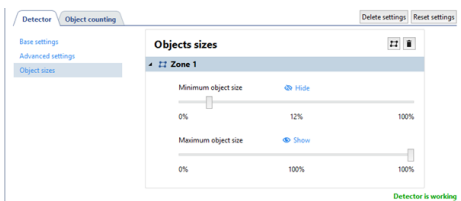
- The **Count objects** and **Track objects** features will operate when the following mode are selected **Default**, **Neuro detector** and **Classifier**.
- The **Classify by upper body color** and **Classify by hard hat presence** work only in the **Classifier** mode.

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.



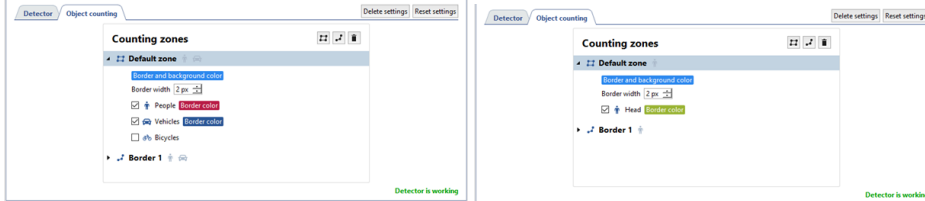
Do not create new object detection zones if it is not necessary, because each new zone increases the server load.


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.

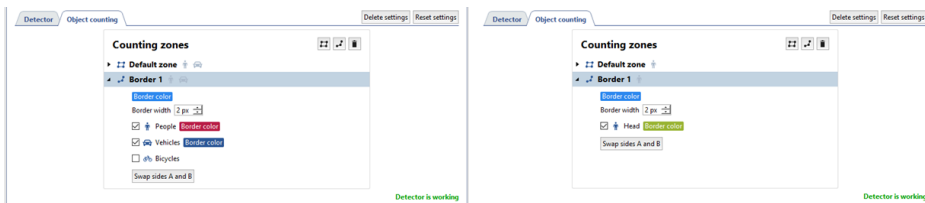
To create a new **counting zone** press  and set its vertices. To finish drawing, left click or press **CTRL+ENTER** at the zone starting point.

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.

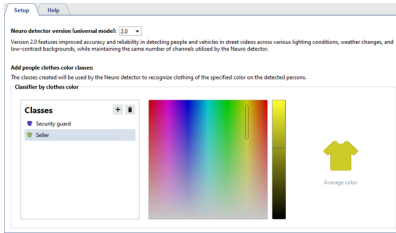
The counting border setup depends on the detected object:



- [Motion detector settings](#)
- [Channel settings](#)

Selection of the neural detector version and creation of classes

Go to the **Server settings**-> **Plugins** -> **Neuro Detector** and select the neuro detector version that will be used for detection of objects.



The **Neuro detector version 2.0** provides enhanced accuracy and reliability in recognizing people and vehicles in street video under various lighting conditions, weather changes and low-contrast backgrounds, while maintaining the maximum number of working channels.

To create a class press **+** and enter the class name.

Next:

- Select the color that is prevailing in the clothing of an employee of this class on the color scale. For example, select the blue color for a security guard, wearing a dark blue uniform.
- Select the color range on the scale that the detector will use to detect people under different lighting conditions.

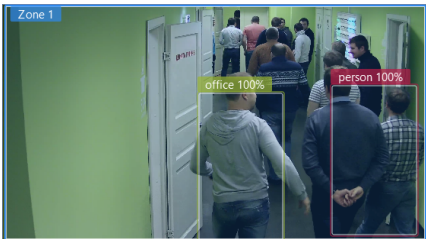


To enhance the module operation quality, we advise to use bright and deep colors in the outfit. It will reduce the number of false activations and will allow the detector to detect the required person from the total quantity of the detected people.

The **Neuro Detector** will use the created classes to detect the color of clothing of the detected people.

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.

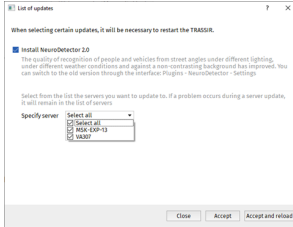


Read more about classes for object detection in **Neuro Detector settings**.

Updating Neuro detector to version 2.0 on connected servers

To improve the system performance and detection, it is necessary to upgrade the **Neuro detector to version 2.0** on all connected servers.

When starting the client/server to which the servers are connected, the **List of updates** will appear with the list of all servers that require updates. In order to upgrade, check the **Install NeuroDetector 2.0** box, specify the servers to upgrade, press **Accept and reload** and wait for download to complete.



The servers experiencing problems with the upgrade, will be marked as inactive.

Check the client's connection to the neuro detector servers and make sure the client user has the appropriate access rights.

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.



With the help of 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:

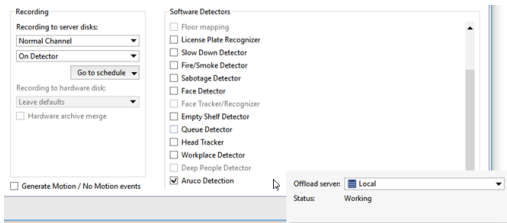
- Shooting area where markers detection takes place should be well lit. Shadows and highlights presence on the marker will reduce probability of its detection and decoding.
- The camera should be mounted in such a way to provide full view of the marker. Partially covered marker will not be detected by 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.



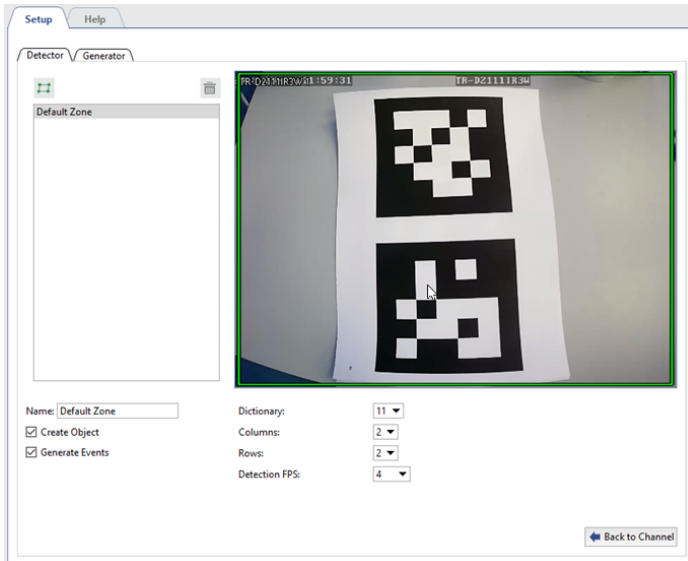
- [ArUco Detection](#)
- [ArUco Marker generator](#)

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:

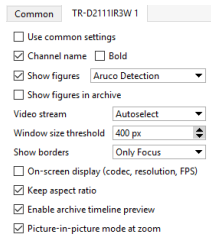


Before setting up the detector, determine the type of markers to be detected. In the section [ArUco Marker generator](#) types of supported markers are described along with their creation procedure. In case you are aware of the type of markers to be detected, go to the detector settings.

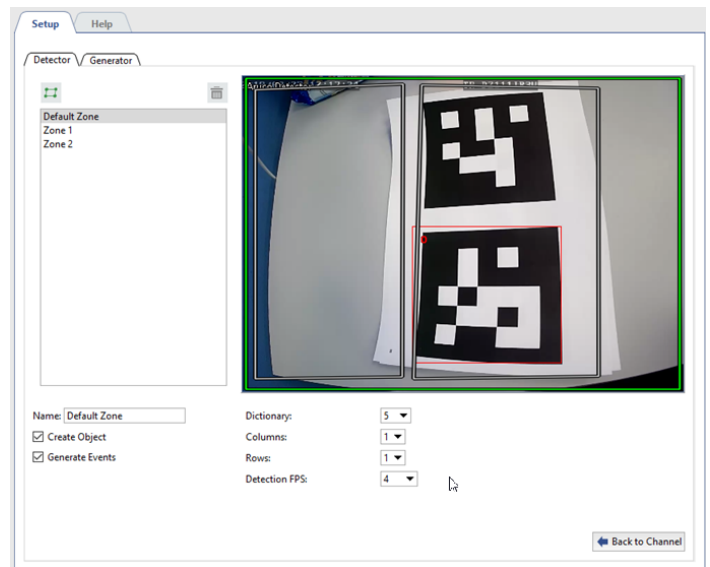
Settings


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](#)).

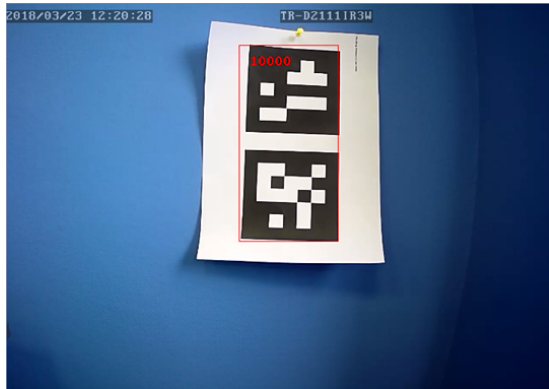


Be careful while selecting detection FPS. Do not set maximum value to detect markers on static or slowly moving objects. The higher the frequency is - the higher is the server load.

3. Verify settings correctness.

Put the sheet with the marker to the camera.

If the detector settings are correct, the marker will be highlighted with a red rectangle.

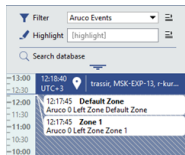


4. Set the detector status tracing parameters.

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](#).

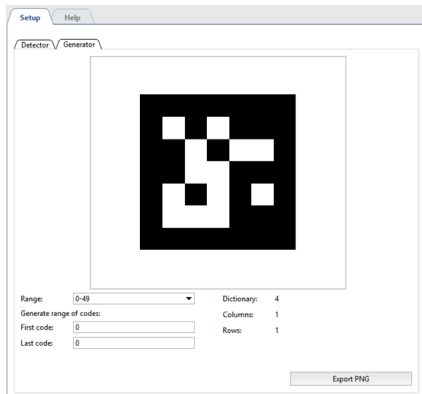
To display detector status check **Generate events** box in the log of events.



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* .



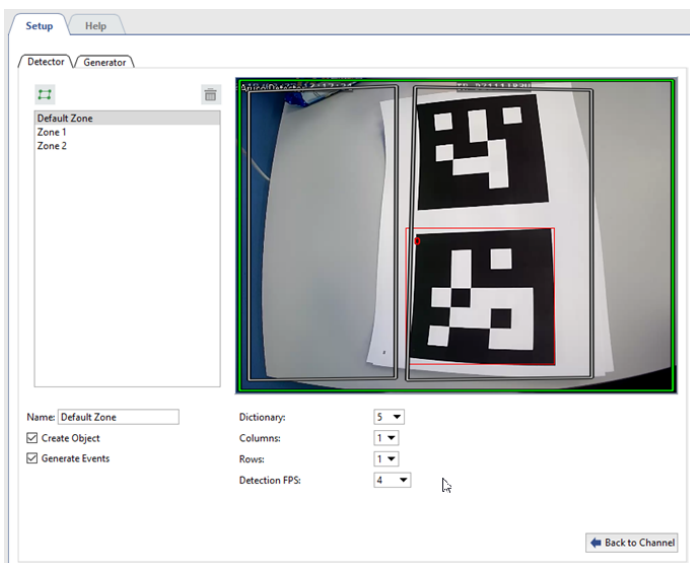
To do this:

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.

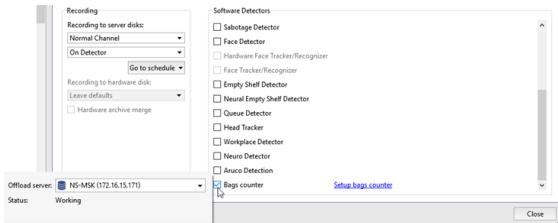
2. To create ArUco marker images, enter the range of numbers into **First code** and **Last code** fields.
3. Press **PNG export** to save the marker images for further printing.
4. The values displayed in the **Dictionary**, **Columns** and **Rows** fields will be used for *ArUco detector settings* on **Detector** tab.



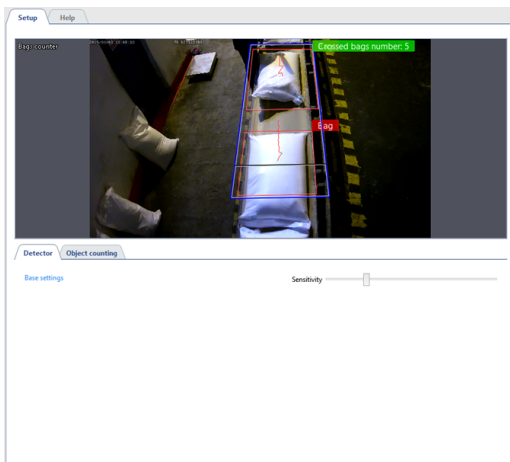
Bags counter

The **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.

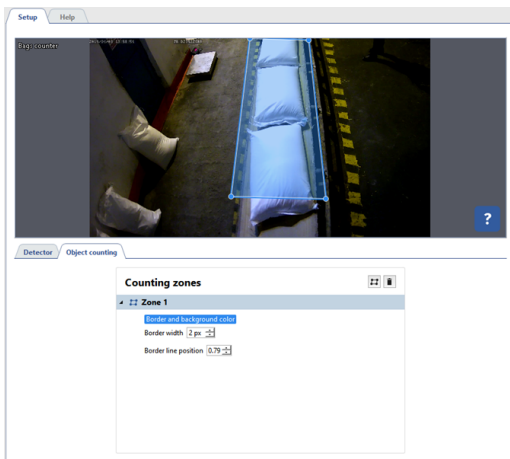


Click **Setup bags counter** to open the detector settings window.



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

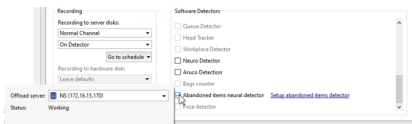
Abandoned items neural detector is designed for building complex video surveillance systems which require detailed image analysis with the help of neural networks. As a result of the detector's operation, the video surveillance system operator will detect various objects of various sizes left in the camera coverage in real-time, as well as instantly identify left and forgotten objects which can potentially threaten the security of the video surveillance object.



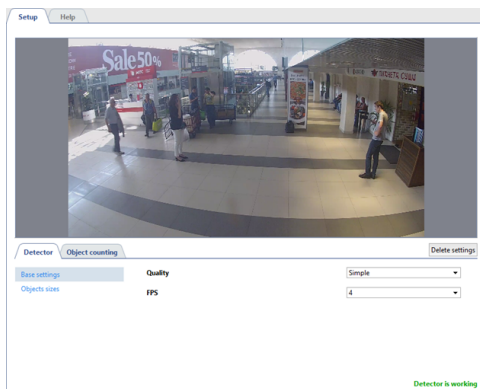
Abandoned items neural detector specifics:

- This plugin operates on **NeuroStation** video recorders or on any 4.x video recorder, connected to **NeuroStation** server, which will be used as the **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.



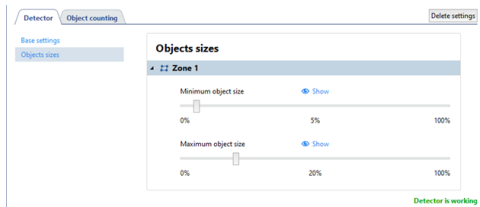
Detector

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.

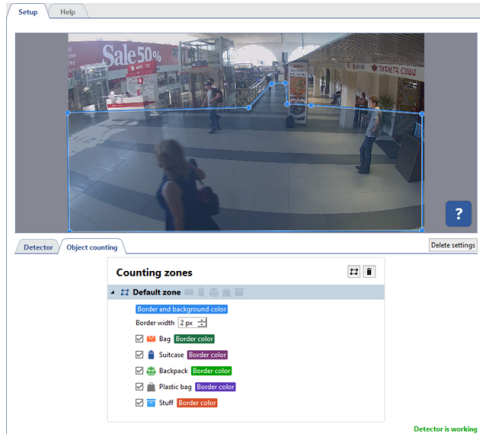


- Create the zones in the **Object size** settings menu. These zones will allow you to select the biggest and the smallest detected object sizes using **Minimal object size** and **Maximum object size** parameters. The object dimensions selection should be based on the detectable object dimensions (boxes, 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 size 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.

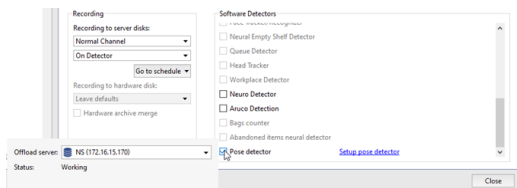
All other postures are classified by the detector as regular.



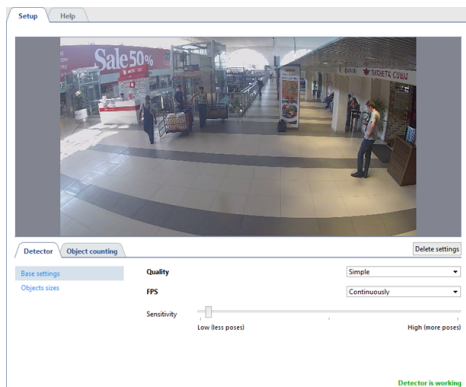
Pose detector features:

- The module works with **NeuroStation** video recorders or on any video recorders of 4.x version, connected to **NeuroStation** server and using it as **Server Analytics**. Read more on 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.



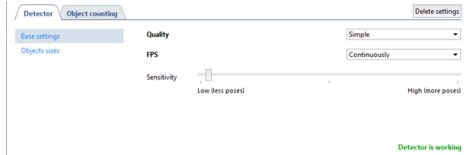
Click the [Setup pose detector](#) link. The settings window will open.



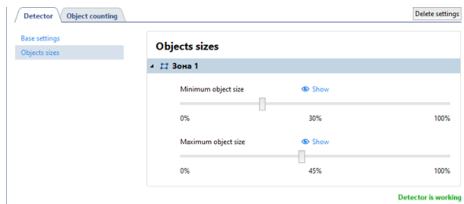
Detector

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.

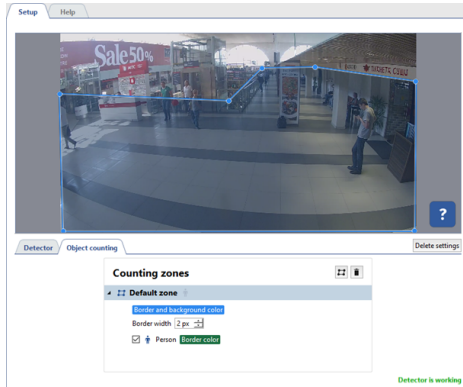



- The **Objects sizes** option lets you create zones in which you should select the biggest and the smallest sizes of a detected object with the help of **Minimal object size** and **Maximum object size** settings. Objects that are smaller than the minimum and larger than the maximum size will not be 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](#)

Camera image quality indicator CiQi

Camera image quality indicator CiQi is neural network module designed to assess the quality of images from street video surveillance cameras. Its purpose is to analyze sharpness, contrast, color and other image parameters. The module makes it possible to enhance control over the territory, increase the efficiency of security services and respond to events.

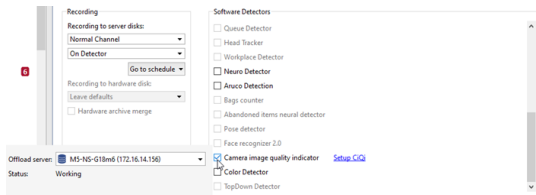
These are some examples of problems to which the module reacts: dirt on the lens, obstacles in front of the camera, environmental changes, and technical issues.



