User manual of the software product

TrustViewerPro

The document corresponds to the version of the
TrustViewerPro **2.12.1**

www.pro.trustviewer.com

Content

1. Introduction....5
  1.1. Purpose and scope....6
  1.2. System requirements....6
  1.3. History of changes in this manual....7
2. License Agreement for the use and distribution of the program....9
3. Choosing a deployment strategy «TrustViewerPro»....10
  3.1. License options....10
  3.2. Using «TrustViewerPro» for home use....11
  3.3. Professional use of «TrustViewerPro» to support users via the Internet....11
  3.4. Administration workstations in the enterprise using «TrustViewerPro»....11
  3.5. Using «TrustViewerPro» in multitasking mode....11
4. Installation....13
  4.1. Installation of the «TrustServer» server....13
    4.1.1 Installing the «TrustServer» server in the Windows operating system....15
    4.1.2 Installing the «TrustServer» server in the GNU/Linux operating system....15
    4.1.3 Configuring the «TrustServer» server after installation....16
  4.2. Installing the client module «TrustViewerPro»....18
    4.2.1 Installation of own branded distributions of client modules signed by the developer's EDS....19
    4.2.2 Manual installation of the «TrustViewerPro client module»....19
    4.2.3 Configuring the distribution package of the «TrustViewerPro» client module....20
    4.2.4 Installing the client module «TrustViewerPro» using the command line....21
    4.2.5 Running of the portable version of the «TrustViewerPro» client module....22
    4.2.6 Setting up the operation of «TrustViewer» in compatibility mode with «TrustViewerPro»....22
    4.2.7 Configuring a stand-alone client module for instant remote support....22
    4.2.8 Running and installing the "TrustViewerPro" client module in the GNU/Linux operating system....23
5. Administration of the «TrustServer» server....25
  5.1. Server Status Information....25
  5.2. User management....26
    5.2.1. Editing user profiles....26
    5.2.2. Permissions to access departments / computers....29
    5.2.3. Additional user rights....34
    5.2.4. Permitted Divisions/Computers Templates....36
    5.2.5. Importing user accounts....36

- 5.3. Computer Management 39
  - 5.3.1. Editing group accounts 39
  - 5.3.2. Editing computer cards 41
- 5.4. Configure integration with Helpdesk / Service desk services 42
- 5.5. Update Management "TrustViewerPro" 48
- 5.6. Branding settings 49
  - 5.6.1. Generation of own distributions signed by the developer's EDS 50
  - 5.6.2. Banner, logo and wallpaper management 51
- 5.7. Main server settings 53
  - 5.7.1. License activation 53
  - 5.7.2 Main settings 54

6. Work with the client module «TrustViewerPro» 57

- 6.1. Settings of the client module «TrustViewerPro» 57
  - 6.1.1. “Main” settings page 57
  - 6.1.2. Personal Settings Page 58
  - 6.1.3. “Voice and Video” settings page 59
  - 6.1.4. “Connections” settings page 60
  - 6.1.5. “Additionally” settings page 61
  - 6.1.6. Settings page “TrustServer” 62
  - 6.1.7. Settings page “Access this computer” 62
  - 6.1.8. Settings page “Security” 63
- 6.2. Work with the «TrustViewerPro» client module in client mode 64
  - 6.2.1. Granting access using a temporary ID 64
  - 6.2.2. Providing access through the application to the helpdesk service 66
  - 6.2.3. Providing access using the contact list 67
- 6.3. Work with the «TrustViewerPro» client module in the operator mode 68
  - 6.3.1. Communication session in desktop view only 70
  - 6.3.2. Communication session in the joint computer control mode 72
  - 6.3.3. Communication session in the mode of full access to the computer 72
  - 6.3.4. View mode “File and folder sharing” 73
  - 6.3.5. Presentation mode “Desktop demonstration” 75
  - 6.3.6. View mode “Video call” 77
  - 6.3.7. Voice mode 77
  - 6.3.8. Connecting to a remote computer using the contact list 78
- 6.4. Working with the «TrustViewerPro» client module in network administrator mode 80
  - 6.4.1. Computer control panel 80

    - 6.4.2. Group sending of messages and commands / scripts / settings 83
    - 6.4.3. Editing computer cards 85
    - 6.4.4. Configuring RDP Connection Settings 85
    - 6.4.5. The mode of fast connection to a computer on the network 86
  - 6.5. Working with recordings and translations of communication sessions 87
  - 6.6. Working with the «TrustViewerPro» client module in operator helpdesk mode 88
    - 6.6.1. Work in the operator mode of the 1st line helpdesk 89
    - 6.6.2. Work in the operator mode of the 2nd line helpdesk 90
  - 6.7. Integration with Active Directory 92
- 7. Contact Information 93

1. Introduction

The software «TrustViewerPro» is an extended version of the free software «TrustViewer» and is distributed on a subscription basis. The main difference between «TrustViewerPro» and the free version is the obligatory use of a dedicated server «TrustServer», which provides additional functionality, when organizing remote access and user support in local networks and via the Internet. «TrustViewerPro» is backward compatible with «TrustViewer», that is, using «TrustViewerPro» you can connect to remote computers on which «TrustViewer» is installed (provided they are connect to the same «TrustServer» server). The following are the main differences between the «TrustViewer» and «TrustViewerPro» products.

	«TrustViewer»	«TrustViewerPro»
Distribution model	Free distribution	Subscription distribution
Support of Users in the local network and via the Internet (remote access based on temporary identifiers, in the joint computer control mode)	Yes	Yes
The possibility of branding and display your advertising materials on end devices, including portable client modules for instant remote support.	Yes, TrustViewerPro compatibility mode only	Yes
Integration with Service desk / Helpdesk systems (remote access based on ticket applications)	-	Yes
Administration of workstations in the local network and via the Internet (remote access to autonomous devices, Wake On LAN, group execution of commands/scripts, etc.)	-	Yes
Remote workplaces of employees (private remote access via the Internet to terminal servers and autonomous working workstations based on the RDP protocol)	-	Yes
Use of dedicated coordinating proxy server «TrustServer»	Yes, optional use	Yes, obligatory use
Independence from public servers (the possibility of full-fledged work in private networks without access to the Internet)	-	Yes
User/operator/administrator rights management using the «TrustServer» control Panel	-	Yes
Support for broadcast communication sessions (mass broadcast to end devices in the local network and over the Internet).	-	Yes
The ability to automatically record all communication sessions with their centralized storage and access on the «TrustServer» server.	-	Yes
Automatic mass deployment of the client module (using group policy in an Active Directory domain)	-	Yes

1.1. Purpose and scope

The software «TrustViewerPro» is specifically designed to provide easy and secure access to remote computers and allows to solve the following main tasks:

- User support on the local network and via the Internet
- Administration of workstations in the local network and via the Internet
- Organization of remote workplaces of employees in the local network and via the Internet

The software «TrustViewerPro» consists of two interrelated modules:

- The «TrustViewerPro» client module is installed on end-user computers and allows both to provide remote access to your computer and to connect to other remote computers
- A specialized server «TrustServer» is installed on a physical or virtual server, and in respect of the client module «TrustViewerPro» acts as a coordinating server (responsible for initializing communication sessions), proxy server (transmits traffic between computers, in case of impossibility of direct p2p-connection between them), update server (allows you to automatically maintain the relevance of versions of both client modules, and the server itself), a record storage server (allows you to organize centralized storage and access to records of communication sessions), a translation server (provides mass broadcasting of communication sessions to terminal devices online) and the administration server (allows you to manage the rights and settings of registered users and computers, as well as the settings of the server itself, using the built-in control panel)

1.2. System requirements

Minimum requirements for hardware and software for the «TrustViewerPro» client module:

- computer running Windows XP SP3, or GNU/Linux
- processor - Pentium IV 1 GHz
- RAM - 128 MB
- 10 Mb free hard disk space

Minimum requirements for hardware and software for the «TrustServer» server:

- computer running the Windows Server 2003 operating system, or GNU/Linux
- processor - Pentium IV 1 GHz
- RAM - 128 MB
- 10 Mb free hard disk space
- OpenSSL cryptographic library (not mandatory, but strictly recommended condition)

1.3. History of changes in this manual

April 07, 2024 (corresponds to TrustViewerPro 2.12.1 build 5195)

- Changing the description of settings and features: configuration of the "TrustServer" server.

March 24, 2024 (corresponds to TrustViewerPro 2.12.0 build 5189)

- Changing the description of settings and features: installation and configuration of the "TrustServer" server.

February 24, 2024 (corresponds to TrustViewerPro 2.11.0 build 5090)

- Changing the description of settings and features: installation and configuration of the "TrustServer" server; work with the client module in client, operator and network administrator modes.

March 31, 2023 (corresponds to TrustViewerPro 2.10.0 build 4500)

- Changing the description of settings and features: administering the TrustServer server, Installing the TrustViewerPro client module (added a description of the installation and configuration of the client module for Linux OS).

September 18, 2022 (corresponds to TrustViewerPro 2.9.0 build 4203)

- Changing the description of settings and features: administering the TrustServer server, Installing the TrustViewerPro client module. Added description of integration with ActiveDirectory.

July 14, 2022 (corresponds to TrustViewerPro 2.8.0 build 4124)

- Changing the text of the license agreement for the use and distribution of the program (added a clause on the conditions for demonstrating branding elements).

July 10, 2022 (corresponds to TrustViewerPro 2.8.0 build 4124)

- Changing the description of settings and features: administration of the server "TrustServer".

October 16, 2020 (corresponds to TrustViewerPro 2.3.0 build 3881)

- Changing the description of settings and features: installation and configuration of the "TrustServer" server; work with the client module in client, operator and network administrator modes.

June 28, 2020 (corresponds to TrustViewerPro 2.2.0 build 3640)

- Changing standard license options.
- Changing the description of settings and features: installing the TrustViewerPro client module; Administration of the TrustServer server (User Management); TrustViewerPro client module settings.

March 31, 2020 (corresponds to TrustViewerPro 2.1.2 build 3550)

- Changing the description of settings and features: installing the "TrustViewerPro" client module; working with the client module in network administrator mode.

March 07, 2020 (corresponds to TrustViewerPro 2.1.1 build 3500)

- Changing the description of settings and features: working with the client module in network administrator mode.

January 05, 2020 (corresponds to TrustViewerPro 2.1.0 build 3450)

- Changing the text of the license agreement for the use and distribution of the program.
- Changing the description of settings and capabilities: branding and demonstration of their advertising materials on end devices; centralized updating of client modules and server; manage computers, users, and user groups using the server control panel; work with the client module in client, operator and network administrator modes.
- Adding a description of new settings and features: support for a stand-alone client module to provide instant remote support; support for automatic recording of all communication sessions with their centralized storage and access on the server; support for broadcasting communication sessions.

June 14, 2019 (corresponds to TrustViewerPro 2.0.0 build 3014)

The first publication of this manual.

2. License Agreement for the use and distribution of the program

Please read this end user license agreement carefully. By installing or using the TrustViewerPro software, you hereby agree to comply with the terms of this license agreement. If for any reason you disagree with this license agreement, you need to delete the distribution files and stop using the TrustViewerPro software.

All copyrights to the TrustViewerPro software belong only to the company-developer – “Trust Ltd” OOO (hereinafter referred to as the “Copyright Holder”).

TrustViewerPro software is distributed freely, provided that this distribution is not modified. It is prohibited to charge for distribution of TrustViewerPro without the written permission of the Copyright Holder.

TrustViewerPro software is permitted to use in all countries of the world, in any form and in any manner not contrary to the law, subject to the rights of the Copyright Holder. It is forbidden to modify, create new versions, emulate, decompile, study and distribute the program code and its components.

TrustViewerPro software allows you to display your branding elements (logo, wallpaper of the main form and banners), but only on condition that they do not fall into the following list of prohibited for posting: False, incorrect or misleading information; Malicious and unwanted programs; Pornography; Lotteries; Fake goods; Media data created with violation of copyright and related rights, use of other people's trademarks; Links to mail and electronic spam mailings; Financial pyramids; Materials with elements of profanity, as well as materials aimed at inciting hatred or enmity, as well as at humiliating the dignity of a person or group of persons.

TrustViewerPro software can send statistical information about usage, as well as error reports on its work, to the server of the Copyright Holder. At the same time, the Copyright Holder guarantees that no information will be transmitted that can identify or compromise computers and their users (such as IP and MAC addresses, serial numbers of equipment, network names, memory dumps, etc.). The Copyright Holder also undertakes not to transfer the information thus obtained to third parties, and use it solely to improve the operation and maintenance of TrustViewerPro software.