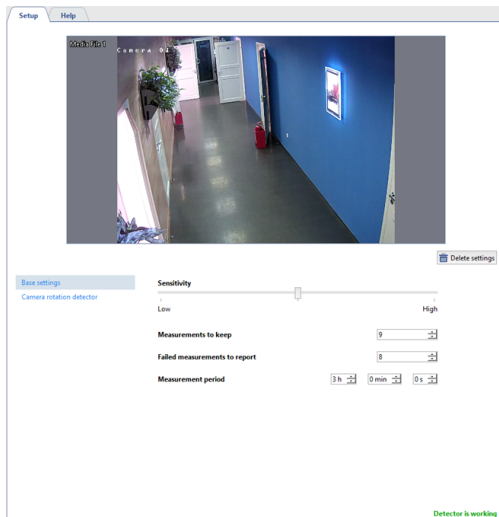
Camera image quality indicator CiQi operation peculiarities:

- The module works on **NeuroStation** network video recorders or any video recorder of version 4.x connected to the **NeuroStation** server and using it as **Analytics Server**. For more information on server connection, check [Connecting to a new server](#).
- Check the [Enable remote analytics](#) flag in the user's settings, which will be connected to the analytics server.
- In the analytics server settings, on the **Analytics** tab, one or more GPUs must have **CiQi Detector** enabled. For more details, see [Analytics](#).

To activate the module, in [Channel Settings](#) in the [Software detectors](#) area, select **Camera image quality indicator** and select **Server**, which will calculate analytics.

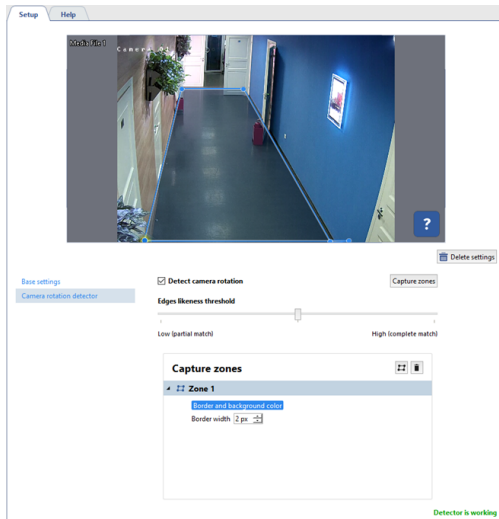


Press **Setup CiQi**. The detector's settings window will open.



In the detector's **base settings** you should:

- Set the detector's **Sensitivity**. A higher value increases sensitivity to image changes, but also increases the probability of false alarms.
- Specify the number of measurements in the **Measurements to keep** settings. It will determine the number of measurements the detector keeps.
- In the **Failed measurements to report** setting, select the number of measurements after which the detector will send a message about changes in the image quality.
- Define the **Measurement period** - the time period, after which the detector will measure the image quality.



In the **Camera rotation detector** settings block, you should:

- Set the **Enable camera rotation detector** flag so that the detector starts analyzing the video stream and tries to determine if the camera is rotated from its normal position.
- Set up **Edges likeness threshold**. This setting determines the level of object boundaries similarity in the image that the system will use to detect camera rotation. The higher the threshold is, the stronger is the similarity of the object boundaries to be detected to consider the camera rotated. This allows you to avoid false positives due to the noise or other artifacts in the image.
- Select **Capture zones**. Specify one area of the image to be analyzed by the detector to determine the camera rotation. Setting the correct capture zone can enhance the accuracy of the analysis and eliminate unnecessary objects or background from consideration.



Enable **CiQi Detector** figure display to monitor changes in the detector's operation (see section ???).

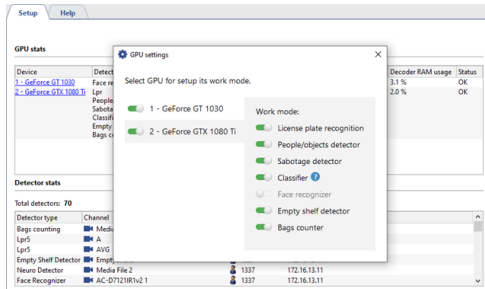


- [Motion detector settings](#)
- [Channel settings](#)

Analytics

One of the problems experienced when building up complex video surveillance systems, where alongside with the archive record the server detects various objects (people, faces, etc.), and analyzes their behavior, is the lack of the server computing resources. In this case, the server lets you move a significant part of the computing resources which are necessary for detectors and video analytics 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 GT 1030	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	Media File 2	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 **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.

TRASSIR ACS

TRASSIR ACS is an access control and management system built into the server, which can:

- determine who, where and when is allowed or not allowed;
- records the pass events and attempts, and sends notifications about them;
- build various types of reports, including time tracking reports.
- and more.

You can find a detailed description of all features in the "Operator's guide" in section ???.

TRASSIR ACS setup procedure:

1. *Connect one or several access controllers to the server. Configure access points and scanners.*
2. *Create a protected area and add access points to the area of use.*
3. *Create one or several access levels and bind the corresponding access points to them.*
4. *Add persons and assign access levels to them.*

To **expand the TRASSIR ACS functionality**, create:

- *work schedules which will be used for building various reports;*
- *various reports;*
- *pass requests templates;*
- *events notifications;*
- *connect to LDAP server;*
- *exculpatory documents approving the employee's absence in the workplace;*
- *pass card design for printing;*
- *rules of passage to the protected areas;*
- *a profile to protect your cards' data.*

You can also *use audit* to **monitor users' actions**, performed in various TRASSIR ACS sections.



You can access **TRASSIR ACS** settings not only via the server settings, but also via web browser. Read more in ???.



You can get acquainted with the **TRASSIR ACS** module functionality in **Demo version**. **TRASSIR ACS** in software 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 the server and configuration of their parameters.

Go to **Plugins** -> **Access Control** -> **Devices** to open.

The screenshot shows the 'Controller' configuration window. The sidebar on the left lists various locations: Company, Office, Entrance, Exit, Warehouse, Fire alarm, and Buzzer. The main configuration area includes the following fields and options:

- Name:** Company
- Family:** Trasair
- Model:** TR-C481
- IP address:** 192.168.50.252
- Port:** 8002
- Login:** admin
- Password:** (empty field)
- Time zone:** By server
- Data format:** Wiegand 26/34
- Access cards:** 2/100000
- Device memory:** (empty field)
- ADVANCED OPTIONS:** (checked)
- AUTONOMOUS RULES:** (checked)

You can find a detailed description of the **Devices** section operation process in the following sections:

- *Connection of controller*
- *Access points settings*
- *Card reader settings*
- *GPIO settings*
- *Autonomous rules settings*

Connection of controller



Before connecting the controller, learn more about its setup and operation features:

- [Features of Hikvision controllers setup and operation.](#)
- [Features of ZKTeco devices setup and operation.](#)

In order to connect the controller to the server, go to the server settings to the **Plugins** -> **Access Control** -> **Devices**, press **Add Controller** and enter the connection parameters into the opened window.



TRASSIR ACS includes a software controller that enables management of GPIO outputs for devices connected to the server (e.g., cameras). This solution is suitable for organizing access with authentication in conditions where installing a hardware controller is not possible.

To connect the software controller, select it in the **Family** field. Learn more in the [Connecting and configuring a software controller](#).

In case of the controller successful server connection, you will see access points on the device connection page. Otherwise, the error message appears.

The **Persons**, depending on their access level, are automatically uploaded to all connected controllers. You can update data on any specific controller, if necessary. To do this, press **Synchronize data**.

If your controller and server are in different time zones, you can configure the **Time Zone** parameter. This allows the device's local time to be synchronized with its time zone while events are logged using the server's time.

The information about the maximum memory capacity of the device and the memory level in the connection settings may vary depending on the connected device.

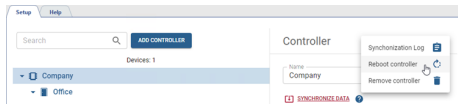
TRASSIR ACS supports operation from GPIO controller. Open the **Advanced Options** to activate it and set the flags next to the required inputs or outputs. After saving the settings, they will be added as independent controller objects.


Read more on GPIO configuration in [GPIO settings](#).

If a terminal connected to the controller is used during person authentication and passage, the **Access granted** and **Pass** events occur on both devices. To disable message reception from the device, set the **Use as reader** flag.

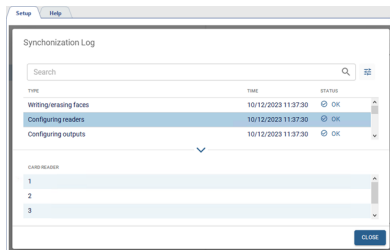
With **Autonomous rules**, you can configure various rules to be executed depending on the current state of the controller, access points, readers, or GPIO inputs.

See more on setting up autonomous rules in [Autonomous rules settings](#).



Click  to do the next steps:

- Open the **Synchronization Log**, which records all synchronization events, date and time of execution, and their status. Select the event in the log to check the detailed information.

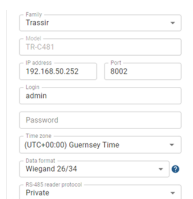


- **Reboot controller**. If this item is selected, a command will be sent to the controller for reboot.
- **Remove controller** from Access Control settings.

Features of setting up controllers of different manufacturers

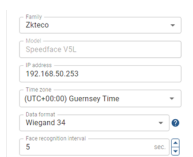
Select in **TRASSIR TR-C481** controller connections settings:

- in the **Data format** field - the format used for storing card numbers in the database: **Wiegand 58** or **Wiegand 26/34**;
- in the field **RS-485 reader protocol** - one of the protocols: **OEM** or **OSDP**, depending on which protocol the reader uses to transfer data to the controller.



In **ZKTeco** controller connection settings in the **Data format** field, it is necessary to select the format to be used for storing card numbers in the database: **Wiegand 34** or **Wiegand 26**. In this case, the data format in the connection settings should match the format set on the readers connected to this controller.

Set the periodicity with which people's faces will be recognized in the **Face recognition interval** field. If the same recognition events appear in the log - increase the value of the interval.

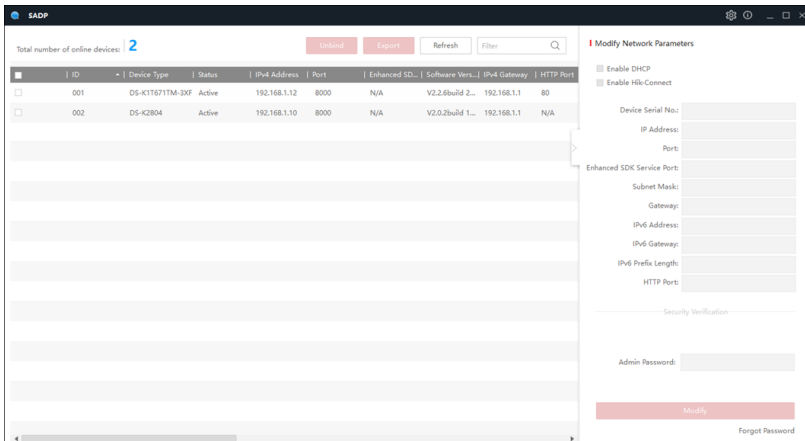


When designing or upgrading an Access Control, it is important to note that **the system can be configured to work with only one data format: **Wiegand 34** or **Wiegand 26**.**

It should also be taken into account that some devices support only one data format. A card read and written as an identifier in the **Wiegand 26** format can not be used on a device that works with the **Wiegand 34** format and vice versa.

Features of Hikvision controllers setup and operation

Before connecting the Hikvision controllers to the server, you need to turn it on, connect to the local network, and configure the network settings. Use the SADP utility that you can download from [our website](#) to find the controller in the local network.



Check the controller's user manual for more information on the controller settings.

Features of Hikvision controllers operation

- 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 the server, 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** is the 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 ACS.

Features of ZKTeco devices operation

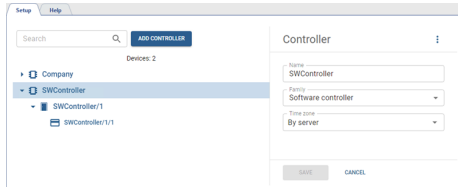
- TRASSIR ACS does not support some authentication modes (by palm, finger veins or QR code), available on ZKTeco terminals. You can see the list of all supported modes in the **reader settings**, after connecting the device.
- The card numbers, read out on ZKTeco terminals, can be used for authentication 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.

Connecting and configuring a software controller

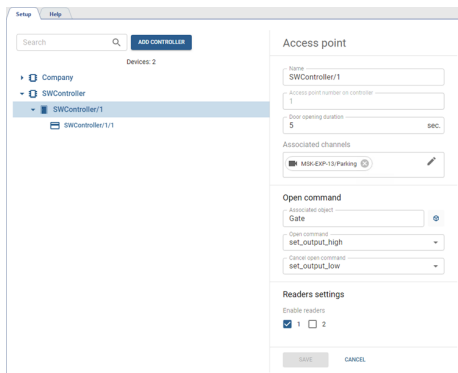


The number of software controllers is determined by the corresponding license.

To connect a software controller, open the server settings, navigate to **Modules** -> **ACS** -> **Devices**, click **Add Controller**, and in the opened menu, select **Software Controller** in the **Family** field.



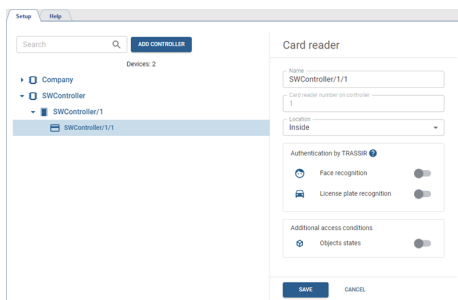
If your controller and GPIO device are in different time zones, you can configure the **Time Zone** parameter. This allows the device's local time to be synchronized with its time zone while events are logged using the server's time. Select an access point and configure its parameters.



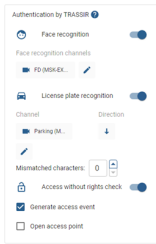
Configure the access point parameters:

- **Name** which will be displayed in the *object tree*.
- In the **Door opening duration** field, select the duration for which the door lock will remain unlocked.
- In the **Associated Channels** field, select video channels to associate them with all events that occur and are logged at this access point. When reviewing events, video from these channels will be displayed in the *TRASSIR ACS template* or on the active monitor.
- In the **Open command** settings block, choose the **Associated object**, to which commands configured below will be sequentially sent, with the interval specified in the **Door opening duration** field.
- In the **Readers settings** block, specify the number of readers the access point will use for personnel authentication. Enable the flags next to the desired readers.

Select a reader, enter its **Name**, and choose its **Location**.



Configure the reader parameters:



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.



All modules used for authentication should be enabled and configured. Read more in: [Face recognizer](#) and [AutoTRASSIR/AutoPass - Automated license plate recognition](#).

The [face database](#) will be used for the face recognition.

The license plate numbers specified in [personnel settings](#) will be used for license plate recognition.

When using the **License Plate Recognition** module, select the direction of vehicle movement and define the error (from 0 to 3 characters) with which the license plate numbers will be searched for in the person's settings.



For example, if the **Mismatched symbols** setting value is set to 1, and one of the person has the **m221co177** number.

If AutoTRASSIR makes a one character error when recognizing a license plate number and instead of **m221co177** recognizes **a221co177** or **m221co77**, the wrongly recognized number will match the person's number due to the set inaccuracy, and TRASSIR ACS will let the vehicle through.

To simplify the entry or exit of vehicles onto a secured area, enable **Access without rights check**. In this case, all vehicles will be granted access without identifying a person.

Enable the **Generate access event** so that the ACS ignores access levels and generates an **Access granted** event for all vehicles with a number, which will appear in the **Access Control Log** of the operator interface.

If the **Open access point** is enabled, after generating the **Access granted** event, the command **Open once** will be sent to the access point.



In the **Additional access conditions** setting, you can enable the **Objects states** option to specify GPIO input/output states required for access after successful identifier authentication.

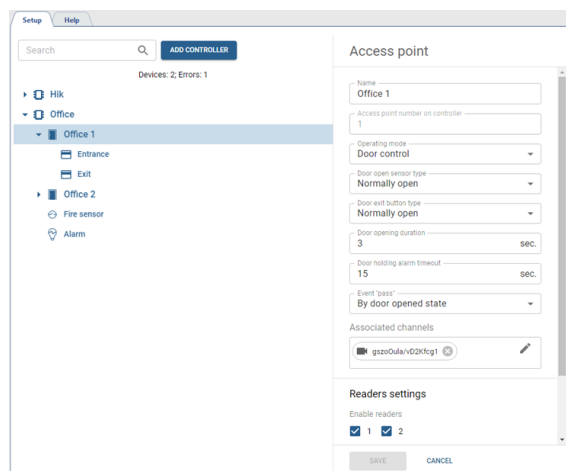
Access will be granted only once—after the object's state changes to the one specified in the settings and within the time set in the **Status waiting timeout** field.



If the authentication settings are configured for simultaneous use of **Authentication mode** and **Authentication by TRASSIR**, and the **AND** option is selected, the time between the two authentications is determined by the value specified in the **Status waiting timeout** field.

Access points settings

The number of access points is determined by the controller technical characteristics. You need to configure them for further use.



To do this, select the access point and configure the following parameters:

- **Name** which will be displayed in the *object tree*.
- Select mode, in which the access point will operate in the **Work mode** field.
The **Door control** mode is the standard access point operation mode, suitable for all readers.
The **Turnstile control** mode is a special mode that uses a pulse of less than 1 sec to open the door and replaces the "Door breaking" event with the "Passing" event.
- Select the door sensor state, which occurs when 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.
If the value **Turnstile control** is selected in the **Work mode** field, the value of the interval must be 1 sec.
- 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 **Event "pass"** field, select on which event, generated on access point, TRASSIR ACS will create the **Pass** event in *Access Control log*:
By door opened state - upon successful authorization, when the door is opened;
By door open event - after successful authorization, as a result of which the door was opened. This option should be used in case the **Turnstile control** value is selected in the **Work mode** field.
- In the **Associated Channels** field, select video channels to associate them with all events that occur and are logged at this access point. When reviewing events, video from these channels will be displayed in the *TRASSIR ACS template* or on the active monitor.
- In order to define the list of readers that the access point will use, open the **Advanced options** and enable the flags next to the required readers.
- The **Confirmation settings** area lets you enable the access point's mode of operation in which the confirmation for certain people to pass will be required.
To do this, select **Confirmation type**, set **Confirmation timeout** and specify **Users need confirmation** and **Users allowed to confirm**.
For the **Operator** and **Breathalyzer** confirmation types, it is possible to set a random check of persons and specify the probability as a percentage of all persons selected for the confirmation pass.



In case of confirmation by the **Operator**, **Users allowed to confirm** must be linked to the server users (check [Creating a new person](#)).
The process of operator pass confirmation is described in [???](#).



Features of **Passage Confirmation**:

- this feature is not supported by all devices (check the instruction manual for the connected device);
- the confirmation of the passage **By Breathalyzer** is available with the appropriate license;
- the feature is not supported when the access point is included in the **Software gateway** (see [Rules of passage](#));
- the simultaneous use of **Passage confirmation** and **Authentication by TRASSIR** is not available.



Using access points, you can configure various rules that will be executed depending on their current state.
See more on setting up autonomous rules in [Autonomous rules settings](#).

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 server 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.



The simultaneous use of **Authentication by TRASSIR** and **Passage confirmation** is not available.

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.