TrustViewerPro software is provided on an “AS IS” basis, no warranty is attached and is not available. You assume the entire risk of using the program. The Copyright Holder under no circumstances shall bear to you any liability for damages, forced business interruptions, loss of business or other data or information, claims or expenses, consequential or incidental damages, as well as lost profits and lost savings caused by the use or related to using TrustViewerPro software.

This license agreement may be amended unilaterally by the Copyright Holder.

3. Choosing a deployment strategy «TrustViewerPro»

TrustViewerPro is a multifunctional software product designed for solving a wide range of tasks, suitable for use both in large and small enterprises and for personal purposes. Therefore, depending on the tasks assigned, TrustViewerPro's deployment strategies may differ significantly.

3.1. License options

All license options (even a free demo version) have the same, unlimited functionality, with the exception of one setting, which is the determining factor when choosing a product deployment strategy - the number of devices simultaneously connected to the server.

Attention! The licensing object is only the server itself, and the number of installed copies of client modules in all installation options and modes of use is unlimited. If the number of devices simultaneously connected to the server is exceeded - the work of the client modules is not blocked (the connection to the server is not broken), but until the server has enough free connections, it will not be possible to initiate a new communication session. For example, sending messages to users will be available).

Attention! Even a client module installed and working on a computer does not necessarily use a permanent connection to the server, so when choosing a license, it is important to understand how the program will be installed and how it will be used on target computers in the future.

The client module, both on the receiving and supporting side, necessarily uses the connection to the server during the initiation of a communication session using the identifier (after the expiration of the identifier and also in the case of canceling the communication session - the connection to the server becomes inactive). Directly during an active communication session, each participant's computer uses the connection to the server only if it was not possible to establish a direct connection between the computers, and the TrustServer server acts as a proxy server (after the end of the communication session, the connection to the server becomes inactive). In addition, the client module installed on the computer has a permanent connection to the server in the following cases:

- the computer is authorized on the server using a group account (it means, the computer card is displayed on the server in the list of computers available for management)
- at least one of the users of the computer has an active request to the Helpdesk service (in case of cancellation / completion of the request - a permanent connection to the server becomes inactive)
- at least one of the users of the computer exchanged contacts with another user (in case of deletion or blocking of all contacts - a permanent connection to the server becomes inactive)
- at least one of the users allowed temporary uncontrolled access to the computer (in case of access cancellation or the expiration of the access granted, permanent connection to the server becomes inactive)

Attention! The TrustViewer program, operating in the TrustViewerPro compatibility mode, uses a connection to the server in the same way, except for authorizing a computer and submitting an application to the Helpdesk service (these modes are not available for TrustViewer). In addition, because the server considers connected devices, simultaneously running on the same computer TrustViewer and TrustViewerPro, consume only one license connection.

Currently, the following standard license options are available (for terms of purchase, see the program’s official website):

- up to 30 simultaneously connected devices to one server
- up to 100 simultaneously connected devices to one server
- up to 200 simultaneously connected devices to one server
- up to 500 simultaneously connected devices to one server
- up to 1000 simultaneously connected devices to one server
- up to 2000 simultaneously connected devices to one server

In addition, the server without license activation, provided it is used for home purposes, allows you to work simultaneously with ten connected devices.

3.2. Using «TrustViewerPro» for home use

Without license activation, the server has a limitation - no more than 10 (ten) simultaneously connected devices. However, this may be quite enough when it is used for home purposes. For example, you can manage your nine home workstations from anywhere on the planet (one connection for each managed workstation, plus one connection to the computer you are managing), or provide remote support via the Internet to your friends and family using temporary access identifiers (in this case, only two connections to the server are spent for each active session, i.e., an unlimited number of serial connections to different computers can be made from one workstation)

3.3. Professional use of «TrustViewerPro» to support users via the Internet

A client module installed in the workplace without authorizing a computer on a server — spends one license connection only during a communication session, thus, it is possible to install client modules on an unlimited number of devices and then connect to them using temporary access identifiers. In this case, licenses for 30 simultaneously connected devices are enough to ensure the full simultaneous operation of several operators to provide remote user support via the Internet, including the possibility of providing temporary unsupervised access.

3.4. Administration workstations in the enterprise using «TrustViewerPro»

To be able to fully administer using TrustViewerPro, both on the local network and over the Internet, it is necessary to authorize computers on the server, i.e. Each authorized computer will constantly use one licensed connection to the server. Thus, the type of license chosen directly depends on the number of computers in the enterprise.

3.5. Using «TrustViewerPro» in multitasking mode

TrustViewerPro allows you to simultaneously solve many tasks: the administration of computers on the local network, centralized administration via the Internet workstations, remote support for clients of the enterprise via the Internet, support users in the mode of integration with already deployed in the enterprise services Helpdesk/ServiceDesk, organization of remote workplaces of employees. In General, the choice of license type depends on the number of computers that require constant connection to the server (computer administration, integration with Helpdesk/ServiceDesk services, remote workplaces of employees), taking into account additional connections related to operational work (connection to computers using temporary identifiers, support of secure contacts and provision of temporary uncontrolled access).

4. Installation

The software product «TrustViewerPro» consists of two modules: the client module «TrustViewerPro», installed on end-user computers running the Windows operating system or GNU/Linux, and a specialized server «TrustServer», installed on computers running the server operating system Windows or GNU/Linux.

4.1. Installation of the «TrustServer» server

«TrustServer» is a program launched by the system itself and running in the background without direct interaction with the user, i.e. is a “demon” in Unix / Linux terminology. In this case, all the settings required for launching are transmitted on the command line. Thus, the installation of «TrustServer» is reduced to setting up an automatic launch at system bootup, and depends on the type of operating system. Settings at startup are transmitted on the command line as follows: “**start [options]**”, where “[options]” is a combination of the possible options. The following is a complete list of possible options when starting the «TrustServer» server.

Option	Description
-udp <value>	Set the udp-port value for local connections, different than the default (27463).
-port <value>	Set the tcp-port value for local and Internet connections, different than the default (443).
-lport <value>	Set the value of the additional dedicated tcp port for local connections. An additional dedicated port for local connections can be used to distinguish between local and Internet traffic. If this setting is specified, only connections made to the specified port will be considered as local inbound connections. If this setting is not specified, incoming connections to the local or Internet network will be made automatically based on the connection address, which may not always be correct, for example, if the server is behind the router.
-cport <value>	Set an additional dedicated tcp-port to access control panel. If the parameter is set, then you can enter the server control panel only at the address specifying this port.
-host <name>	Set the value of the host name for local connections, different than the value determined automatically.
-wport <value>	Announce the value of the external tcp-port for incoming Internet connections, different from the value specified by the "- port" option (it can be useful when forwarding ports for the server to work through the router).
-whost <name>	Declare the value of the external host name for incoming Internet connections, different from the value defined automatically. Here you can also specify the URL of the service that returns the external IP address (by default, the service is used at the address "http://trustviewer.com/cgi-bin/server.pl?cmd=myip").
-rhost <name@value>	Set the address of the backup communication channel for the server, indicating the percentage probability that if both communication channels are available, then the backup communication channel will be preferred when the client connects for the first time.
-redirproxy	Set up redirection of local requests to the server to an upstream server (used by the client module operating in the local network behind the router to automatically detect the Internet server). The address of the upstream server is specified using the "-host" and "-port" settings.
-localsocks5	Block Internet connections to the server using the socks5 protocol (only http / https protocol will be available for Internet connections).
-localproxy	Block all Internet connections to the server (server mode only in LAN).
-pass <text>	Set a password to access the server. It is used as a temporary password to access the server control panel (for the period of the initial server setup after its

	installation). It is also used for compatibility with the free client module “TrustViewer” in the secure access mode to the “TrustServer” as a coordinating proxy server.
-ssl <name>	Set the path to the directory with the OpenSSL libraries, different from the automatically defined one.
-cert <name>	Specify the path to the SSL-certificate file
-key <name>	Specify the path to the SSL-key file
-keypass <txt>	Specify the password to SSL-key
-log <name>	Set the path to the log file (by default, the log file is created automatically in the folder where the server executable file is located).
-data <name>	Set the path to the directory with the server data (by default, the directory structure containing all the files necessary for the server to work is created automatically in the folder where the server executable file is located).
-data <name>	Specify the path to the directory with recordings data (different from the one created automatically or specified using the “–data” parameter)
-cpt <value>	Limits the maximum number of connections served a single thread (value from 1 to 64, default 16)
-nossl	Отключить явное использование библиотеки OpenSSL
-nowatch	Disable the additional process that monitors the correct operation of the server (used to automatically restart the server in case of failures in its operation).
-foreground	Disable startup in the background.

Command line examples for starting the server using settings(here “**TrustServer.exe**” is the name of the executable file “**TrustServer**” for the Windows operating system, for Linux 32 and 64 bit operating systems - the name of the executable file must be “TrustServer” and “**TrustServer64**” respectively):

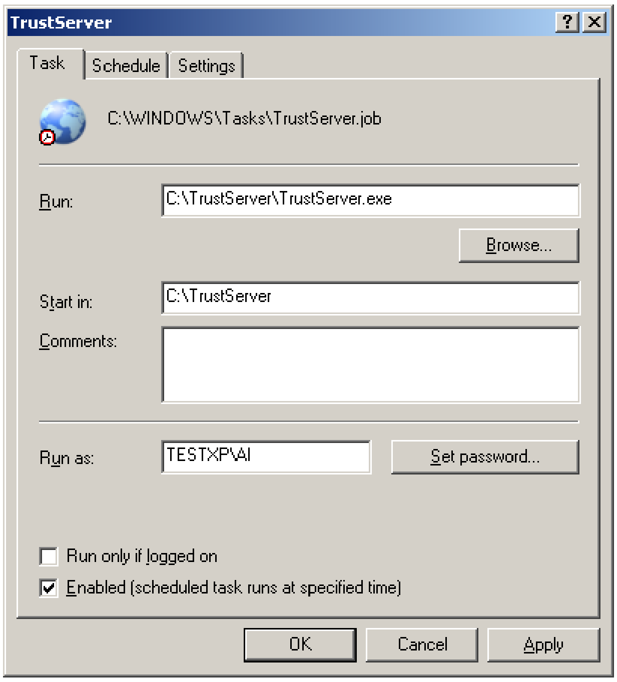
- “**TrustServer.exe start**” - start the server with default settings
- “**TrustServer.exe start -port 8080 -pass 123456**” - starting server with tcp-port “8080” and password "123456"
- “**TrustServer.exe start -port 8080 -host youservername.com -redirproxy**” - starting the server in request redirection mode (redirecting local requests to the server at "www.youservername.com:8080")
- “**TrustServer.exe start -port 8080 -wport 443 -whost youservername.com**” - starting the server with tcp port 8080 and declaring a public address "www.youservername.com:443" for incoming Internet connections (on the router, you must configure the port mapping correctly for the server)
- “**TrustServer.exe start -whost http://www.youserverutils.com/myip**” - starting the server with TCP port 443 by default and declaring the public address received from the service "http://www.youserverutils.com/myip" (for example, if the service returned the address "194.58.92.117", the public address for incoming Internet connections will be declared as "194.58.92.117:443")
- “**TrustServer.exe start -whost 194.58.92.117 -rhost 89.108.115.128@25**” - starting the server with the main address for incoming Internet connections “194.58.92.117”, as well as the address of the backup communication channel “89.108.115.128”, and the probability with which client modules will connect via the backup channel (provided that both communication channels are available) is 25%.

Attention! Setting up an SSL certificate (parameters –cert, –key and –keypass) is optional, but strictly recommended condition, because it allows not only to safely manage the server using the browser over https, but also to provide additional functionality of the client modules. You can use a self-signed SSL certificate created, for example, using the OpenSSL utility with the command “openssl.exe req -x509 -newkey rsa:2048 -days 365 -keyout mykey.key -out mycert.crt”

4.1.1 Installing the «TrustServer» server in the Windows operating system

«TrustServer» is not a Windows service, it is a regular program, but with the ability to run in the background, both on behalf of the system and on behalf of the user. Thus, the automatic startup at system boot can be performed both by the system itself and by third-party applications / scripts. The following is an example of setting up an automatic launch using the Windows Task Scheduler:

- Create a new folder, for example “**C:\TrustServer**” and copy the executable file **TrustServer.exe** there
- Start the Windows Task Scheduler, for example, using the command line “**Taskschd.msc**”
- Create a new task.
- Specify the path to the executable file **TrustServer.exe**
- Select the startup condition “At system startup”
- In the advanced settings of the task, specify the settings of the launch, for example “**Start –port 443**”