If **AND** is selected, the time between the two authentications (**Authentication by TRASSIR** and **Authentication Mode**) depends on which authentication happens first:

- **no more than 10 seconds**, if the first authentication is via the reader (specified in the **Authentication Mode** field);
- **no more than 20 seconds**, if the first authentication is **Authentication by TRASSIR**.



If the **Shared license plate number** feature is enabled in **personnel settings** as an identifier, it is recommended to select the **AND** option. When selecting the **OR** option, the person will be recognized as an **Unknown Person** with an event **Access Denied**.



All modules used for authentication should be enabled and configured. Read more in: **Face recognizer** and **AutoTRASSIR/AutoPass - Automated license plate recognition**.

The **face database** will be used for the face recognition.

The license plate numbers specified in **personnel settings** will be used for license plate recognition.

When using the **License Plate Recognition** module, select the direction of vehicle movement and define the error (from 0 to 3 characters) with which the license plate numbers will be searched for in the person's settings.



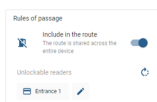
For example, if the **Mismatched symbols** setting value is set to 1, and one of the person has the **m221co177** number.

If AutoTRASSIR makes a one character error when recognizing a license plate number and instead of **m221co177** recognizes **a221co177** or **m221co77**, the wrongly recognized number will match the person's number due to the set inaccuracy, and TRASSIR ACS will let the vehicle through.

To simplify the entry or exit of vehicles onto a secured area, enable **Access without rights check**. In this case, all vehicles will be granted access without identifying a person.

Enable the **Generate access event** so that the ACS ignores access levels and generates an **Access granted** event for all vehicles with a number, which will appear in the **Access Control Log** of the operator interface.


If the **Open access point** is enabled, after generating the **Access granted** event, the command **Open once** will be sent to the access point.



In order to build a passage route in a certain area or inside a building, use the **Rules of passage** setting. Set the **Include in the route** flag and select the readers to configure the rules. The **Unlockable Readers** list will contain the readers that will become available after passing through the customized reader.

For example, if you have two readers, you can specify the second reader in the settings of the first reader and the first reader in the settings of the second one. Thus, after passing through the first reader, the second reader will be activated and vice versa. In this case, the visitor will be able to enter through the first reader, but exit only through the second one. Further passes through the same reader will not be available.

You can build more complex routes if you have three and more readers.

Click  to reset the current person's location and let the person authorize again.



Features of rules of passage usage:

- The rules of passage setting is available only on **Hikvision** and **TRASSIR TR-C241/TR-C481** readers.
- You can build only one route on one device. For the pass rule to work, the flag **Include in the route** must be set on all configurable readers.
- The feature interacts directly with the card readers and doesn't need constant server connection to the card reader. At the same time, the cards on the device will be rewritten after any change in the feature settings.
- The feature is not supported when the access point connected to the card reader is included in the **Software gateway** (see [Rules of passage](#)).



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.

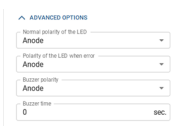


Select the **Temperature** mode in the **Authentication mode** setting, enable **Temperature control** and set the **Upper threshold** to make the reader operate in the thermometer mode, determining the temperature of people passing by. Other modes of authentication will not be available in this mode.

Additionally, you can enable the **Objects states** option to specify the state of GPIO inputs and/or outputs required to grant access after successful authentication by identifier. Access will be granted only once—after the object's state changes to the one specified in the settings and within the time set in the **Status waiting timeout** field.



If the authentication settings are configured for simultaneous use of **Authentication mode** and **Authentication by TRASSIR**, and the **AND** option is selected, the time between the two authentications is determined by the value specified in the **Status waiting timeout** field.



The reader's **Advanced options** let you change the polarity of the light indicator and the buzzer, as well as the duration of the alarm.



Using readers, you can configure various rules that will be executed depending on their current state. See more on setting up autonomous rules in [Autonomous rules settings](#).

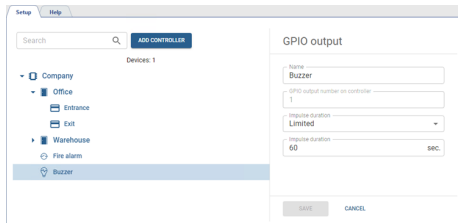
GPIO settings

The **GPIO input** is the port of the controller which is intended to receive signals about the occurrence of some alarm event. You can change its **Name** if necessary.



The screenshot shows the 'GPIO input' configuration window. On the left, a tree view shows the hierarchy: Company > Office > Entrance > Exit > Warehouse > Fire alarm > Buzzer. The 'Buzzer' device is selected. The main panel is titled 'GPIO input' and contains the following fields: 'Name' (set to 'Fire alarm'), 'GPIO input number on controller' (set to '1'), and 'GPIO input type' (set to 'Normally open'). At the bottom are 'SAVE' and 'CANCEL' buttons.

The **GPIO output** is used to indicate alarm conditions. You can change its **Name**, if necessary.



The screenshot shows the 'GPIO output' configuration window. On the left, the same tree view is shown, but 'Buzzer' is selected under the 'Warehouse' category. The main panel is titled 'GPIO output' and contains the following fields: 'Name' (set to 'Buzzer'), 'GPIO output number on controller' (set to '1'), 'Impulse duration' (set to 'Limited'), and 'Impulse duration' (set to '60' with a 'SEC' unit). At the bottom are 'SAVE' and 'CANCEL' buttons.

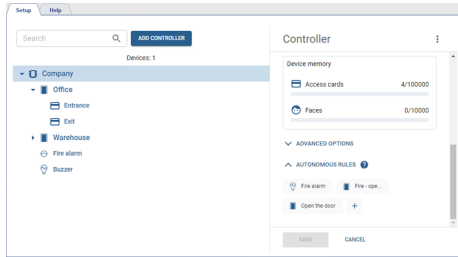
Additionally, you can specify the time during which an impulse will be sent to the **GPIO output** contacts. To do this, in the **Impulse duration** field, select **Limited** and specify the time in seconds.



Using GPIO inputs, you can configure various rules that will be executed depending on their current state. See more on setting up autonomous rules in [Autonomous rules settings](#).

Autonomous rules settings

To create autonomous rules, open the server settings section **Modules -> PACS -> Devices**, select the controller, and open **Autonomous Rules** in its settings.



To create a rule, click the button **+**.


Next:

1. Enter the **Name** of the rule.
2. Select **Origin** and **Event** for the rule to be executed.

The list of available events depends on the selected origin:

- Events for **Controller**: Controller tampering alarm, Network - disconnected, Network - recovered, Battery - low voltage, Battery - voltage recovered, AC power - off, AC power - recovered.
- Events for **Access point**: Opened, Closed, Button press, Remote open, Break-in, Open timeout, Unlocked, Locked, Workmode always open - started, Workmode always open - stop, Workmode always close - started, Workmode always close - stop, Multifactor authentication - success, Multifactor authentication - need remote open, Multifactor authentication - failed, Multifactor authentication - timeout.
- Events for **Card reader**: Access granted, Access denied, Card reader tamper alarm, Card swipe.
- Events for **GPIO inputs**: Input Low to High, Input High to Low.



If the **Card reader** is selected as the source and **Card reading** as the event, an additional **Card number** field appears in the rule. The rule will be executed only when the specified card number is read. To enter the number, click  and select or manually enter the person's card number. Note that the rule uses the card ID, not the person associated with it. This means the rule remains active even if the person is deleted, as the card number stays in the rule. You can reassign the card to another person or delete the rule if necessary.

3. Select the **Type**, and depending on it, the **Object** and **Action**:

- for the **Access points control** type, the objects will be access points of the controller, and the action will be the command sent to them;
- for the **GPIO outputs control** type, the objects will be the GPIO outputs of the controller, and the action will be the command to close or open the output.



All created rules are stored in the controller memory and will function in the event of a connection loss between the controller and the TRASSIR ACS server.

Examples of rules:

Setting up a rule

Name

Open the door

Origin

Distance

Event

Card swipe

Card number

2345678901

John Smith

Type

Access points control

Object

Warehouse

Action

Open once

SAVE

CANCEL

Setting up a rule

Name

Fire - open the doors

Origin

Fire alarm

Event

Input Low to High

Type

Access points control

Object

Office, Warehouse

Action

Workmode always open

SAVE

CANCEL

Setting up a rule

Name

Fire alarm

Origin

Fire alarm

Event

Input Low to High

Type

GPIO outputs control

Object

Buzzer

Action

Set output high

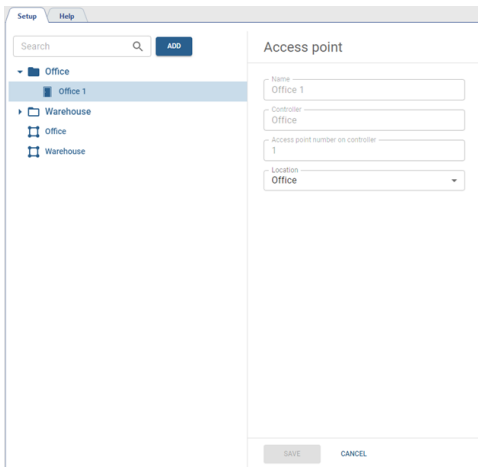
SAVE

CANCEL

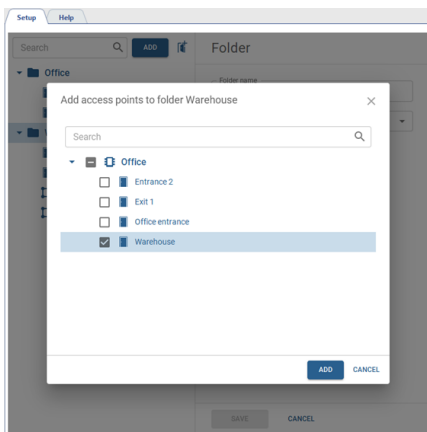
Areas of use

Open the **Plugins** -> **Access Control** -> **Areas** section to set up the zones.

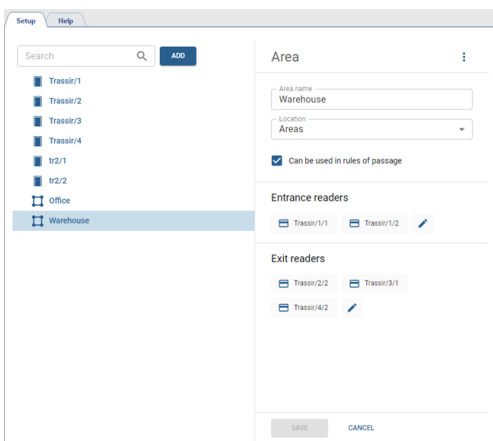
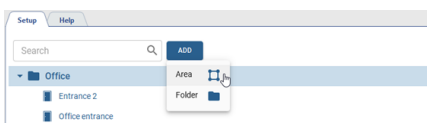
All **access points** appear in the **Areas** section automatically. You can also group them into folders for your convenience. To do this, create the required folders amount and select **Location** in the access point settings.



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.



In order to track the movement of persons inside the secured perimeter, you must create zones and select readers that will identify persons entering and exiting the zone. To do this, click **Add**, select **Area** and specify all the necessary parameters.



Set the **Can be used in rules of passage** flag, to enable the option to specify this area in rules of passage settings (see [Rules of passage](#)).

Work schedules

This section allows you to create and edit work schedules that are used to determine the working time of an employee when building [various reports](#).

Go to **Plugins -> Access Control -> Work Schedule** to open.

In order to create a new work schedule, press **Add** and follow the next steps:

- add a new work schedule name that will be displayed in the [person's settings](#);
- add comment, if necessary;
- add groups of persons or individual person to whom this work schedule will be assigned;
- customize the schedule (the detailed instructions on how to customize the schedule are described below).

After creating a work schedule, you can check its timing for the week as well as for the month.

Schedule settings

You can use the following schedule types when creating:

- **Calendar week** is a schedule that lets you create a working schedule with reference to the specific days of the week.
- **Shifts** is a schedule that specifies a cycle of intervals in which the work schedule depends on the day number in the cycle.

Press **Setup schedule** to open the schedule settings.

Follow the next steps to create the **Calendar week** schedule type:

1. Use the **Working day/Day off** flag to identify working days and days off.
2. Select one of the workdays, and use the sliders or the **Beginning** and **End** fields to set up the start and the end time of the workday and, if necessary, add one or several breaks.
3. Press the **Duplicate for all work shifts** link to copy the created schedule to all working days of the week.

Follow the next steps to create the **Shifts** schedule type:

1. Set the start date of the first shift and create the desired number of working and weekend shifts.
2. Select one of the work shifts, and use the sliders or the **Beginning** and **End** fields to set up the start and the end time of the shift and, if necessary, add one or several breaks.
3. Click **Duplicate for all shifts** to copy the created schedule to other shifts.



The breaks define only the interval of time during which a person can be absent from the workplace for the entire working day. The strict time limits for the beginning and end of breaks are not taken into account in Access Control.



In order to create a shift that begins on one day and ends on another, choose the time in the **End** field that is less than or equal to the time in the **Beginning** field.

5-2

The **Holidays** tabs lets you add the dates, in which another schedule will be in effect (for example, on pre-holiday and holiday days).

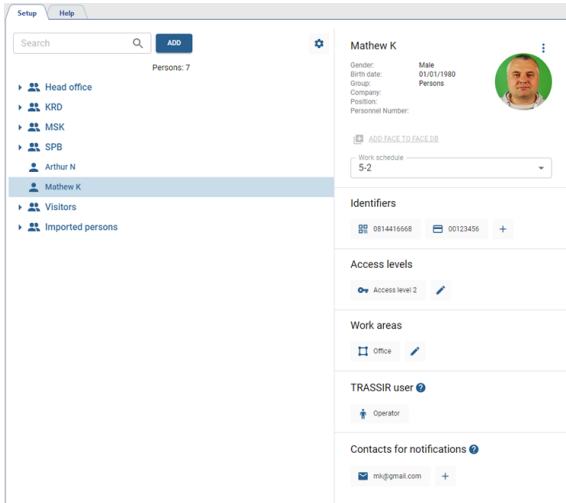
The **Variations** tab provides parameters that can be used for more flexible customization of the employees' working schedules.

- The **Delays and early leaves** parameter defines the maximum time intervals that will be used to calculate lateness or early departures. If an employee comes in late or leaves early, the difference between the actual time and the scheduled time will be reported as **Delays** or **Early leaves**.
- The **Consider overtime** parameter sets the minimum time that will be used to calculate overtime. If an employee comes in earlier or leaves later than the set time period, the time worked by the employee will be reported as **Overtime**.
- The **Allow work on weekends** parameter sets the minimum time that will be used to calculate overtime when working on weekends. If an employee works on weekend for more than the specified time, the actual time worked will be reflected in the report as **Overtime**.
- The **Work area leaving** parameter sets the minimum time for which an employee can leave his workplace. If an employee will be absent more than the specified time, this time of absence will be indicated as **Absenteeism** in the reports.

Personnel

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 server modules (for example, by *Face Recognizer*).

Open **Plugins->Access Control->Personnel**.



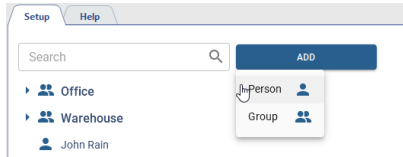
At least one *access level* should be created for operation with TRASSIR ACS persons.

A detailed description of the process for working with the **Personnel** section is outlined in the following sections:


- *Creating a group*
- *Creating a new person*
- *Additional actions with persons*

Creating a group

To create a new group, open **Plugins->Access Control->Personnel**, press **Add** and select **Group**.



After that:

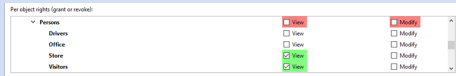
- Enter the **Group name** and select its **Location** in the persons' tree.
Click  next to the **Location** field, to save the current group location to the clipboard. It can be used when **creating a file** to import new persons into the same group.
- Set the **Assign general parameters** flag to let the group parameters be inherited by all the persons added to this group.
Set the parameter values that will be automatically assigned to all persons in that group.
All assigned parameters will become unavailable for the person in the group after the saving. In order to keep the editing options, set the **Allow to change person's settings** flag.

The **Imported persons** group displays the persons imported from TRASSIR ACS Enterprise. Read more in **Personnel**.



You can use *rights to individual server objects* to assign viewing and management access to various groups of persons.

The rights are located on the rights tree at: **Server name** -> **Server settings** -> **Persons**.

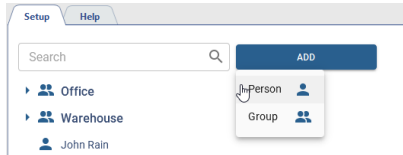


Creating a new person




At least one **access level** should be created for operation with TRASSIR ACS persons.


In order to create a new Access Control person, open **Plugins->Access Control->Personnel**, press **Add** and select **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.

Click  next to the **Group** field, to save the current person's location to the clipboard. It can be used when **creating a file** to import new persons into the same group.

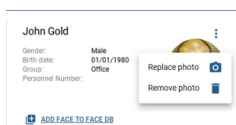
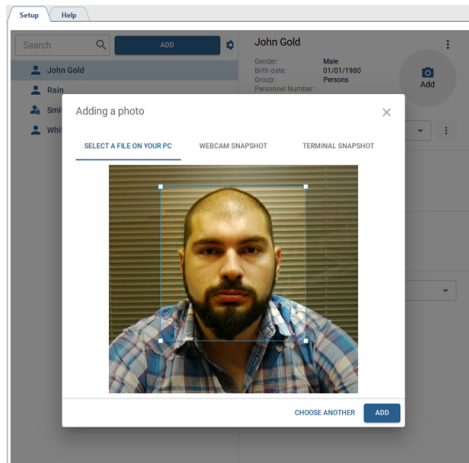
The **Department** and **Job title** are the additional person's fields that can be created by pressing .

Set the **Period of access rights** for this person in order to set limit to use identifiers and access levels.

2. Upload an employee's photo by pressing **Add photo**.

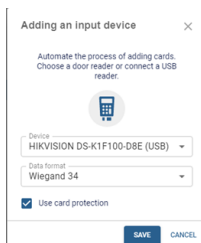
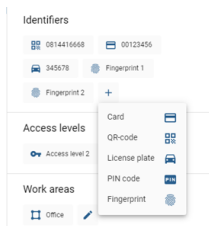
In the window that opens, select one of the ways: **Select a file on your PC**, **Webcam snapshot** or **Terminal snapshot** and add the employee's photo.

When uploading a photo from your PC or creating a photo using webcam, you can use the crop feature to resize the added photo.



In order to use the face for *Face Recognizer* authentication, click **Add face to face DB**. If a controller or terminal that can recognize faces is added to the Access Control, the photo with the face 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 *Work schedules*).
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 the client/server;
- using the reader installed at the access point;
- by entering the card data into the input field manually.

Set the **Use card protection** flag, to protect the card data using the active profile configured in section *Card protection*.



If **UID type** is set to **Manual input** in the profile settings, the **Use card protection** function is unavailable.



Features of data entry from identification cards:

- Data input from an ID card using a USB reader is only supported in **Windows version**.
- ZKTeco CR10 and ZKTeco CR20 readers transfer data in keyboard emulation mode. That's why you should use **Without reader (manual input)** mode in order to enter ID card data using these readers.
- ZKTeco USB readers store data in **Wiegand 34** format. If the readers used by personnel for authentication use **Wiegand 26** format, set the **Convert to Wiegand 26** flag when adding the card.
- HIKVISION DS-K1F180-D8E USB reader supports data protection when using **Wiegand 26** and **Wiegand 34** formats. For the **Wiegand 58** format, data protection is unavailable - the **Use card protection** flag must be disabled, and the card data must be 7 bytes in size.



QR Code - download an automatically generated QR code that can be used to authenticate with a QR code scanner.

License plate - enter the vehicle license plate number that will be used for **AutoTRASSIR** module authentication.

When saving, ACS checks the uniqueness of the vehicle's license plate number. If multiple persons use the same number, enable the **Shared license plate number** option for all persons using this number to bypass the uniqueness check.



It is recommended to use the **Shared license plate number** feature if the **reader authentication mode settings** have the **AND** option selected. If the **OR** option is selected, the person will be recognized as an **Unknown person** with the event **Access denied**.



When entering the number, you can use letters of Latin alphabet, as well as "mask", in which unknown characters are replaced by "*" or "?". The **"?"** symbol is used to indicate only one unknown character, and the **"**"** symbol - one or more unknown characters. For example, if the license plate number is known, but the region is unknown, you can use the following types of masks:

b663kt?? - for numbers with two-digit region only: **b663kt77** or **b663kt95**.

b663kt??? - for numbers with a three-digit region only: **b663kt777** or **b663kt190**.

b663kt* - for numbers with both two- or three-digit regions: **b663kt77** or **b663kt190**.

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 **reader's settings**.

- Assign the corresponding **Access levels** to a person (see section **Person access levels**).

- Assign **Rules of passage** to protected areas to a person (see **Rules of passage**).

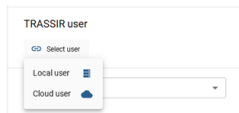


In order to reset the current location of a person, click . The person will be able to authorize again to enter or exit the zone.

- Select **Work areas** to track the person within the secured perimeter (see **Areas of use**).

- Enter a local or cloud user account so that user will be **allowed to confirm**, and use **WEB interface** and **mobile app** to work with TRASSIR ACS.

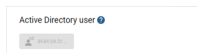
Enter a local user account so that user will be **allowed to confirm**, and use **WEB interface** to work with TRASSIR ACS.



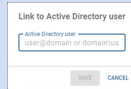
The access rights to the TRASSIR ACS module are set depending on the user type:

- local users - in server settings (check [Determining access rights](#));
- cloud users - in TRASSIR Cloud settings (check [???](#)).

9. When using the function [Data Synchronization](#) an Active Directory account associated with the person is displayed under the **Active Directory user**.



Click **Select user** and enter the user data to link the person manually to the Active Directory account.




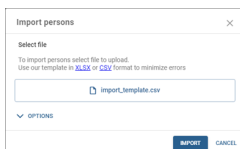
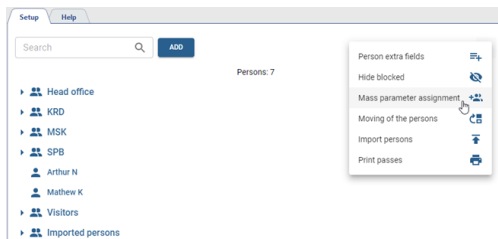
- 10 Add contact information to receive notifications about TRASSIR ACS events (see [Notifications](#)).



Enter your ID from telegram bot [@trassirbot](#) as your **Telegram ID**. In order to find out your ID, open the bot and run the **/start** command.

Import of persons

In case you need to add a large number of personnel, there is an import function. To activate it, click  and select **Import persons** feature.



Select a file with a list of persons.

Use a ready-made template to simplify the process of creating a persons list.

When importing persons with extra fields, make sure these fields already exist in Access Control settings.

In the case the **Block Time** parameter is used, which specifies the time period for which the user will be blocked, you should pay attention to:

- If the value in the cell is less than the current date, the user will be imported with the **Blocked** status.
- If the value in the cell is greater than the current date or time (if the date is the same), the user will be created with the **End** parameter filled in the **Period of access rights** setting. The user will be locked once the specified date and time occurs.
- If the value in the cell is empty, the user will be created without this parameter.

Make sure you use the proper value format in the columns before import:

- **Group** - a text field in which groups and subgroups are written with a "/" (e.g. Company/Department/Division);
- **Birth date** - a date in the format DD.MM.YYYY;
- **Block time** - date and time in the format DD.MM.YYYY HH:MM:SS;
- in the rest of the columns - text.

Configure the necessary import parameters:

The 'Import persons' dialog box contains the following sections and options:

- Actions on existing persons:**
 - ☒ Keep and add new ones
 - ☐ Remove and add new ones instead
- Actions when names match:**
 - ☒ Add new persons
 - ☐ Overwrite existing persons
 - ☐ Update existing persons
- Bounds of name matching check:**
 - ☒ All persons
 - ☐ One group
- Use hexadecimal format for cards:**
 - ☐ Yes
 - ☒ No
- Date format:**
 - DD.MM.YYYY (selected)
- Fields delimiter (for CSV format):**
 - ☒ Colon (,)
 - ☐ Semicolon (;)
- Quote character (for CSV format):**
 - ☒ Double quote (")
 - ☐ Single quote (')

Buttons: **IMPORT** and **CANCEL**.

- **Actions on existing persons** - select one of the options the system should perform when existing persons are detected during the import process.
- **Actions when names match** - specify what will occur if matching names are found during the import process.
- **Bounds of name matching check** - customize name matching check. When the **All persons** option is selected, the system will respond to name matches in the entire list of persons. If **One group** is selected, the check will be limited to name matches within the groups specified in the file.
- **Use hexadecimal format for cards** - enable or disable the use of hexadecimal card format when importing data.
- **Fields delimiter** - specify the symbol to be used as a separator between data fields during import.
- **Quote character** - specify which character will be used as the quotation marks' opening and closing character.
- **Date format** - select the format in which the dates in the imported data are displayed.

Click **Import** to load the data.

The 'Import persons' dialog box shows a progress indicator with a circular arrow icon and the text: "Import in progress, completed 0 of 165". A **CANCEL** button is at the bottom right.

The 'Import persons' dialog box shows a green checkmark icon and the text: "Import completed successfully". Below this, it displays statistics: "Imported: 1", "Added: 1", "Changed: 0", and "Left without changes: 0". A **CLOSE** button is at the bottom right.

All added persons will be displayed after updating the **Personnel** section.

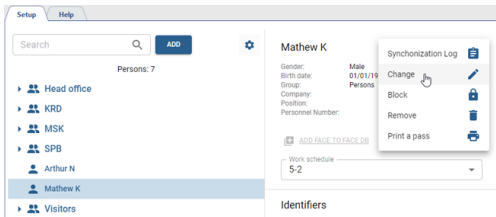
Additional actions with persons

In order to find the required person, you can use the filter that searches for a person not only by name but also by company, job title, time card number, access card, license plate number and additional fields.



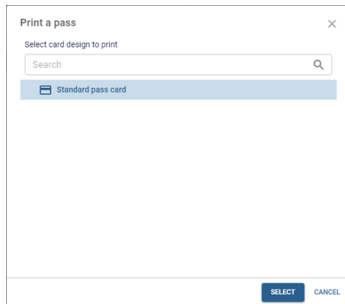
Actions with one person

To enter the single-person action mode, press  next to the photo and select the appropriate menu item.



- **Print a pass**

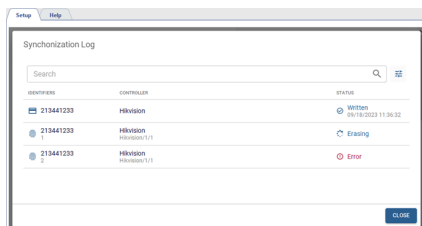
To print a pass, select **Print a pass** and, in the window that opens, select a layout option.



The **Print passes** feature is available only with the corresponding license. The process of pass layout creation is described in [Pass design](#).

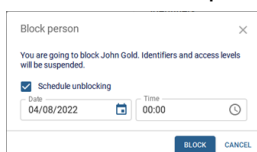
- **Synchronization log review**

Select **Synchronization Log** to open a list of person IDs that have been sent to all devices available to this person and their status.

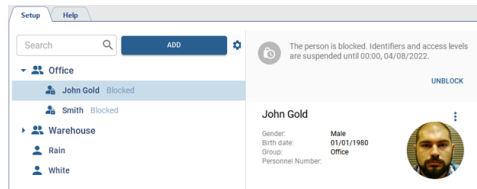


- **Locking/unlocking a person**


In order to block a person, select the corresponding menu item and specify the date when the person is automatically unlocked in the opened window, if necessary.

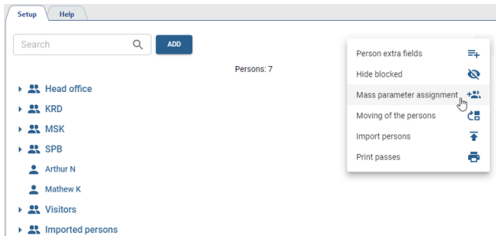


The blocked person will be marked with a corresponding icon and caption. You can unblock it any time by pressing **Unblock**.



Actions with several persons

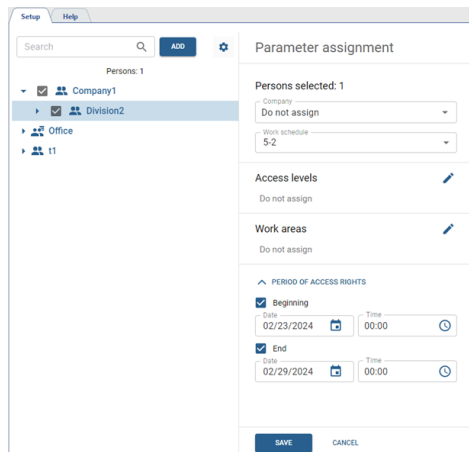
To enter the multi-person action mode, press  and select the appropriate menu item.



The **Person extra fields** and **Import persons** features are described in [Creating a new person](#)

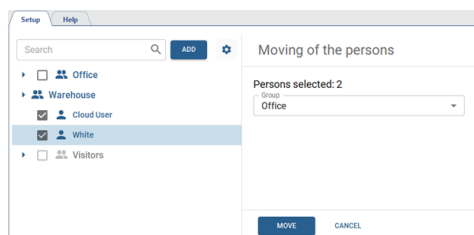
- **Mass parameter assignment**

Select **Mass parameter assignment** to enter the mass person parameter modification mode. Next, select the required persons and the parameters to be assigned to those persons.



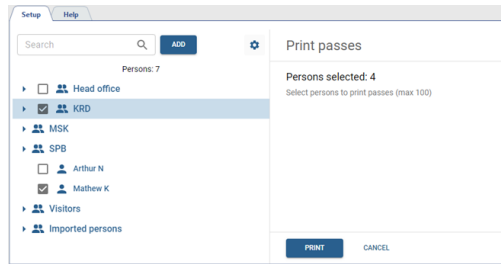
- **Moving of persons**

The **Moving of the persons** features works the same way. Instead of parameters, you need to select the group to which the selected persons will be moved.

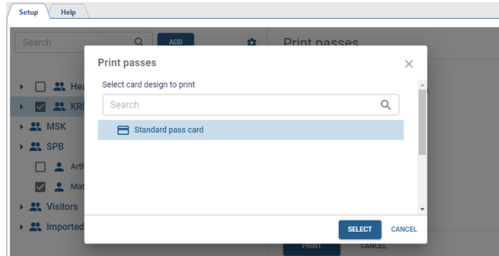


- **Print a pass**

Select **Print passes** to print out the pass cards. After that, select persons or group of persons for which you want to print pass cards and click **Print**.



In the window that opens, select a layout option.



The **Print passes** feature is available only with the corresponding license.
The process of pass layout creation is described in [Pass design](#).

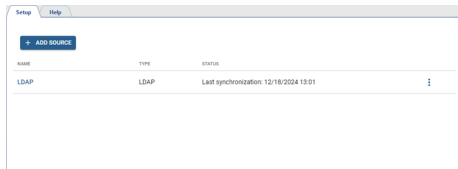
Data Synchronization

This section allows you to set a LDAP server connection. After the setup, the connection will be used to automatically update and synchronize *persons data*.



TRASSIR ACS supports synchronization with LDAP servers using **LDAPv3** protocol and **Basic** authentication.

To open the section go to **Plugins** -> **Access Control** -> **Data synchronization**.



To create new connection press **Add source**, select **LDAP** and perform the following:

1. Enter the **Name** of the source.
2. **Setup a LDAP server connection.**

The server connection settings window opens, fill the fields: **Address**, **Port**, **Login** and **Password**.

To test the connection press **Test connection**.

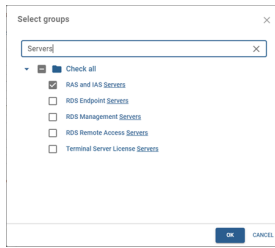
3. **Set the synchronization parameters.**

Enter a LDAP tree search start point in the **Directory** field to indicate the section to execute the data requests in (e.g., a division or organization). Use the **Filter** field to enter conditions to limit the list of persons to be synchronized (e.g., active users or certain roles).

In **When deleting in AD** select what to do when deleting an Access Control person from a LDAP server: **Remove person** or **Block person**.

Press next to **Person ID in AD** and select an attribute to use as a unique person ID for data synchronization.

4. To use server groups set on the LDAP server as access levels, check **Use AD groups as access levels** and select groups.



5. Set the synchronization interval.

Check **Periodic synchronization** and enter the time interval for the synchronization.

- Check **Block AD accounts outside work areas**. As a result, the Active Directory account will be available to the person only within their work area. Otherwise, the account will be blocked on the LDAP server until the person returns to their work area.

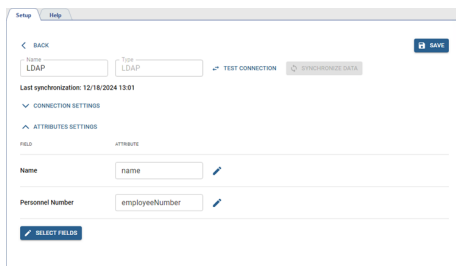


The block will work under the following conditions:

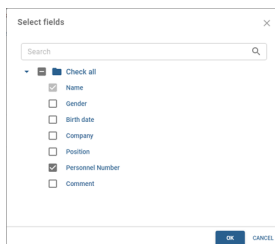
- Work areas are present in the Access Control settings (see [Areas of use](#)).
- An **Active Directory account** and work areas are selected for the person (see [Creating a new person](#)).

The Active Directory account will not be blocked for a person, if it matches the username in the LDAP server connection settings.

7. Select the synchronization attributes.



Press **Select Fields** and select the person attributes to be filled with data from the LDAP server.



To select the LDAP server user attribute to be placed in the field press  and select it from the list.

- Save the connection parameters. Press **Synchronize data** to start the synchronization.



If the synchronization is successful:

- In the [Personnel](#) section, a group named as in the field **Name** will be created with the list of persons downloaded from the server.
- Fields selected to be used as the synchronization attributes will be inaccessible to edit for all downloaded persons.
- In the [Access levels](#) section, the access levels will be created corresponding to the groups in the connection settings.

Person access levels



At least one access level should be created for operation with TRASSIR ACS.

Open the **Plugins -> Access Control -> Access Levels** section to set up access levels.

Access levels can be used to allow people to enter the entire area or only certain rooms. The settings page displays all created access levels and the number of persons to whom they are assigned to.

In order to create a new access level, press **Add** and follow the next steps:

- Enter the access level name and add comment, if necessary.
- Add access points that people with this access level are permitted to use.




The number of simultaneous access point assignments for a person/group/template in different schedules depends on the device functionality.

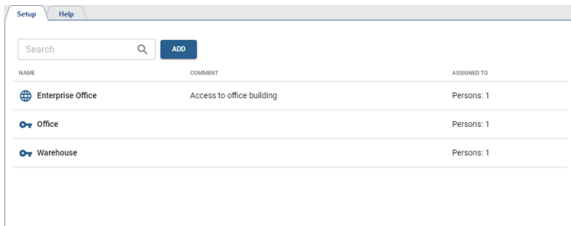
In addition, the number of access levels assigned to *one person* or selected in the *visitor template* should be taken into account. This number also depends on the functionality of the device and the number of identical access points specified in the assigned access levels.




Set the **Allow to open from the mobile client** flag to let the person with this access level use this feature (see ???).

- Add groups of persons or separate persons to whom this access level will be assigned.

- Select the schedule which this access level will use. Section [Access schedule](#) describes the detailed instruction for access schedule creation.

Access levels downloaded from the LDAP server or server with TRASSIR ACS Enterprise are marked with . See [Data Synchronization](#) and TRASSIR ACS Enterprise user manual (see [Access levels](#)).



NAME	COMMENT	ASSIGNED TO
 Enterprise Office	Access to office building	Persons: 1
 Office		Persons: 1
 Warehouse		Persons: 1



In access levels downloaded from LDAP server or TRASSIR ACS Enterprise server, you cannot edit the list of assigned persons. Add or remove the persons on the corresponding server.

Access schedule

This section allows you to create and edit schedules for access levels setting.

Go to the **Plugins -> Access Control -> Access levels -> Access schedule** to open.

In order to create a new schedule, press **Add** and follow the next steps:

- enter the schedule name, which will be displayed in the **access level settings**;
- add comment, if necessary;
- add access levels to which this schedule will be assigned to;
- customize the schedule (the detailed instructions on how to customize the schedule are described below).

After that, you can check the schedule for the week as well as for the month.

Schedule settings

You can use the following schedule types when creating:

- **Calendar week** is a schedule created attached to the specific days of the week.
- **Shifts** is a schedule that specifies a cycle of intervals in which the work schedule depends on the day number in the cycle.

Press **Setup schedule** to open the schedule settings.

Follow the next steps to create the **Calendar week** schedule type:

1. Use the **Working day/Day off** flag to identify working days and days off.
2. Select one of the workdays and use the sliders or the **Beginning** and **End** fields to set up the start and the end time of the access level availability and, if necessary, add one or several breaks.
3. Press the **Duplicate for all work shifts** link to copy the created schedule to all working days of the week.

Follow the next steps to create the **Shifts** schedule type:

1. Set the start date of the first shift and create the desired number of working and weekend shifts.
2. Select one of the work shifts and use the sliders or the **Beginning** and **End** fields to set up the start and the end time of the shift and, if necessary, add one or several breaks.
3. Click **Duplicate for all shifts** to copy the created schedule to other shifts.

In order to create a shift that begins on one day and ends on another, choose the time in the **End** field that is less than or equal to the time in the **Beginning** field.

The breaks define the time interval within which the person will not have access. The schedule may not contain more than 3 work intervals per day or shift.

The **Holidays** tabs lets you add the dates, in which another schedule will be in effect (for example, on pre-holiday and holiday days).

Access schedules downloaded from the TRASSIR ACS Enterprise server are not available for editing and use in the TRASSIR ACS access level configuration. See TRASSIR ACS Enterprise user manual for details (see [Access schedule](#)).

Setup

Help

Search

ADD

NAME	COMMENT	ASS
24/7		No
Enterprise office		Ac
Schedule (office)	Access to office	Ac
Schedule (warehouse)	Access to warehouse	Ac

Access schedule

Name

Enterprise office

Comment

Access levels

Enterprise

Calendar

VIEW SCHEDULE

WEEK

MONTH

Mo 02/17/2025

01 * 02 * 04 * 06 * 08 * 10 * 12 * 14 * 16 * 18 * 20 * 22 * 24

Tu 02/18/2025

03 * 05 * 07 * 09 * 11 * 13 * 15 * 17 * 19 * 21 * 23 * 25

We 02/19/2025

04 * 06 * 08 * 10 * 12 * 14 * 16 * 18 * 20 * 22 * 24

CLOSE

Rules of passage

This section is intended for creating rules that will be used to authenticate persons and allow them to enter protected areas.