C:\WINDOWS\Tasks\TrustServer.job

Run: C:\TrustServer\TrustServer.exe

Start in: C:\TrustServer

Comments:

Run as: TESTXP\Al

☐ Run only if logged on

☑ Enabled (scheduled task runs at specified time)

4.1.2 Installing the «TrustServer» server in the GNU/Linux operating system

“TrustServer” is a daemon, which is started by the “**Start**” setting, and for stop - by the “Stop” setting. The following is an example of creating a service to start automatically at boot:

- Create a new folder, for example **“/srv/TrustServer**”, copy the executable file **TrustServer64** (for a 64-bit operating system) or **TrustServer** (for a 32-bit operating system) and mark it as “Executable”
- Create a new file “/etc/systemd/system/TrustServer.service”

```
[Unit]
Description=TrustServer
After=multi-user.target

[Service]
Type=forking
```

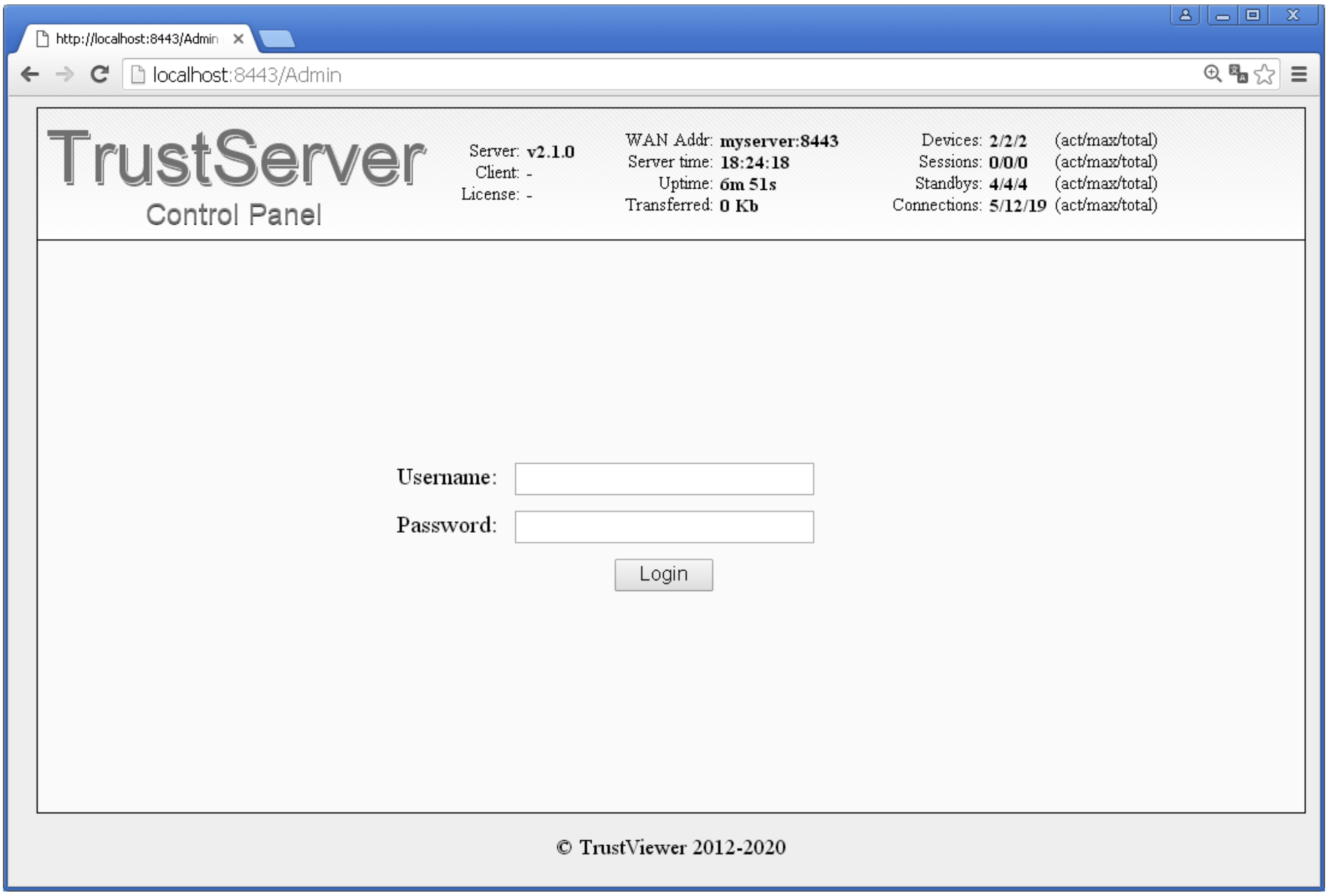
```
WorkingDirectory=/srv/TrustServer/

ExecStart=/srv/TrustServer/TrustServer64 start -port 443
ExecStop=/srv/TrustServer/TrustServer stop

Restart=always

[Install]
WantedBy=multi-user.target
```

- Execute commands sequentially with administrator rights

```
systemctl daemon-reload
systemctl enable TrustServer
systemctl start TrustServer
```