In TRASSIR ACS, you can create the Rules of passage of the following types:

- The **Re-entry ban** is the type of the rule that forbids the re-entry through the reader in the selected area, if the person has already authorized on this reader. For example, if the person has passed through the **Entrance reader** in a specified zone, he/she can exit only through the **Exit reader** of the same area. However, the person can freely use other readers that do not belong to this area.
- **Gateway** allows to set a rule for consecutive passage through several access points united in a gateway. To create a rule, indicate the device and the list of access points forming a gateway.
- **Software gateway** is similar to the standard gateway but allows to create routes to pass any access points irrespective of their binding to certain devices.

Go to **Plugins** -> **Access Control** -> **Rules of passage**.



NAME	TYPE	COMMENT
Office re-entry ban	Re-entry ban	
Software gateway	Software gateway	
Warehouse re-entry ban	Re-entry ban	

Re-entry ban



Re-entry ban usage pattern:

- At least **one protected area should be created** to create a rule of passage. The **Entrance readers** and **Exit readers** should be selected in its settings and the **Can be used in rules of passage** flag should be set.
- One or more **Authentication Types** should be selected in the **reader settings**, and/or **Authentication by TRASSIR** should be enabled.
- In order to store information about the current persons' location and to confirm the passage, the access points with readers in the protected area must be permanently connected to TRASSIR ACS the server. If the server is unavailable, the person will not be able to authorize and pass through the reader.


The screenshot shows the 'Re-entry ban' configuration window. On the left, a table lists existing rules: 'Office re-entry ban' (Re-entry ban), 'Software gateway' (Software gateway), and 'Warehouse re-entry ban' (Re-entry ban). The 'Warehouse re-entry ban' rule is selected. The right panel shows the configuration for this rule. It includes a warning message: 'Granting access after checking the rule is performed by the server'. Fields for 'Name' (Warehouse re-entry ban) and 'Comment' are present. The 'Apply rule to' dropdown is set to 'Person', and 'The event being processed' dropdown is set to 'Access granted'. Checkboxes for 'Reset rule at system startup' (checked), 'Skip with recording of rule violation' (unchecked), 'Allow re-entry after' (checked, with a time of 01:00), and 'Prohibit repeated visits to zone for' (unchecked) are shown. An 'Areas' section contains a 'Warehouse' button. 'SAVE' and 'CANCEL' buttons are at the bottom.

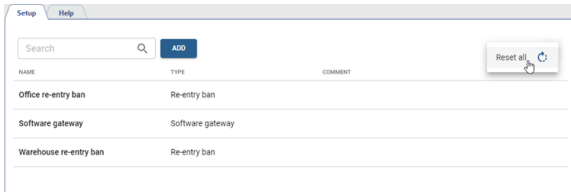
To create a new rule, press **Add**, choose **Re-entry ban** and proceed as follows:

1. Enter the **Name** of the rule and add a **Comment**, if necessary.
2. In the **Apply rule to** field, select the option to which this rule will be applied:
 - **Person** — the rule will be applied to all of the person's identifiers.
 - **Identifier** — the rule will be applied to each of the person's identifiers separately.
For example, if a person has two cards listed as identifiers, and the **Re-entry ban** rule is triggered with one of them during authorization, the employee can use the second card for re-authorization.
This condition is ignored if biometric or personal identifiers are used for authorization: face, fingerprint, or PIN code.
3. Select **The event being processed**, which will trigger this rule:
 - **Access granted** — the rule will be triggered after the person's successful authorization (even if they do not pass through the access point).
 - **Pass** — the rule will only be triggered after the person passes through the access point.
4. If the **Reset rule at system startup** flag is set, then upon launching TRASSIR ACS the current location of the person will be reset. In this case, the person will be able to re-authorize to enter or leave the protected area.
5. Choose one of the options to enable the person's re-entry:
 - Set the **Skip with recording of rule violation** flag. Regardless of the rule settings, the passage will be allowed, but if the rule is violated, the system will capture a re-pass event.

- Set the **Allow re-entry after** flag and select the time period, after which it will be allowed. This option is valid for the readers in the area and allows passing through them again after a specified period of time. If a person leaves the area through the **Exit reader**, the counter will be reset, and it will be possible to re-enter it through the **Entrance reader**.
- Set the **Prohibit repeated visits to zone for** flag and select the time period, within which they will be prohibited. This feature is valid for the entire area and prohibits re-entry even if the person has already exited through the **Exit reader**.

6. Add the **Areas** to which this rule will be implemented.

In order to reset the current location of persons using all the pass rules, click  and select **Reset all**.



Gateway



Gateway rule usage pattern:

- The rule setting is available only on the **TRASSIR TR-C481** controller.
- The rules do not require constant connection to the server to operate, since their settings are stored directly on the device.
- You cannot open several doors of the gateway simultaneously. The gateway uses door sensors: when one of the gateway doors is open, the others will remain locked until all doors of the gateway are locked.
- If a door of the gateway is opened by the *autonomous rule*, it will remain open irrespective of the state of other gateway doors.

NAME	TYPE	CON
Gateway	Gateway	
Office re-entry ban	Re-entry ban	
Software gateway	Software gateway	
Warehouse re-entry ban	Re-entry ban	

Gateway

Name:

Comment:

Access points

Controller:

Office Warehouse

To create a new rule, press **Add**, choose **Gateway** and proceed as follows:

1. Enter the **Name** of the rule and add a **Comment**, if necessary.
2. Select **Controller** and **Access points** to form a gateway.

Software Gateway



Software Gateway rule usage pattern:

- The rule setting is available on several controllers from any manufacturer.
- The rules require constant connection to the server to operate, since their settings are stored directly on the server.
- You cannot open several doors of the gateway simultaneously. The gateway uses door sensors: when one of the gateway doors is open, the others will remain locked until all doors of the gateway are locked.
- If a door of the gateway is opened by the *autonomous rule*, it will remain open irrespective of the state of other gateway doors.
- **Confirmation settings** are ignored for the access point in the Software gateway (see *Access points settings*), and connected card readers ignore the **Rules of passage** (see *Card reader settings*).

The screenshot shows the 'Software gateway' configuration window. On the left, a table lists existing rules: 'Office re-entry ban' (Re-entry ban), 'Software gateway' (Software gateway), and 'Warehouse re-entry ban' (Re-entry ban). The 'Software gateway' rule is selected. On the right, the configuration form includes fields for 'Name' (set to 'Software gateway') and 'Comment'. Below these are 'Access points' selected: 'Office', 'Service/1', 'Service/2', 'Service/3', and 'Warehouse'. The 'Auto open of access point' checkbox is checked. Underneath, two rows of configuration are shown: 'Service/1' with a 0:10 countdown and 'Service/2', and 'Office' with a 0:10 countdown and 'Warehouse'. 'SAVE' and 'CANCEL' buttons are at the bottom.

To create a new rule, press **Add**, choose **Software gateway** and proceed as follows:

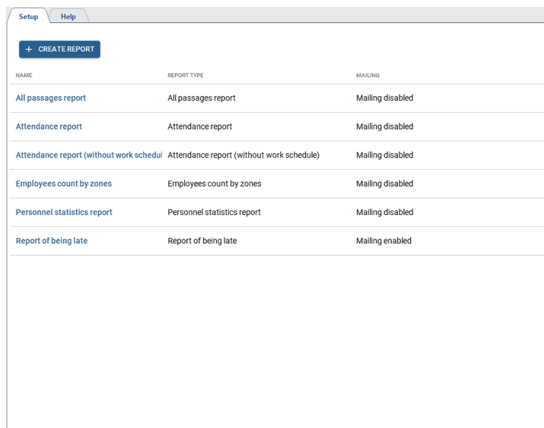
1. Enter the **Name** of the rule and add a **Comment**, if necessary.
2. Select **Access points** to include in the gateway.
3. If you need one door of the gateway to open automatically after the closure of the other door, check **Auto open of access point**, select the relevant access points and countdown time to the opening of the second door:
 - Left field: the first access point that triggers countdown to the opening of the other door upon passage.
 - Right field: the second access point that opens its door automatically after the countdown.
 - Middle field: countdown time from the closure of the first door to the opening of the second door.



If three or more access points are selected in the **Access points** parameter, and the door of one of them is open upon the end of the countdown, the access point in the right field will not open its door and **Access denied** event will occur.

Reports

Go to the **Plugins** -> **Access Control** -> **Reports**.



NAME	REPORT TYPE	MAILING
All passages report	All passages report	Mailing disabled
Attendance report	Attendance report	Mailing disabled
Attendance report (without work schedule)	Attendance report (without work schedule)	Mailing disabled
Employees count by zones	Employees count by zones	Mailing disabled
Personnel statistics report	Personnel statistics report	Mailing disabled
Report of being late	Report of being late	Mailing enabled

Read more about working with the reports in ???.

Notifications

This section lets you create and edit notifications on various events, occurred in TRASSIR ACS. Go to **Plugins->Access Control->Notifications** to open.

Press **Add** to create a new notification and follow the next steps:

1. Enter the name of the notification
2. Select the events to be notified by specifying the **Event Types**, **Persons** and **Objects**:

3. Choose the way of sending notifications:



If the **Email** is selected, then select the account **configured in Automation** in the **Login** field. TRASSIR ACS will use it to send notifications.
If **Telegram** is selected, notifications will be sent to the **@trassirbot** bot.

Specify the time interval, during which TRASSIR ACS will not send the same notifications, in the **Do not resend** field.

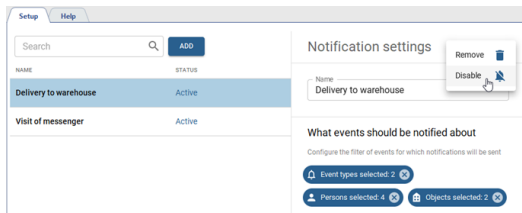
Set the **Add a frame from an associated channel** to add a screenshot from the channel, taken at the moment of the monitored event, to each notification. For more information about adding related channels, see **Devices**.

4. Select the recipients who will receive notifications when the monitored events occur. You can select only one of these options:
 - specify the TRASSIR ACS groups or persons who will be notified when an event occurs;
 - set the **Send a notification to a person from an event** flag, to notify the person with whom the event occurred.



The notifications are sent to the addressees at the contact information specified in the *person's settings*.

You can disable any notification by selecting **Disable** in the notification settings.



Visitor templates

This section allows you to create or edit visitor templates. The **Visitor templates** are the special TRASSIR ACS 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**.

The screenshot shows the 'Template (office)' configuration page. It includes a search bar at the top with an 'ADD' button. The main content area is divided into several sections: 'Pass requests' (Users allowed to create requests: Head office, KRD), 'Pass requests administration' (Users allowed to administrate requests: Head office), 'Pass issue' (Automatic pass issue checkbox, Users allowed to issue passes: Matthew K), 'Available identifiers types' (QR-code 1 d from the moment of issue), 'Template access levels' (Access level 1, Access level 2), and 'Visits' (Limit the number of visits checkbox).

Press **Add** to create a new template for visitors and follow the next steps:

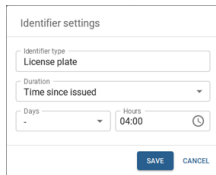
1. Enter the **Name** of a new template.

The screenshot shows a dialog box titled 'Creating a new visitor template'. It has a text input field for 'Name' containing 'Template (office)'. Below the input field are 'SAVE' and 'CANCEL' buttons.

2. Select persons or a group of persons who will have access to the option of creating pass requests.

The screenshot shows a dialog box titled 'Users allowed to create requests'. It has a search bar and a list of users with checkboxes. The list includes 'Check all', 'Office', 'Warehouse', and 'John Rain'. The 'John Rain' checkbox is checked.

3. Choose persons or groups of persons, who will have access to the functions of **Administrator of requests**, if necessary. The administrator of requests will be able to reject the requests created by this template at any time (including even if the pass is issued). For more details, check ???.
4. 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.
5. Select and set up on or several identifier types (**Card**, **QR-code** or **License plate**), that the visitors will use to authenticate.



Identifier settings

Identifier type
License plate

Duration
Time since issued

Days: - Hours: 04:00

SAVE CANCEL

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:

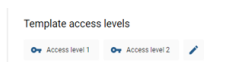
- If **Automatic pass issue** is selected, then the pass time countdown starts from the moment the pass request is created.
- If a list of persons issuing passes is selected, the countdown of the validity time starts from the moment of confirmation and issuing of the pass by this person.

When the pass expires, it is archived. The storage time of passes in the archive is determined by the database settings. All the 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 [???](#).

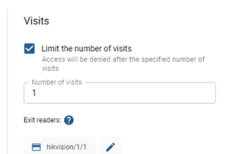
6. Select **Template access levels** that will be provided to a visitor who has received a temporary visitor's pass (see section [Person access levels](#)).



Template access levels

Access level 1 Access level 2

7. To create a template with one-time use or with a limited number of visits, it is necessary to specify the **number of visits** and select the readers through which the visit will be completed. After this number of visits, the pass with the person ID specified in it will automatically become invalid.



Visits

☒ Limit the number of visits
Access will be denied after the specified number of visits

Number of visits
1

Exit readers: 1
1/1/1

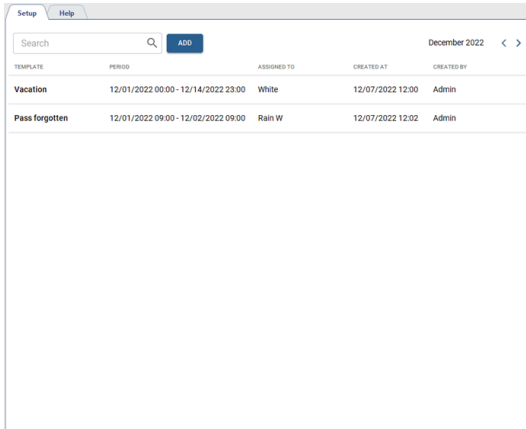


The process of the request creation is described in the "Operator's Guide" (in section [???](#))

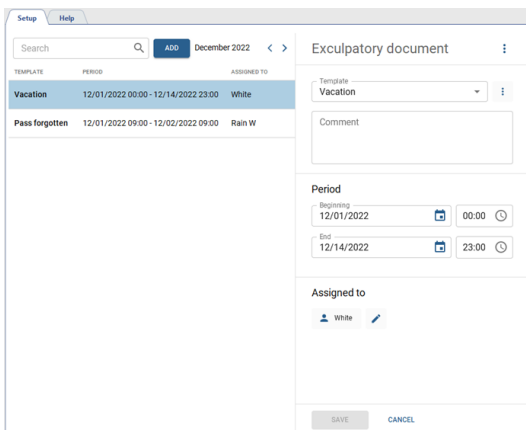
Exculpatory documents

Exculpatory document is the information that supplements the Access Control with certain data on persons' working time, which will be used in the formation of [reports](#). The following documents can be used as exculpatory: holiday request, sick list, business trip, etc. Without a corresponding explanatory document, the Access Control will mark an employee's absence from the workplace as unauthorized.

This section allows you to create and edit documents confirming an employee's absence from work. Go to **Modules** -> **Access Control** -> **Exculpatory Documents**.



Press **Add** to create a new person in Access Control.



Follow the next steps:

1. Select the explanatory document template.

If there is no suitable template, then create one. To do this, click near the **Template** field and select **Add**.

In the opened window, enter the **Name**, **Comment** and select one of the **Accounting types**:

- **Strictly as in exculpatory document** - the entire period of time specified in the exculpatory document is counted as working time, regardless of the actual presence of the person at the workplace.
- **Overlap with work schedule** - only the period of time specified in the explanatory document and coincides with the planned work schedule of the person, is considered as the working time.
- **Work schedule cancellation** - the person's work schedule is cancelled for the entire period of time, specified in the explanatory document.
- **Do not take** - this type of accounting does not count in any way in the calculation of working time. It can be used when it is necessary to leave some additional information in the commentary to the explanatory document.

2. You can add a comment to the explanatory document, if necessary.
3. Specify the period of time, within which the document will be valid.
4. Add a person to whom this exculpatory document will be assigned.

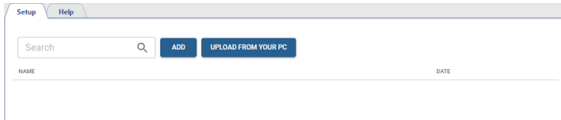
Pass design

The **Card design** is an editor for customization of the employee ID card appearance. With its help, you can customize the appearance of the passes, creating unique layouts and adding information about the employee on them. The pass layout editor allows you to add fields with the employee personal data, his photo, as well as change the background image of the pass.

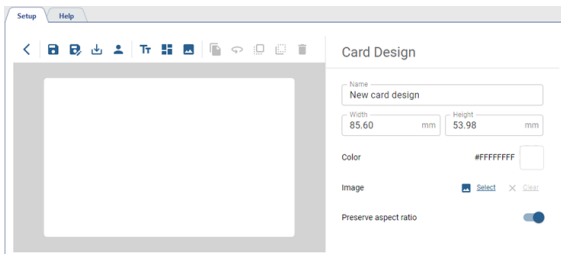


The creation of pass layouts is available with the appropriate license.

In order to create a new layout, open **Plugins -> Access Control -> Card design**.



Press **Add** to open the pass layout editor:



Use the layout settings panel to define the size of the pass, as well as choose its background color or background image. Next, use the editor buttons to add necessary fields to the layout and customize their parameters.

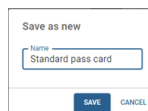
Description of buttons of the pass layout editor.



Save - save the pass layout.



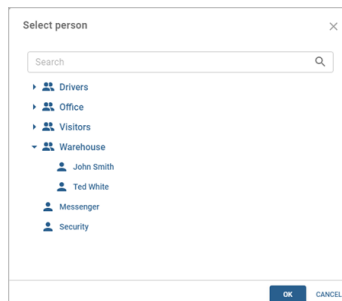
Save layout as new - press this button to save the layout template with a new name.



Download - save the pass layout to a file for later uploading.

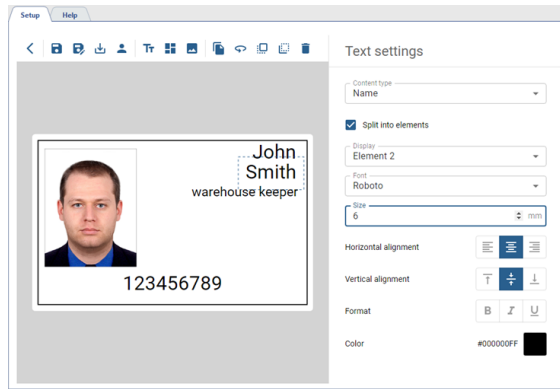


Person for preview - select the person, whose details will be displayed on the created pass card layout.

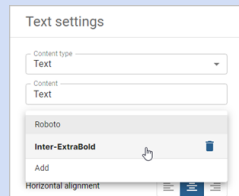


Text - add a text field or a person data field (including **Person extra fields**) to the layout.

Text fields comprising a list of values, e.g., **Name**, **License Plates**, **Pass Cards**, and **Access Levels**, can be placed in various areas of the template with individual format settings. Check **Split into elements** and select the element in the **Display** field to be displayed in the selected area of the template.



You can also add your own font for use in your pass design. This will allow you to create unique layouts and ensure consistency with the style of your company or organization.



You can select any number of TTF (TrueType Font) fonts.



Rect - add a rectangle to the layout.

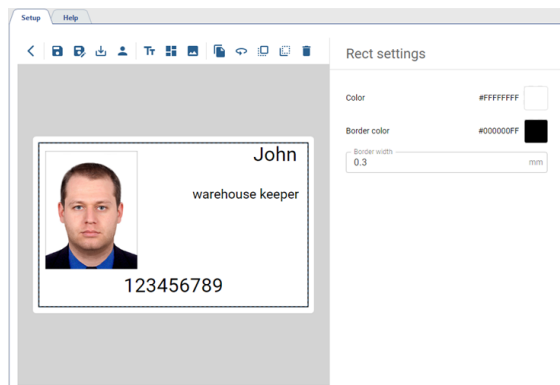
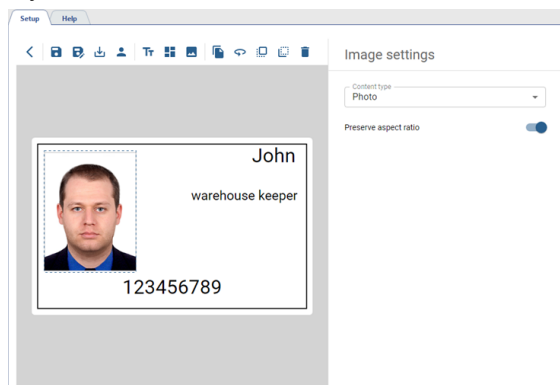


Image - add a field with an image or photo of the person to the layout.



Clone - copy the selected field.



Rotate - rotate the selected field 90 degrees counterclockwise.



Bring to front - move the selected field to the foreground.



Send to back - move the selected field to the background.



Delete - delete selected field.

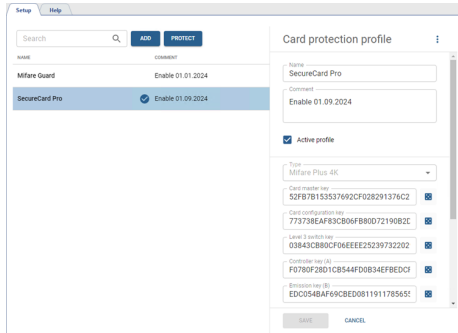


The process of printing a pass card based on the created layout is described in [*Additional actions with persons*](#) and [*???*](#).

Card protection

This section lets you configure card security profiles to provide an additional level of security when issuing employee identification cards. In addition, you can protect cards that have already been issued, keeping them private and secure while in use.

To create a new profile, open **Plugins -> Access Control -> Card protection**.



Press **Add**, enter the profile name, add comment and configure the protection parameters.

- Select **Type**: **Mifare Classic 1K**, **Mifare Plus 1K** or **Mifare Plus 4K**.



When selecting **Mifare Plus 1K** or **Mifare Plus 4K** types, it should be taken into account that this profile will work only with the **TRASSIR TR-R1D**.

- Enter the protection parameters, corresponding to the selected type. To generate a random security key, click



When selecting a value in the **UID size in bytes**, you should into account the data format selected *in the controllers' settings*:

- **3** bytes for **Wiegand 26**;
- **4** bytes for **Wiegand 34**;
- **7** bytes for **Wiegand 58**.

- To enhance the security of card data, you can set the **Reverse byte order** flag and select the **UID type** that will be written to the protected memory block of the card.



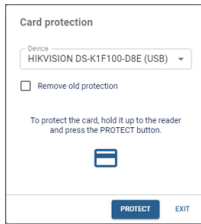
If **Manual input** is selected, the **Use card protection** function will be unavailable when creating or editing a person (see section [Creating a new person](#)).

Also, the value in the **UID size in bytes** field must be considered. An error will occur in the following cases:

- the number entered when creating the secured card exceeds the **UID size in bytes**;
- the data size on the card is less than 7 bytes, if **Card number** and **7** are selected in the **UID type** and **UID size in bytes** settings.

- Set the **Active profile** flag, to activate the current security settings for the operation with the cards and ensure their safe use in the access system.

Press **Protect** to protect already issued cards with an active profile.




Card protection

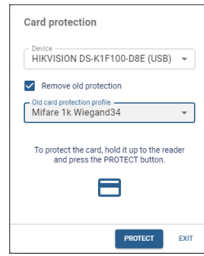
Device
HIKVISION DS-K1F100-D8E (USB) ▼

☐ Remove old protection

To protect the card, hold it up to the reader
and press the PROTECT button.



PROTECT EXIT




Card protection

Device
HIKVISION DS-K1F100-D8E (USB) ▼

☒ Remove old protection

Old card protection profile
Mifare 1k Wiegand34 ▼

To protect the card, hold it up to the reader
and press the PROTECT button.



PROTECT EXIT

In the window that opens, select the **Device** to which the cards will be applied. Then apply the card to the reader and click **Protect**. Repeat the protection procedure for the remaining cards. If you need to disable the previous protection level and enable the new one, set the **Remove old protection** flag and select **Old card protection profile**.

Audit

This section provides a convenient way for the user to review all actions taken in various sections of TRASSIR ACS, including auditing the actions of *operator over access points*, *pass cards layout editor*, and *pass cards printing*.

Go to **Plugins -> Access Control -> Audit** to open.

Time	User	Action
07/09/2024 12:08:55	Admin	View
07/09/2024 12:07:04	Admin	Edit
07/09/2024 12:06:44	Admin	Edit
07/09/2024 12:06:45	Admin	View
07/09/2024 12:06:00	Admin	Edit

Various search criteria such as **Time interval**, **Objects**, **Users**, **Persons**, **Parameters**, and **Action Types** are conveniently provided to help you quickly find the information you need.



Persons search criterion allows to find actions done for deleted persons. To view details, select persons from the **Deleted persons** group.

The information storage period for deleted persons is limited by the parameter **Keep records for** in the database settings (see [Database connection settings](#)).

The **Filter** field lets you refine the search results and find the desired actions. Click on the action to check its parameters, and they will be displayed below the list.

You can save the log as a file. To do this, click **Download XLSX**.

date	time	user	action
John Smith	07.09.2024	Admin	View
Persons	12.08.35		
John Smith	07.09.2024	Admin	Edit
Persons	12.07.04		
John Smith	07.09.2024	Admin	Edit
Persons	12.06.44		
John Smith	07.09.2024	Admin	View
Persons	12.06.42		

action	action date	action user
Work schedule	9-2	

TRASSIR ACS Enterprise

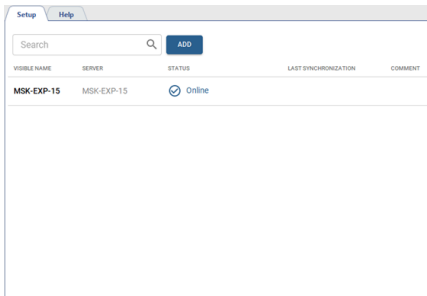
TRASSIR ACS Enterprise is a module that combines several TRASSIR ACS servers into a single access control and management system.

TRASSIR ACS Enterprise setting procedure:

1. *Connect one or more servers with a local TRASSIR ACS version to the server.*
2. Create *working schedules* and *areas*, which will be used to generate various reports.
3. *Create one or several access levels and link them to the corresponding access points.*
4. *Add persons and set up access to various objects for them.*
5. *Create reports.*
6. *Audit user actions* performing the configuration of **TRASSIR ACS Enterprise**, if necessary.

Servers

This section allows you to set up TRASSIR ACS Enterprise connection to the servers where the local versions of TRASSIR ACS are running.



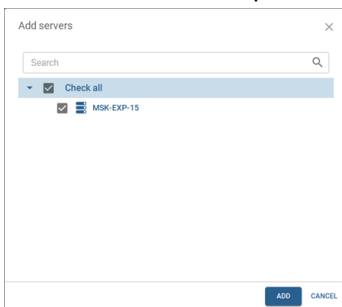
Go to **Plugins** -> **Access Control Enterprise** -> **Servers**.



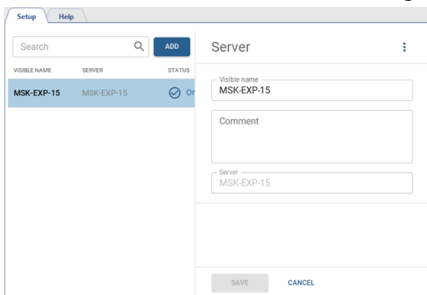
The server with the local version of TRASSIR ACS must be connected to the server with TRASSIR ACS Enterprise before adding.

Read more about server connection in [Connecting to a new server](#).

To add new servers, press **Add** and select the required servers from the list:

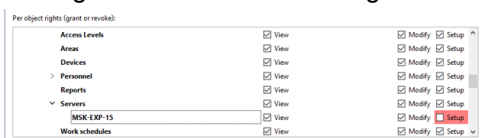


Click on the added server to change its name or add a comment.



You can use the [rights to the individual server objects](#) to set different options to access viewing and editing functions of servers running local versions of TRASSIR ACS.

The rights are located on the rights tree at: **Server name** -> **Plugins** -> **Access Control enterprise** -> **Servers**.



- If the server has the **View** right enabled, the areas and access levels configured on it will be displayed on the **Servers**, **Access Levels**, **Areas** and the **Personnel** tabs.

The servers that have the **View** right disabled will not be displayed on the tabs. However, if, for example, an access level or zone from this server is selected, it will be displayed along with the selected item, but the full list of items will not be available for viewing.

- The server with **View** and **Modify** rights enabled will appear on the **Servers**, **Access Levels**, **Areas** and **Personnel** tabs, but their parameter editing will not be available.

- The server with the **Setup** right enabled is available for editing and assigning access levels and areas configured on it to the persons.

Personnel

This section allows you to create and edit TRASSIR ACS Enterprise persons.

Go to **Plugins -> Access Control Enterprise -> Personnel**.

The screenshot shows the 'Personnel' management interface. On the left, a sidebar under 'Management' lists 'AI G' and 'Mike M'. The main panel displays details for 'AI G', including a profile picture, gender (Other), birth date (01/01/1990), group (Management), company (Personnel Number: A123434566), and work schedule (5-2). Below this, there are sections for 'Identifiers' (A4864AA, 987711), 'Access levels' (Server: MSK-EXP-15, Office), 'Work areas' (Server: MSK-EXP-15, Office), and 'Contacts for notifications' (boss@mycompany.com).


A detailed description of the process for working with the **Personnel** section is outlined in the following sections:

- *Creating a group*
- *Creating a new person*
- *Changing the person's data and blocking the person*

Creating a group

To create a new group, go to **Plugins** -> **Access Control Enterprise** -> **Personnel**, press **Add** and select **Group**.

After that:

- Enter the **Group name** and select its **Location** in the persons' tree.
Click  next to the **Location** field, to save the current group location to the clipboard. It can be used when **creating a file** to import new persons to this group.
- Set the **Assign general parameters** flag to let the group parameters be inherited by all the persons added to this group.
Set the parameter values that will be automatically assigned to all persons in that group.
All assigned parameters will become unavailable for the person in the group after the saving. In order to keep the editing options, set the **Allow to change person's settings** flag.

You can use the rights to the **individual server objects** to set different options to access the viewing and editing functions of the person groups themselves, as well as the persons in the groups.

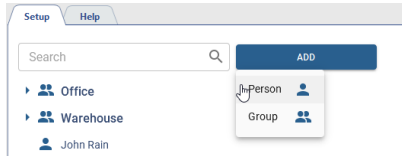
The rights are located on the rights tree at: **Server name** -> **Plugins** -> **Access Control Enterprise** -> **Personnel**.

Object	View	Modify	Setup
Devices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Personnel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Managers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Reports	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Servers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MSK-EXP-15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- If a person group has the **View** right, it will be displayed in the **Personnel**, **Work Schedules** and **Access Levels** tabs, but the Person and the Group settings editing function will not be available.
The groups of persons that have the **View** right disabled on the tabs will not be displayed. However, they will be displayed if their subgroups have the **View** right disabled.
- The person group with the **Modify** right enabled can not create new groups, but can create new persons in the existing groups and modify the existing group parameters.
- The person groups with the **Setup** right enabled can create and edit the person groups, as well as persons in these groups.


Creating a new person

In order to create a new Access Control Enterprise person, go to **Plugins** -> **Access Control Enterprise** -> **Personnel**, press **Add** and select **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.

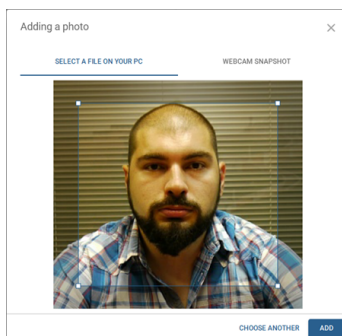
Click  next to the **Group** field, to save the current person's location to the clipboard. It can be used when [creating a file](#) to import new persons into the same group.

Set the **Period of access rights** for this person in order to set limit to use identifiers and access levels.

2. Upload an employee's photo by pressing **Add photo**.

In the opened window, select one of the ways: **Select a file on PC** or **Webcam snapshot** and add an employee photo.

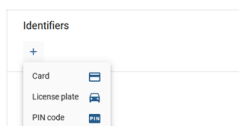
When uploading a photo from your PC or creating a photo using webcam, you can use the crop feature to resize the added photo.

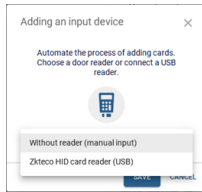


3. in order to manage an employee's working hours, select **Work schedule**.

Use various settings to create any work schedule (read more in [Work schedules](#)).

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 the client/server;
- by entering the card data into the input field manually.



Features of data entry from identification cards:

- Data input from an ID card using a USB reader is only supported in **Windows version**.
- ZKTeco USB readers store data in **Wiegand 34** format. If the readers used by personnel for authentication use **Wiegand 26** format, set the **Convert to Wiegand 26** flag when adding the card.



License plate - enter the vehicle license plate number that will be used for **AutoTRASSIR** module authentication.



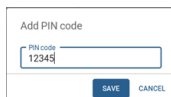
When entering the number, you can use letters of Latin alphabet, as well as "mask", in which unknown characters are replaced by "*" or "?".

The "?" symbol is used to indicate only one unknown character, and the "*" symbol - one or more unknown characters. For example, if the license plate number is known, but the region is unknown, you can use the following types of masks:

b663kt?? - for numbers with two-digit region only: **b663kt77** or **b663kt95**.

b663kt??? - for numbers with a three-digit region only: **b663kt777** or **b663kt190**.

b663kt* - for numbers with both two- or three-digit regions: **b663kt77** or **b663kt190**.

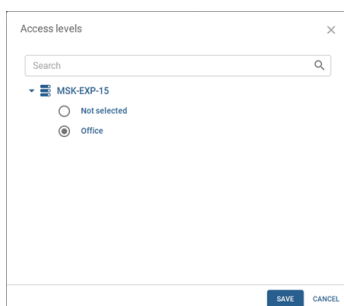


PIN-code - enter the pin code that will be entered by the employee on the controller panel.

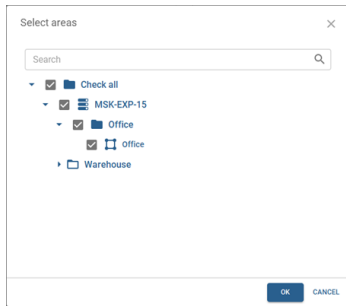


All identifiers will be used for Access Control authentication, depending on the **Authentication mode** selected in the **reader's settings**.


5. Assign the corresponding **Access levels** to the person. For each server added, only one level of access can be assigned.



6. Select **Areas** that can be accessed by this person.

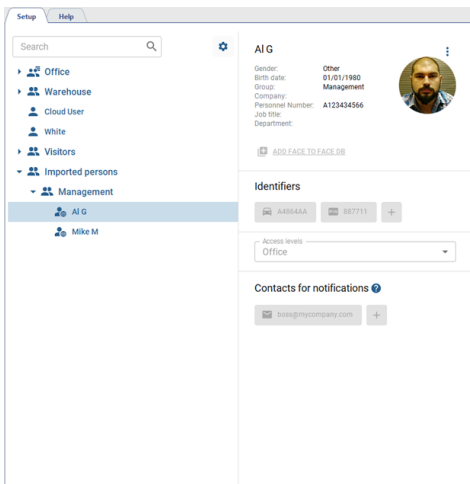


7. Add contact information to receive notifications about TRASSIR ACS events (see [Notifications](#)).

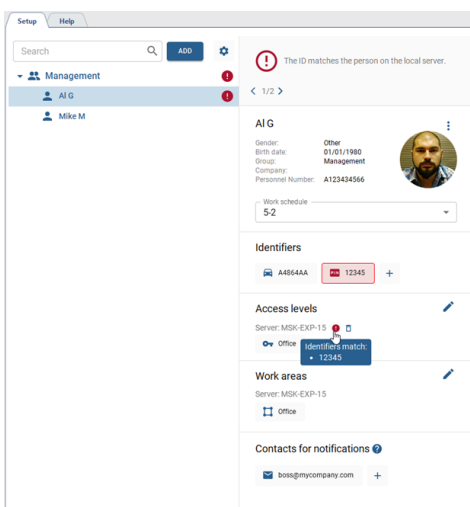


Enter your ID from telegram bot **@trassirbot** as your **Telegram ID**. In order to find out your ID, open the bot and run the **/start** command.


After the synchronization, the persons added to TRASSIR ACS Enterprise, will appear in the corresponding local versions of TRASSIR ACS, in the **Imported persons** group, depending on the access level selected in the person.

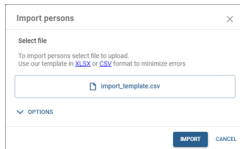


If the data synchronization process finds a match of the TRASSIR ACS person number or identifiers of the TRASSIR ACS Enterprise and the person on the local TRASSIR ACS version, you will see the corresponding error message.



Import of persons

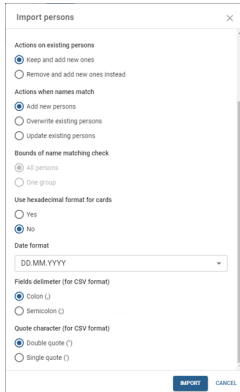
In case you need to add a large number of personnel, there is an import function. To activate it, click  and select **Import persons** feature.



Select a file with a list of persons.



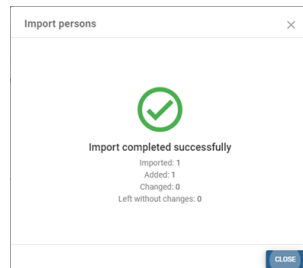
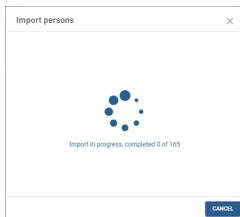
Use a ready-made template to simplify the process of creating a persons list.



Configure the necessary import parameters:

- **Actions on existing persons** - select one of the options the system should perform when existing persons are detected during the import process.
- **Actions when names match** - specify what will occur if matching names are found during the import process.
- **Bounds of name matching check** - customize name matching check. When the **All persons** option is selected, the system will respond to name matches in the entire list of persons. If **One group** is selected, the check will be limited to name matches within the groups specified in the file.
- **Use hexadecimal format for cards** - enable or disable the use of hexadecimal card format when importing data.
- **Fields delimiter** - specify the symbol to be used as a separator between data fields during import.
- **Quote character** - specify which character is used as the opening and closing character of the quotation marks.
- **Date format** - select the format in which the dates in the imported data are displayed.

Click **Import** to load the data.




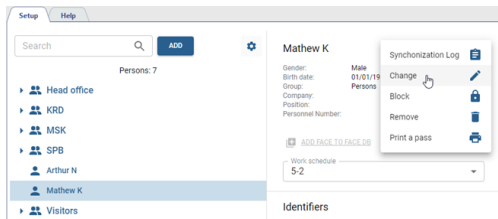
All added persons will be displayed after updating the **Personnel** section.