4.1.3 Configuring the «TrustServer» server after installation

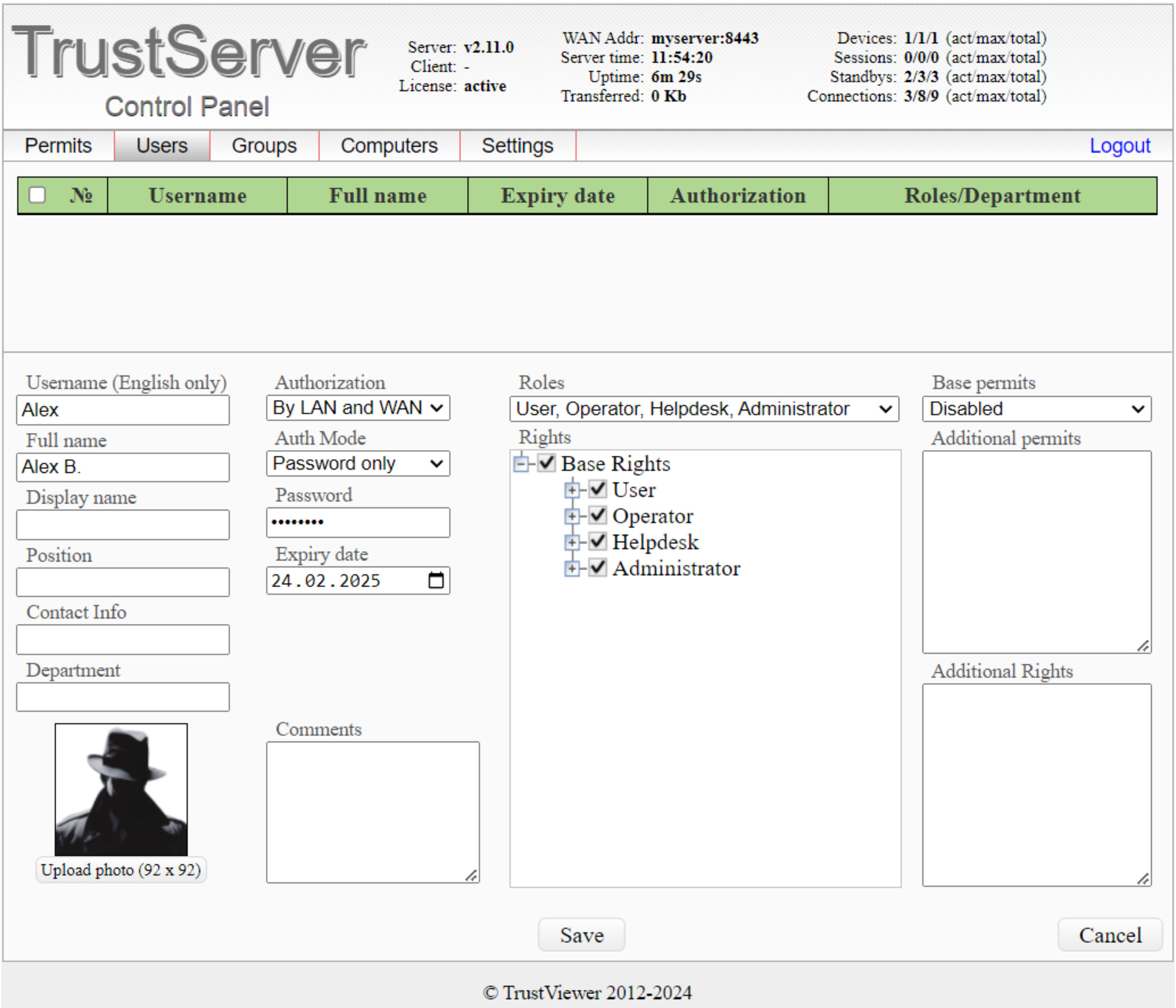
The TrustServer server is managed via the built-in control panel, which can be accessed from any modern browser. To access the initial settings of the “TrustServer” server, you must first start it with a password (the “-pass” setting in the server launch command line), then you can use a special temporary account “root” for authorization. For example, if you start the server with the setting “**TrustServer.exe start -port 8443 -whost myserver -pass 123456**”, then the control panel page will be accessible at the addresses “https://myserver:8443/Admin” and “http://localhost:8443/Admin”, and for authorization you need to use the login “root” and the password “123456”.



Server: v2.1.0
Client: -
License: -
WAN Addr: myserver:8443
Server time: 18:24:18
Uptime: 6m 51s
Transferred: 0 Kb
Devices: 2/2/2 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 4/4/4 (act/max/total)
Connections: 5/12/19 (act/max/total)

After successful authorization, you need to create a permanent server administrator account: go to the “Users” page, click “Add new user”, fill in the required fields (“Username”, “Full name”, “Password”), and in the “Authorization" field” specify the “Super admin" authorization mode for the user, then save the changes (click the “Save” button).

Attention! For the program to work correctly, at least one account with server administrator rights must be active, otherwise the connection of client modules to the server will be suspended.



Server: v2.11.0
Client: -
License: active
WAN Addr: myserver:8443
Server time: 11:54:20
Uptime: 6m 29s
Transferred: 0 Kb
Devices: 1/1/1 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 2/3/3 (act/max/total)
Connections: 3/8/9 (act/max/total)

Username (English only): Alex
Full name: Alex B.
Display name:
Position:
Contact Info:
Department:
Authorization: By LAN and WAN
Auth Mode: Password only
Password: ••••••••
Expiry date: 24.02.2025
Roles: User, Operator, Helpdesk, Administrator
Base permits: Disabled

Rights:
- ☑ Base Rights
  - ☑ User
  - ☑ Operator
  - ☑ Helpdesk
  - ☑ Administrator

Attention! After creating a server administrator account, a temporary account with the login “root” is blocked, and subsequent authorizations must be performed with a new account. At the same time, the “-pass” setting can be deleted from the server launch command line.

Attention! By default, authorization with server administrator privileges is allowed both on the local network and over the Internet. If there is a need to prohibit authorization with administrator rights over the Internet, then on the “Settings”->”General” tab, select the “By local network only” setting for “TrustServer auth mode”.

Attention! Unregistered copy of “TrustViewerPro” has restrictions on the number of connections to the server, so product registration is required to complete the work. To register a product, on the “Settings”->”General” tab, click the “New license” button, enter the license number in the “License number” field, and click the “Apply” button. For more information on the registration procedure, see “License Activation”, in the “Administration of the TrustServer Server” section of this manual.

4.2. Installing the client module «TrustViewerPro»

Distributions of the TrustViewerPro client module are presented in a portable version of the program installed using the built-in wizard, as well as in an msi-package, with the ability to both configure installation parameters directly in the package itself and pass parameters on the command line during installation. It is preferable to generate such distributions on your own in the trustserver control panel, but it is also possible to install the original distributions in manual mode, followed by setting the parameters using the interface of the client module itself. The following is a list of installation settings available for editing in the msi-package, as well as for passing as settings on the command line:

Setting	Description
INSTALLSERVER <value>	Sets the server address, as well as credentials for authorizing a computer on the server, in the format “login:password@host:port”, where “login:password” respectively the login and password of a group account, and “host:port” is the address of the TrustServer server .
INSTALLDIR <value>	Specifies the destination folder where the client module will be installed
INSTALLFLAGS <value>	Specifies, in decimal format, a combination of bit flags responsible for additional installation settings: “1” (0b00000001) - install the program for all users “2” (0b00000010) - add icon to desktop “4” (0b00000100) - add an icon to the “Start” menu “16”(0b00010000) - set association with record files (*.tvr)

There are two options for installing the TrustViewerPro client module: in limited mode and in full functionality mode. The limited functionality mode is intended primarily for distribution in open access via the Internet. In this case, access to the computer with the installed client module is possible only by the ID or the ticket of the Helpdesk application, and the number of copies installed is not limited by the terms of the purchased license. In the full functionality mode, all additional functions are available, including uncontrolled access to this computer, however, the number of copies installed is limited by the terms of the purchased license (for more information on license restrictions, see “License Activation”, in the “Administration of the TrustServer server” section of this manual).