Changing the person's data and blocking the person

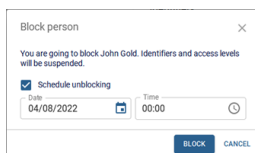
You can use the filter that searches for the person not only by name, but also by account number, access card or license plate.



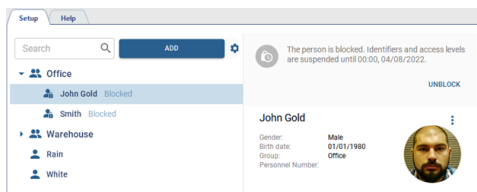
In order to change data in a created person, select the person and click  near the photo and select **Change**.




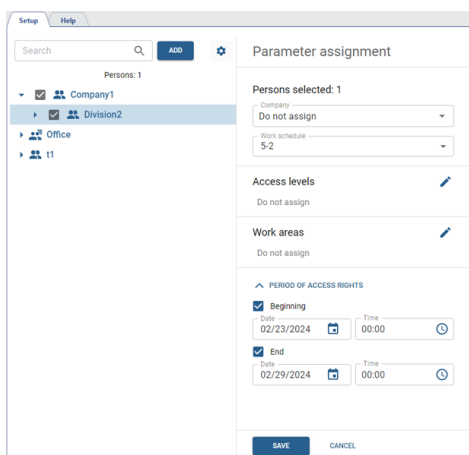
In order to block a person, select the corresponding menu item and specify the date when the person is automatically unlocked in the opened window, if necessary.



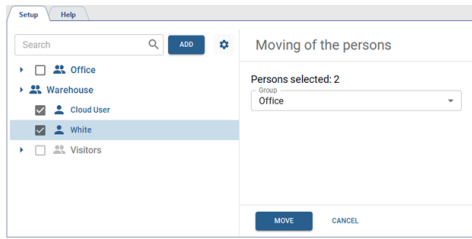
The blocked person will be marked with a corresponding icon and caption. You can unblock it any time by pressing **Unblock**.



In order to enter the person settings mass change mode, press  and select **Mass parameter assignment**. After that, select the persons and other parameters to be assigned to these persons.



The **Moving of the persons** features works the same way. Instead of parameters, you need to select the group to which the selected persons will be moved.



Access levels

You can configure access levels in **Plugins -> Access Control Enterprise -> Access levels** section.

Access levels can be used to allow people to enter the entire area or only certain rooms. The settings page displays all the created access levels.

In order to create a new access level, press **Add** and follow the next steps:

- Enter the access level name and add comment, if necessary.
- Add access points that people with this access level are permitted to use.

- Add groups of persons or separate persons to whom this access level will be assigned.

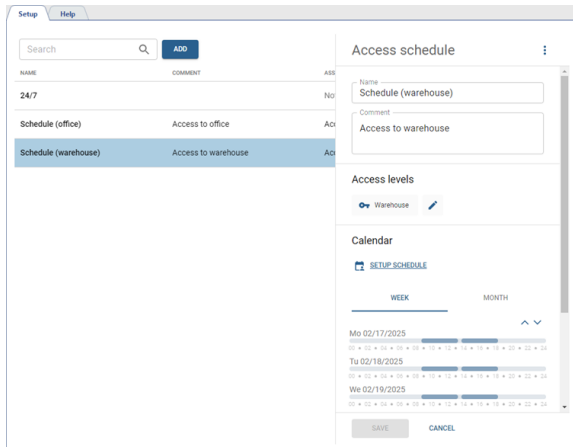
- Select the schedule which this access level will use. Section [Access schedule](#) describes the access schedule creation in detail.

After the synchronization, the access levels added to TRASSIR ACS Enterprise will appear on the corresponding TRASSIR ACS servers.

NAME	COMMENT	ASSIGNED TO
Enterprise Office	Access to office building	Persons: 1
Office		Persons: 1
Warehouse		Persons: 1

Access schedule

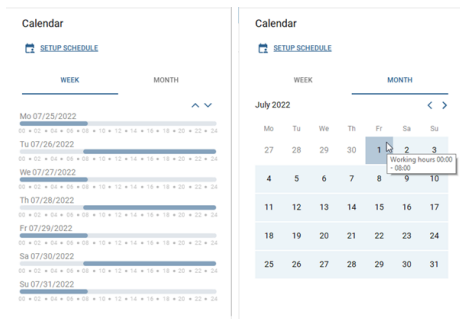
This section allows you to create and edit schedules for access levels setting.
Go to **Plugins -> Access Control -> Access levels -> Access schedules**.



To create a new schedule, press **Add** and follow the next steps:

- enter the schedule name, which will be displayed in the *access level settings*;
- add comment, if necessary;
- add access levels to which this schedule will be assigned to;
- customize the schedule (the schedule customization is described in detail below).

After that, you can check the schedule for a week as well as for a month.



Schedule settings

You can create the following types of schedule:

- **Calendar week** is a schedule for the specific days of the week.
- **Shifts** is a schedule that specifies a cycle of intervals in which the work schedule depends on the day number in the cycle.

Press **Setup schedule** to open the schedule settings.

Follow the next steps to create a **Calendar week** schedule:

1. Use the **Working day/Day off** toggle switch to identify working days and days off.
2. Select one of the workdays and use the sliders or the **Beginning** and **End** fields to set up the start and the end time of the access level availability and, if necessary, add one or several breaks.
3. Press the **Duplicate to all work shifts** link to copy the created schedule to all working days of the week.

Follow the next steps to create a **Shifts** schedule:

1. Set the start date of the first shift and create the desired number of working and weekend shifts.
2. Select one of the work shifts and use the sliders or the **Beginning** and **End** fields to set up the start and the end time of the shift and, if necessary, add one or several breaks.
3. Click **Duplicate to all shifts** to copy the created schedule to other shifts.



In order to create a shift that begins on one day and ends on another, choose the time in the **End** field that is less than or equal to the time in the **Beginning** field.



The breaks define the time interval within which the person will not have access. The schedule may not contain more than 3 work intervals per day or shift.

The **Holidays** tab lets you add the dates, in which another schedule will be in effect (for example, on pre-holiday and holiday days).

After the synchronization, the access levels added to TRASSIR ACS Enterprise will appear on the corresponding TRASSIR ACS servers.

Setup

Help

Search

ADD

NAME	COMMENT	ASS
24/7		No
Enterprise office		Ac
Schedule (office)	Access to office	Ac
Schedule (warehouse)	Access to warehouse	Ac

Access schedule

Name

Enterprise office

Comment

Access levels

Enterprise

Calendar

VIEW SCHEDULE

WEEK

MONTH

Mo 02/17/2025

01 * 02 * 04 * 06 * 08 * 10 * 12 * 14 * 16 * 18 * 20 * 22 * 24

Tu 02/18/2025

03 * 05 * 07 * 09 * 11 * 13 * 15 * 17 * 19 * 21 * 23 * 25

We 02/19/2025

04 * 06 * 08 * 10 * 12 * 14 * 16 * 18 * 20 * 22 * 24

CLOSE

Work schedules

This section allows you to create and edit work schedules that are used to determine the working time of an employee when building [various reports](#).

Go to **Plugins-> Access Control Enterprise -> Work Schedules**.

In order to create a new work schedule, press **Add** and follow the next steps:

- enter the working schedule name that will be displayed in the [person's settings](#);
- add comment, if necessary;
- add groups of persons or individual person to whom this work schedule will be assigned;
- customize the schedule (the detailed instructions on how to customize the schedule are described below).

After creating a work schedule, you can check its timing for the week as well as for the month.

Schedule settings

You can use the following schedule types when creating:

- **Calendar week** is a schedule that lets you create a working schedule with reference to the specific days of the week.
- **Shifts** is a schedule that specifies a cycle of intervals in which the work schedule depends on the day number in the cycle.

Press **Setup schedule** to open the schedule settings.

Follow the next steps to create the **Calendar week** schedule type:

1. Use the **Working day/Day off** flag to identify working days and days off.
2. Select one of the workdays, and use the sliders or the **Beginning** and **End** fields to set up the start and the end time of the workday and, if necessary, add one or several breaks.
3. Press the **Duplicate for all work shifts** link to copy the created schedule to all working days of the week.

Follow the next steps to create the **Shifts** schedule type:

1. Set the start date of the first shift and create the desired number of working and weekend shifts.
2. Select one of the work shifts, and use the sliders or the **Beginning** and **End** fields to set up the start and the end time of the shift and, if necessary, add one or several breaks.
3. Click **Duplicate for all shifts** to copy the created schedule to other shifts.



The breaks define only the interval of time during which a person can be absent from the workplace for the entire working day. The strict time limits for the beginning and end of breaks are not taken into account in Access Control.



In order to create a shift that begins on one day and ends on another, choose the time in the **End** field that is less than or equal to the time in the **Beginning** field.

5-2

The **Holidays** tabs lets you add the dates, in which another schedule will be in effect (for example, on pre-holiday and holiday days).

The **Variations** tab provides parameters that can be used for more flexible customization of the employees' working schedules.

- The **Delays and early leaves** parameter defines the maximum time intervals that will be used to calculate lateness or early departures. If an employee comes in late or leaves early, the difference between the actual time and the scheduled time will be reported as **Delays** or **Early leaves**.
- The **Consider overtime** parameter sets the minimum time that will be used to calculate overtime. If an employee comes in earlier or leaves later than the set time period, the time worked by the employee will be reported as **Overtime**.
- The **Allow work on weekends** parameter sets the minimum time that will be used to calculate overtime when working on weekends. If an employee works on weekend for more than the specified time, the actual time worked will be reflected in the report as **Overtime**.
- The **Work area leaving** parameter sets the minimum time for which an employee can leave his workplace. If an employee will be absent more than the specified time, this time of absence will be indicated as **Absenteeism** in the reports.

Areas of use

This section allows you to create and edit areas that can be used to track the movement of persons within the protected perimeter and to use them to build [various reports](#).

You can configure the areas of use in **Plugins** -> **Access Control Enterprise** -> **Areas**.

To create an area, press **Add**, select the **Area** item, specify the required parameters and select the readers that will identify persons entering and leaving the area.



Only one server's readers can be used as entrance and exit readers. You can't select the readers from different servers in the area settings.

You can not use the same reader as an entrance (exit) reader in the settings of two different areas. At the same time, the same reader can be an entrance reader in one area and an exit reader in another.

If you delete a device on the TRASSIR ACS server, the areas, where that device readers were used, will be marked with an error message, and the **Removed** will be displayed instead of the deleted readers.

For ease of use, all areas can be grouped into folders. In order to create a folder, press **Add**, select **Folder** and specify the required parameters.

Reports

Go to **Plugins** -> **Access Control Enterprise** -> **Reports**.

Setup Help		
+ CREATE REPORT		
NAME	REPORT TYPE	MAILING
All passages report	All passages report	Mailing disabled
Attendance report	Attendance report	Mailing disabled
Attendance report (without work schedule)	Attendance report (without work schedule)	Mailing disabled
Employees count by zones	Employees count by zones	Mailing disabled
Personnel statistics report	Personnel statistics report	Mailing disabled
Report of being late	Report of being late	Mailing enabled

TRASSIR ACS lets you create the following report types:

- **All passages report** - a report on all persons passages for a specified period of time.

All passages report						
All passages report (11/09/2021 00:00 - 11/30/2021 00:00)						
Name	Personnel number	Group	Date	Time	Access point	Direction
John Rain	1		2021.11.30	16:54:13	Office 3	Exit
White	1234567890			16:55:08	Office 2	Exit
				16:55:16	Office 2	Entrance
				16:55:24	Office 2	Exit
				16:55:44	Office 2	Entrance
				16:55:51	Office 3	Exit
				16:56:03	Office 1	Unspecified
				16:56:19	Office 1	Exit
				16:56:25	Office 3	Exit
				16:56:54	Office 2	Entrance

- **Employees count by zones** - report on the location of people in zones, depending on the time of day.

Employees count by zones				
Employees count by zones (09/01/2022 - 09/01/2022)				
Date	Time	Count	Company	
09/01/2022	00:00 - 08:00	0	Ela	
09/01/2022	00:00 - 08:00	0	helpforce	
09/01/2022	08:00 - 16:00	1	Ela	
09/01/2022	08:00 - 16:00	1	helpforce	
09/01/2022	16:00 - 00:00	0	Ela	
09/01/2022	16:00 - 00:00	1	helpforce	

- **Report of being late** - a report on employees arriving later than the arrival time, specified in the work schedule.

Report of being late							
Report of being late (12/01/2021 - 12/01/2021)							
Report was generated at 01.12.2021 16:41							
Name	Personnel number	Group	Date	Arrival - Plan	Arrival - Fact	Being late	
Cloud User	123		01.12.2021	09:00	12:19	03:19	
John Rain	1		01.12.2021	10:00	-	Truancy	
White	1234567890		01.12.2021	08:00	12:19	04:19	

- **Personnel** - a summarized report on all employees.

Personnel										
Personnel 02/26/2024 14:07:44										
Name	Group	Birth date	Created at	Personnel Number	Card	License plate	Other identifiers	Access levels	Work schedule	Blocked
James Smith	Company1/Division2/Office3	05/12/1989	02/22/2024 14:28:52	12345	12345678, 87654321	A123BC777				

- **Personnel statistics report** - a summary report on the person's time at the workplace.

- Set the **Display timezone** flag to display the time zone column, ensuring that the time of events is presented correctly depending on the time zone. This setting will be useful when working with different regions when the devices are configured with different time zones.
- When building **Personnel** report, you can select specific columns that contain employees key information, such as their names, identifiers, access levels, work schedules and other required parameters.
You can also set **Hide blocked persons** flag to exclude them from the report.
- The **Time spent at the workplace** report filter parameters are customized depending on the **Show all stay intervals** checkbox:

If **Show all stay intervals** is checked, the report will show all intervals (entries and exits by reader) for the selected **Time interval**.

You can choose the length of the tolerance intervals, within which the system will search for events (employee entries and exits) regarding the selected Time interval in the **Tolerance interval for events search** field.



If only one event (i.e. entry or exit) within the **Time interval** is found, considering the **Tolerance interval for events search**, it will be displayed as a blank line in the report.

If **Show all stay intervals** is unchecked, the report will show all intervals (entries and exits by reader) for the selected **Work shift**.

Apart from that, the values **Plan**, **Delays** and **Early Leaves** will become available to check or uncheck in **Advanced Options** to show or hide them in the report.

You can choose the length of the time intervals, within which the system will search for events (employee entries and exits) regarding the selected shift in the **Tolerance interval for events search** field.

The value set in the **Minimum hours worked** parameter will allow you to exclude the employees who have worked less than the set minimum time, from the report.



If only one event (i.e. entry or exit) within the **Work shift** is found, considering the **Tolerance interval for events search**, it will be displayed as a blank line in the report.

- In order to display the direction of the passage (entrance or exit), you should select its location in the **reader settings**.



A report with a large amount of data will show only the first 300 lines. Click **Download XLSX** to download the full report with all the data.

If **Export XLSX file horizontally** is checked in **Advanced Options** for **Attendance report** and **Time spent at the workplace** report, the dates in the exported report will be listed in a row and information for them in columns.



All server users can view created reports.

Only those users who have the **Plugins** -> **Access Control Enterprise** -> **Reports** -> **Settings** flag enabled in their rights settings, will have access to create, edit and delete reports.

Read more about user rights settings in the "Administrator's Guide" (**Determining access rights**).

You can set up automatic sending of reports by e-mail. To do this, set the **Automatically mailing a report** flag in the **Mailing parameters** list.



The **Automatically mailing a report** if the **Other** value is set in the **Report period** field.

Specify the mailing addresses in the **Addresses** field. Select the preconfigured email account in the **Mail account** field (see [Adding an email account](#)).

Select the mailing frequency in the **Periodicity** field:

- **Day** - set the start date and also how often in how many days and at what time the report and mailing will be generated.

- **Week** - specify the days of the week, when the report will be generated and sent out.

- **Month** - specify, separated by commas, on which days of the month the report will be generated and sent out.

Audit

This section provides a convenient way to review all actions taken in the various sections of TRASSIR ACS Enterprise. Go to **Plugins -> Access Control Enterprise -> Audit** to open.

OBJECT	TIME	USER	ACTION
John Smith Persons	07/09/2024 12:08:35	Admin	View
John Smith Persons	07/09/2024 12:07:04	Admin	Edit
John Smith Persons	07/09/2024 12:06:44	Admin	Edit
John Smith Persons	07/09/2024 12:06:42	Admin	View
John Smith Persons	07/09/2024 12:06:09	Admin	Edit

Various search criteria such as **Time interval**, **Objects**, **Users**, **Persons**, **Parameters**, and **Action Types** are conveniently provided to help you quickly find the information you need.

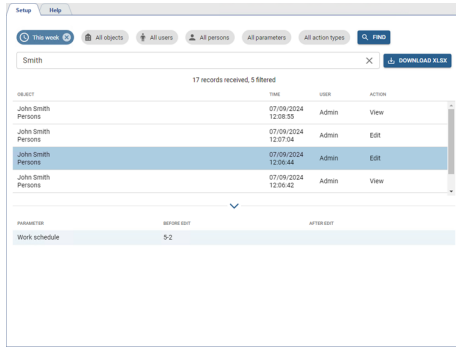


Persons search criterion allows to find actions done for deleted persons. To view details, select persons from the **Deleted persons** group.

The information storage period for deleted persons is limited by the parameter **Keep records for** in the database settings (see [Database connection settings](#)).

The **Filter** field lets you refine the search results and find the desired actions. Click on the action to check its parameters, and they will be displayed below the list.

You can save the log as a file. To do this, click **Download XLSX**.



The screenshot shows a web application interface for log management. At the top, there are tabs for 'This week', 'All objects', 'All users', 'All persons', 'All parameters', and 'All action types'. A search bar contains the text 'Smith'. To the right of the search bar is a 'Download XLSX' button. Below the search bar, a message states '17 records received, 5 filtered'. A table displays log entries with columns for 'OBJECT', 'TIME', 'USER', and 'ACTION'. The table contains five rows of data. Below the table, there is a section for 'PARAMETER' with a table showing 'Work schedule' and '5-2'.

OBJECT	TIME	USER	ACTION
John Smith Persons	07/09/2024 12:05:35	Admin	View
John Smith Persons	07/09/2024 12:07:04	Admin	Edit
John Smith Persons	07/09/2024 12:06:44	Admin	Edit
John Smith Persons	07/09/2024 12:06:42	Admin	View

PARAMETER	BEFORE EDIT	AFTER EDIT
Work schedule	5-2	

Access monitoring control and security and fire alarm systems

TRASSIR allows you to arrange the integrated security system in which the video surveillance system interacts with access control systems and security and fire alarm systems. The server and the connected system can interact both on the same server and on different servers connected via the local network.

The 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.
- **FireSec** by Rubezh.
- **Biostar 2** by Suprema.
- **Hikvision** from Hikvision Digital Technology Co.,Ltd.
- **Sigur(Sphinx)** of PromAvtomatika company.

List of features used for work depends on the connected system:

Feature	Orion Pro	Hikvision	FortNet	Gate	Sigur	Itrium	NeoGuard	Schrack	Spica	Paradox	Stemax	MaxLogic	FireSec	Biostar 2
Automatically load the tree of objects corresponding to the devices in the system.	+	+	+	+	+	+	+		+	+	+	+	+	+
Link system devices	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Feature	Orion Pro	Hikvision	FortNet	Gate	Sigur	Itrium	NeoGuard	Schrack	Spica	Paradox	Stema	MaxLog	FireSec	Biostar 2
to channels.														
Locate system devices on maps.	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Arrange the system devices status monitoring with the object tree .	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Accept system events from systems devices and conduct search by them.	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Set up server response using rules and scripts for acquired events.	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Manage system objects or change system objects status using server commands.	+	+			+				+	+				

Feature	Hikvision	Sigur
Automatically load the tree of objects corresponding to the devices in the system.	+	+
Link system devices to channels.	+	+

Feature	Hikvision	Sigur
Locate system devices on maps.	+	+
Arrange the system devices status monitoring with the <i>object tree</i> .	+	+
<i>Accept system events</i> from systems devices and conduct search by them.	+	+
Set up server response using <i>rules and scripts</i> for acquired events.	+	+
Manage system objects or change system objects status using server commands.	+	+



- *Server settings for operation with Orion Pro Access Control System*
- *Connection of server to operate with "Hikvision" ACS control panels*
- *Typical server settings for operation with Access Control or FAC*
- *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 the server settings for operation with Schrack security and fire alarm system*
- *Specific features of server settings for operation with Spica access monitoring and control system server*
- *Features of server settings for operation with Paradox access monitoring and control system panels*
- *Stemax system server settings features*
- *Server settings features for operation with "MaxLogic" panels*
- *Server settings for operation with "Rubezh (FireSec)" fire alarm system*
- *Configuration of Suprema (Biostar 2) Access Control*
- *Connection of server to operate with "Hikvision" ACS control panels*
- *Typical server settings for operation with Access Control or FAC*
- *Sigur(Sphinx) ACS server settings features*

Server settings for operation with Orion Pro Access Control System



Orion Pro Integration Module should be installed and configured for correct server operation with Orion Pro Access Control. You can find instructions on the module configuration on the Bolid official website. The server works with the following versions of Orion Pro software and higher:

- **Orion Core 1.20 (release 3, build 5788)**
- **Orion Pro 1.3 Integration Module (release 0, build 1849)**

If you are using earlier versions, upgrade the Orion Pro software.

In the **Settings window**, the settings for connecting to an Orion server are specified on the **Modules -> Orion** tab.

- **Protocol** - protocol of connection to the "Orion Pro" access control system server.



When selecting a protocol, you should select the **SOAP** as it is the most current protocol to work with. It is strongly recommended that new video surveillance and access control projects avoid using the **XML-RPC** protocol for data exchange. This protocol is obsolete, its support has ended, and it is retained solely for compatibility with current integrations.



- **Address** - IP address or DNS name of a server with **Orion Pro integration module**.
- **Port** - the number of port, selected in **Orion Pro Integration module**.
- **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** - the IP address or DNS name of the current 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".
- **User token** and **Password token** - username and password to connect to the Orion Pro Access Control database.

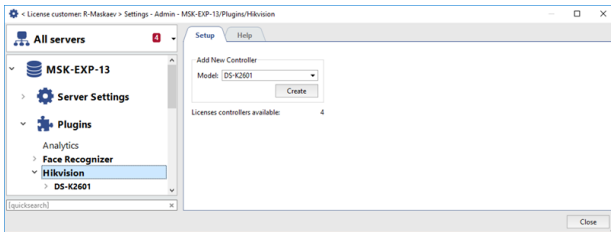
The **Status** field indicates the connection state. If all the parameters are set properly, an **Orion connected** entry is displayed and the new ACS "Orion Pro" objects appear in the object tree.

- >  **Server Settings**
- ▼  **Plugins**
 - Analytics
 - Access Control
 - ActiveDome
 - > **ActivePOS**
 - AutoTrassir
 - > **Face Recognizer**
 - Neuro Detector
 - ▼ **Orion**
 - > **C2000-2 (127)**
 - SipPhone

System objects settings is described in the *[AMCS or security and fire alarm system objects settings tree](#)*.

Connection of server to operate with "Hikvision" ACS control panels

Select the panel model, to which the server will be connected, in the **Settings window**, on the **Plugins -> Hikvision** tab.



The maximal amount of the panels that can be connected to the server is defined by the license and displayed in the **Available licenses** field.

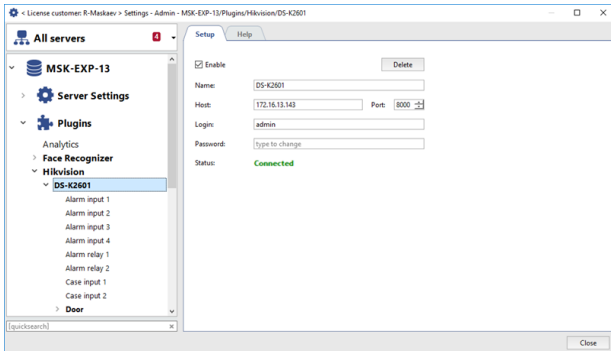
Select the connected controller model and press **Create**. The created controller will appear in the server settings tree. After that, you should set up the **server connection to the panel**.



- *Connection of server to the "Hikvision" ACS control panel*
- *AMCS or security and fire alarm system objects settings tree*

Connection of server to the "Hikvision" ACS control panel

In order for the server 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 the object tree.

Read more about control panel object settings in the *AMCS or security and fire alarm system objects settings tree*.

Server settings for operation with "Rubezh (FireSec)" fire alarm system



TRASSIR supports FireSec software version 3.2.3.0 and higher and R3-based Rubezh fire alarm devices.

Before setting up the connection between the "Rubezh (Firesec)" fire alarm system, perform the following actions:

1. Install the FireSec software.
2. Configure Firesec software operation with the devices, the information on which will be displayed on server.
3. Perform additional FireSec software settings: add zones, configure scripts, etc.
4. Use "FireSec Operational Task" utility, which is included in FireSec software distribution kit, to check the devices' functionality.
5. Run and configure "FireSec Integration Service".
Activate data transfer via HTTP.
Add a client. In the client settings, specify the TRASSIR server port through which the FireSec software will connect (default port value: **8096**).
Enter the IP address and port through which the TRASSIR server will connect to the FireSec software (default port value: **8097**).

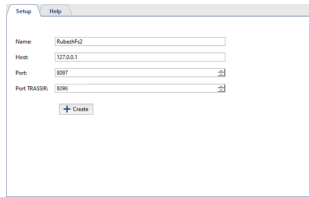


For detailed information on the "Rubezh (FireSec)" fire alarm system, please refer to the corresponding guidelines that can be downloaded from the FireSec software manufacturer's website.

In [Adding Rubezh Firesec module](#) and [FireSec software module settings](#) you can find the detailed information on the following steps to connect the server to the FireSec software and configuring its operation.

Adding Rubezh Firesec module

In order to add Rubezh (FireSec) integration modules, press **Add** in the **Settings window** on the **Plugins -> Rubezh FireSec** tab.



After that, specify the following parameters:

- **Name** - the name of the module, which will be displayed in the settings tree.
- **Host** - the system module IP address or DNS-name.
- **Port** - the module port, through which the server will connect to the system module.
- **Port TRASSIR** - the server port, through which the system module will connect to the server.

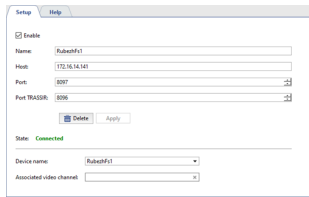


The default port values are:

- **Port** : **8097**;
- **Port TRASSIR** : **8096**.

Press **Create** upon completion. A new object will appear in the settings tree. Read more about its settings in [FireSec software module settings](#).

FireSec software module settings

The screenshot shows a 'Setup' dialog box with a 'Help' button. It contains an 'Enable' checkbox which is checked. Below it are input fields for 'Name' (containing 'Fubus001'), 'Host' (containing '192.16.16.141'), 'Port' (containing '8087'), and 'Port Timeout' (containing '6000'). There are 'Cancel' and 'Apply' buttons. Below these is a 'Status' field showing 'Connected'. At the bottom, there is a 'Device name' dropdown menu (showing 'Fubus001') and an 'Associated video channel' dropdown menu.

Set the **Enable** flag. The **Status** field will display the connection state. If all parameters are specified correctly, the **Connection established** line will appear, and the connected system objects will be added to the server object tree. For each module device, you can select one or more video channels to be associated with the specified devices. To do this:

- Select the device name in the **Device name** field.
- Select the video channel to be associated with this device in the **Associated Channel** field. One channel can be associated with several devices. For example, if several sensors are installed in the room, they can all be associated with a single camera.

Typical server settings for operation with Access Control or FAC



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 the server settings for operation with Schrack security and fire alarm system*
- *Specific features of server settings for operation with Spica access monitoring and control system server*
- *Features of server settings for operation with Paradox access monitoring and control system panels*
- *Stemax system server settings features*
- *Server settings features for operation with "MaxLogic" panels*
- *Configuration of Suprema (Biostar 2) Access Control*
- *Sigur(Sphinx) ACS server settings features*

In order to connect the server to the system, select the name of the module corresponding to the system being connected in the **Settings window** 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, the connection state will appear in the **Status** field. In case all parameters are entered properly, the **Connected** message will appear, and all the connected system objects will be added to the 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



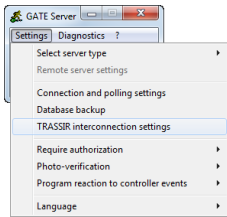
Modify the configuration file before connecting the server to the FortNet Access control system `fortnet.ini` server. The following block should be added to the end of the file:

```
[HTTPService]
Active=1
Port=8080
```

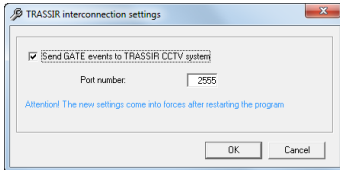
You can specify a different value for the network port. Make sure the port is not being used by third-party software.

"Gate" ACS server settings features

Set up the events transfer from Gate server objects to the video surveillance server before connecting to ACS. To do this, go to Gate server settings to **Settings** -> **Transmission settings**



Check the **Send events to video surveillance system** box and specify the **Communication port number** with which the data will be transferred from Gate ACS to the server.



Restart the server to apply settings. After that, you can proceed to the **connection settings**.

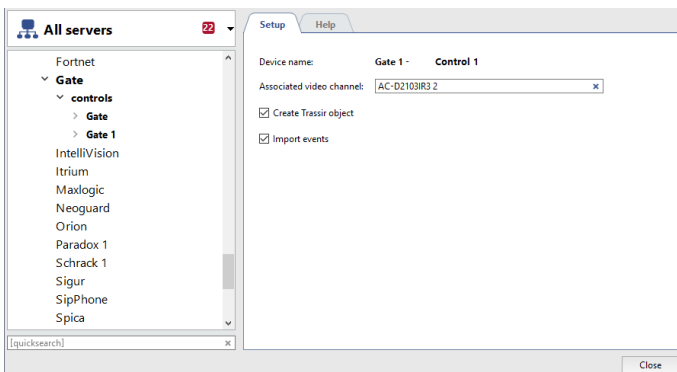
"Gate" ACS controller creation

The server is connected to Gate ACS via the controller. Open the **Plugins** -> **Gate** -> **Controllers** tab to create.

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.



The server 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

In order to connect the server to the "Itrium"ACS, you need from [our website](#). After that:

1. Unzip archive content on PC where Client DNO will be started.
The OPC Client can run on any PC in the same local network with the server and Itrium ACS servers. We advise running it at the same PC where the ACS 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** is the port via which the server will connect to the OPC Client's security and fire alarm system. The same value should be specified in [system connection settings](#).
- **localhost** - IP-address or DNS-name of PC on which "OpenOPC Gateway Service" is running.
- **7776** - 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.
You can connect any number of servers to a single OPC Client.

After that, you can proceed to [server to Access Control connection settings](#).

Specific features of the server settings for operation with Schrack security and fire alarm system

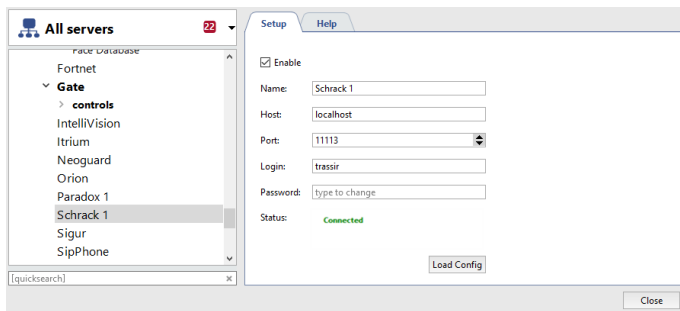
TRASSIR supports operation with all Schrack security and alarm systems operating on ISP protocol.



Schrack does not support automatic loading of the system objects.

To make objects appear on the server, it is necessary to load a configuration file with the connected object settings. You can get information on configuration files creation at "[Schrack Seconet AG](#)" company technical support.

The configuration file is downloaded immediately upon connection to Schrack security and fire alarm system. To do this, click **Download configuration** and select the file to download. After the download, security and fire alarm system objects will appear in server objects tree.

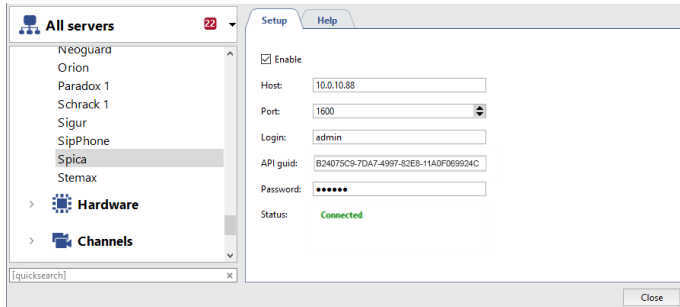


Specific features of server settings for operation with Spica access monitoring and control system server



TRASSIR supports operation with Spica software of 10.00.B. and newer versions.

While connecting to Spica ACS server, it is necessary to enter the **API identifier**. It can be received from [Spica International](#) company technical support service.



Features of server settings for operation with Paradox access monitoring and control system panels



TRASSIR supports working with the following ACS control panels:

- SP4000
- SP5500
- SP6000
- SP7000
- MG5000
- MG5050
- EVO192
- EVOHD

In order to connect the server to the Paradox system, you need **Paradox-Trassir-client**, which you can download from [our website](#). Next, execute:

1. Unzip the application archive on a PC used for launching the application.

Paradox-Trassir-client can run on any PC with OS Windows installed, located in the same local network with "Paradox" system servers and control panels.

2. In the configuration file `connection.ini` specify client connection parameters to Paradox system control panel and 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:

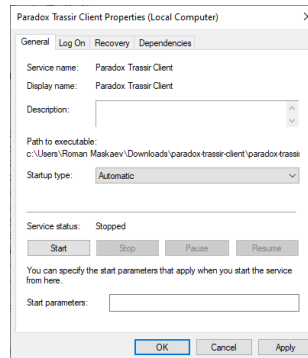
- **host** - control panel IP-address
- **port** - connection port.
- **panel_id** is the number of the panel to be used by the server for its identification.
- **login** and **password** - code of user and password which will be used to connect the Client to control panel.
- **local_port** is the port via which the server will connect to "Paradox Trassir Client". The 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.

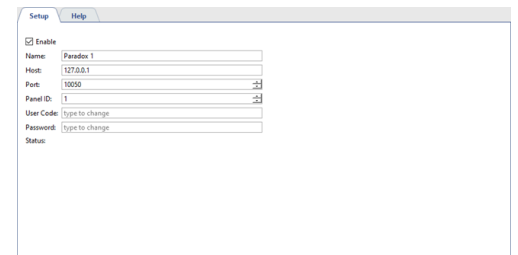
4. For automatic start of the service, change **Run type** in its settings.



After that, you can proceed to *to adjust server connections for Paradox system client*.



You can connect any number of servers to a single PC with "Paradox Trasser Client" installed.



Specify the following parameters in the "Paradox Trasser Client" connection settings:

- **Address** - IP-address or DNS-name of PC where "Paradox Trasser Client" has been started.
- **Port** - port of connection to "Paradox Trasser Client" specified in configuration file `connection.ini`.
- **Panel ID** is an identification number of the panel to which the server 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 the server to the "Stemax" system, you need **Stemax-Trassir-client**, which you can download from [our website](#). After that:

1. Unzip the application archive on a PC used for launching the application.
Paradox-Trassir-client can run on any PC in the same local network with the servers. We recommend running it on the same PC as the Stemax server.
2. In the configuration file `connection.ini` specify the client connection parameters to Stemax system and the 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
```

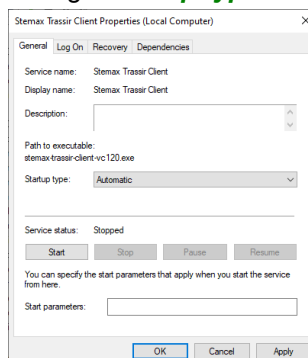
whereas:

- **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 the server will connect to "Stemax Trassir Client" service. The 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.



After that, you can proceed to [server connection settings to Stemax system client](#).



You can connect any number of servers to a single PC with "Stemax Trassir Client" installed.

Server settings features for operation with "MaxLogic" panels



TRASSIR supports operation with the following panels:

- ML-1207.MX
- MLY-1219.MX

In order to connect the server to the MaxLogic panels, you need **ModbusServer**, which you can download from [our website](#). Next, execute:

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 the server will connect to "ModbusServer". The same value should be set in [system connection settings](#).
- **COM3** - is a serial port, to which the panel is connected.
- **19200** - is the connection speed of the serial port.

After that, you can proceed to [server connection to "ModbusServer" settings](#).

Setup Help

☒ Enable

Name: Maxlogic

Host: 127.0.0.1

Port: 5050

Login:

Password: type to change

Status: Connected

Specify the following parameters in the server 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.

Configuration of Suprema (Biostar 2) Access Control

Suprema (Biostar 2) Access Control is an open integrated security system based on web technology offering a wide range of access control, time tracking, and customer management functions.



The time zone on the server should match the one on Suprema (Biostar 2) Access Control for the proper work of the system.

Suprema (Biostar 2) Access Control connects to servers via HTTPS secure protocol. Prior to the connection, do the following:

1. Download the certificate to connect Access Control to the server.



See how to create and download a certificate in details on the Suprema company site <https://support.supremainc.com>.

2. Add the downloaded certificate to the server certificate list.



To add a certificate, use **Import** function on the **Authorities** tab. See details in [Local server settings](#).



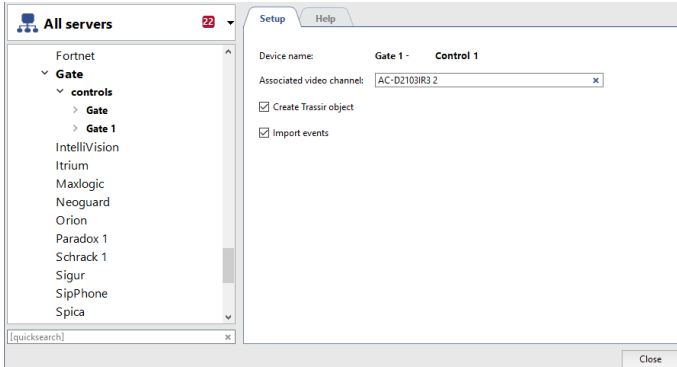
See [Typical server settings for operation with Access Control or FAC](#) for the rest of Access Control configuration steps.

See details on connecting Suprema (Biostar 2) Access Control to TRASSIR in our [knowledge base](#).

AMCS or security and fire alarm system objects settings tree

Upon successful connection to the server, all the objects corresponding to connected system objects will be created. You can select only those objects required for video surveillance system integration.

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 for the given device. This box is checked by the system for all the objects as default setting. In case such a device is not used in video surveillance system, it should be unchecked. It will allow refraining 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".