The installation mode (limited or functionality) is selected automatically, and depends on the installation setting “INSTALLSERVER“. If the “INSTALLSERVER” setting is not explicitly specified or only the server address is specified, the installation will be performed in reduced functionality mode. If, in addition to the server address, the setting also specifies the login and password of the group account, the installation will be performed in full functionality mode (for more information on setting up group accounts, see “Editing group accounts”, in the “Administration of the TrustServer” section) of this manual).

Attention! For security reasons, after installing the client module in the full functionality mode, uncontrolled access to the computer is disabled by default. To enable unsupervised access to a computer, in the menu of the main window of the program, open the computer access settings page (“Menu” → “Settings” → “Access to this computer”), and depending on the required, check the “Access via RDP” box and / or “Uncontrolled access” with the password for access to the computer (if necessary).

Attention! You can change the client module's mode of operation (limited or full functionality mode) - at any time after its installation, by disabling / enabling computer authorization: in the program’s main window, open additional network settings (“Menu” → “Settings” → “Connections” → “TrustServer”), and depending on the required, uncheck or check the “Authorization (computer registration on the server)” box with the login and password of the group account.

Attention! You can change the client module settings remotely from the computer control panel (right mouse button on the computer card, “Send settings“), but the corresponding permission must be set in the remote computer program settings (”Menu“→”Settings“→”Security“, the ”Allow remote modifications of program settings" check box). In addition, you can also set the appropriate permission remotely (right-click on the computer card “Enable Remote Settings”), however, for security reasons, in this case you need to specify the username/password of the system account with administrator rights (both the local account and the active directory account will work).

Attention! Msi-package distribution package of the client module “TrustViewerPro” does not support the update mode of an already installed product. To manage client module updates on workstations, you need to use the TrustServer update center (for more information, see the “Update Management TrustViewerPro” section, in the “Administration of the TrustServer Server” section of this manual). To update the client module in manual mode, you must first uninstall an already installed version of the product, and then install a new one.

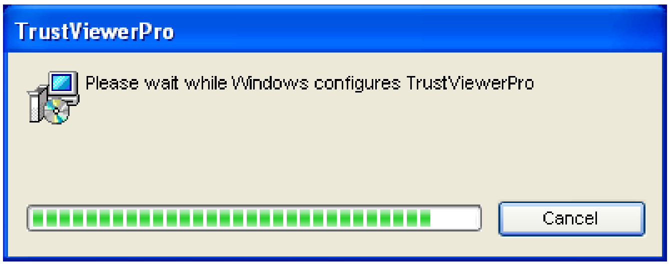
Attention! If the program is deployed to computers by cloning a hard disk, the client module must be installed on the reference computer without being able to connect to the TrustServer server, otherwise duplication of computer cards is possible.

4.2.1 Installation of own branded distributions of client modules signed by the developer's EDS

The option of installing your own branded distributions is preferable, because. in this case, the settings for connecting to the trustserver are saved inside the distribution files signed with the developer's EDS, and in most cases, after installing them, no additional settings are required. For more information about generating your own branded distributions, see the paragraph “Generation of your own distributions signed by the developer's EDS”, in the “Administration of the TrustServer” section of this manual.

4.2.2 Manual installation of the «TrustViewerPro client module»

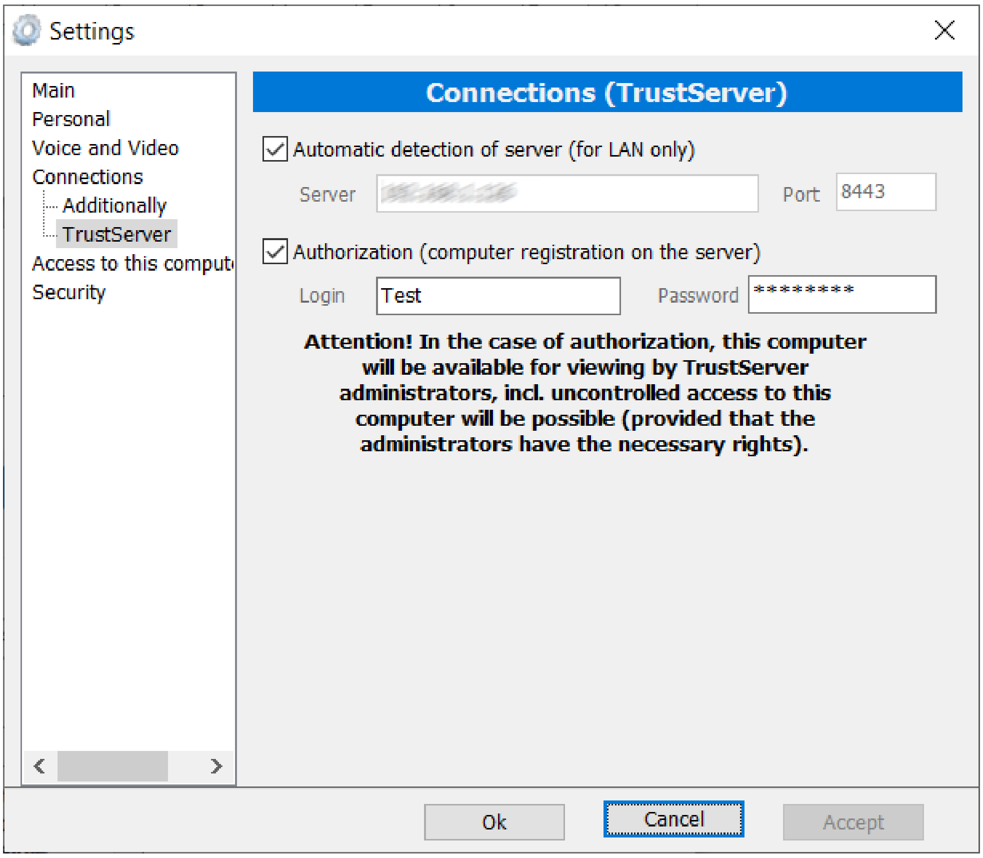
To install the TrustViewerPro client module in manual mode, launch the original TrustViewerPro.msi file for execution and wait for the installation to complete.



Please wait while Windows configures TrustViewerPro

Attention! To install the client module “TrustViewerPro”, computer administrator rights are required.

If the client module is supposed to work only in the limited functionality mode, and also if it is supposed to work only on the common local network, then no further configure of the network settings of the program is necessary (detection of the TrustServer server in the local network, by default, is performed automatically). If the client module of the TrustServer server cannot be automatically detected (the client module and server are in different networks, for example, they are separated by the global Internet), after the installation is completed, you must specify the server address in the program settings: open the main program window (click on the icon “TrustViewerPro” in the tray, or open it using the corresponding shortcut on the desktop), open the additional network settings in the menu (“Menu” → “Settings” → “Connections” → “TrustServer”), uncheck the “Automatic server detection” checkbox and enter the values of the TrustServer server host and port respectively in the “Server” and “Port” fields. Also, if you expect the client module to work only in full functionality mode, then on the same tab “Server TrustServer” – you need to configure computer authorization: check the “Authorization (computer registration on the server)” with the login and password of the group account.



Connections (TrustServer)

☑ Automatic detection of server (for LAN only)

Server [redacted] Port 8443

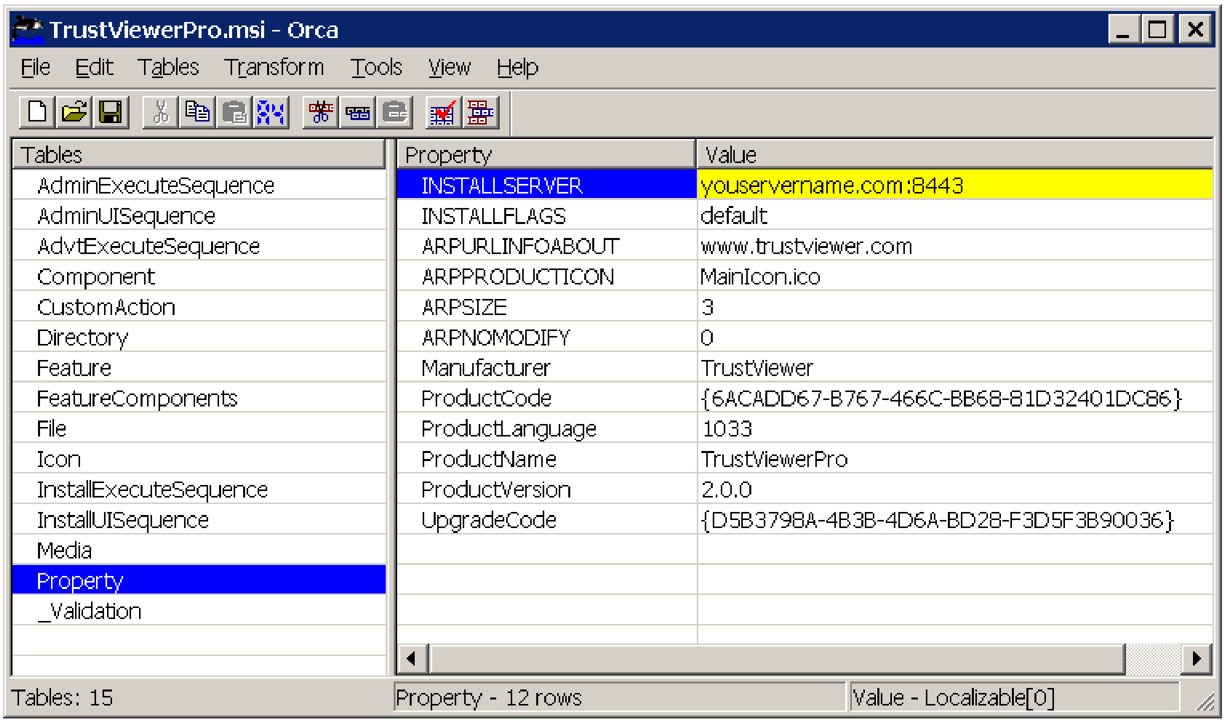
☑ Authorization (computer registration on the server)

Login Test Password *********

Attention! In the case of authorization, this computer will be available for viewing by TrustServer administrators, incl. uncontrolled access to this computer will be possible (provided that the administrators have the necessary rights).

4.2.3 Configuring the distribution package of the «TrustViewerPro» client module

You can change the settings of some installation options directly in the distribution package, using any editor msi-installer, for example, using the standard utility “Orca”, which is part of the “Windows SDK Components for Windows Installer Developers”. For example, to specify the server address: open the original distribution file “TrustViewerPro.msi” using “Orca”, find the "INSTALLSERVER” setting and set the “default” value to the address of your server.


TrustViewerPro.msi - Orca
File Edit Tables Transform Tools View Help

Tables
AdminExecuteSequence
AdminUISequence
AdvtExecuteSequence
Component
CustomAction
Directory
Feature
FeatureComponents
File
Icon
InstallExecuteSequence
InstallUISequence
Media
Property
_Validation

Property	Value
INSTALLSERVER	youservername.com:8443
INSTALLFLAGS	default
ARPURLINFOABOUT	www.trustviewer.com
ARPPRODUCTICON	MainIcon.ico
ARPSIZE	3
ARPNOMODIFY	0
Manufacturer	TrustViewer
ProductCode	{6ACADD67-B767-466C-BB68-81D32401DC86}
ProductLanguage	1033
ProductName	TrustViewerPro
ProductVersion	2.0.0
UpgradeCode	{D5B3798A-4B3B-4D6A-BD28-F3D5F3B90036}

Tables: 15
Property - 12 rows
Value - Localizable[0]

Attention! As part of branding, you can also change the application icon (the “Icon” table, the “MainIcon.ico” setting) and the display name of the application (in the “Files” table, for the “TrustViewerPro” entry, change the “FileName” field value, for example, to “MyApp .exe | MyApplication.exe”). For more information about branding options, see “Branding settings” in the “Administration of the TrustServer Server” section of this manual.

4.2.4 Installing the client module «TrustViewerPro» using the command line

Regardless of whether you are using the original distribution package of the TrustViewerPro client module or modified using the msi package editor, you can override the installation settings using the command line during the installation. MSI packages are installed by the system program “msiexec.exe”, thus, to install the client module distribution using the command line, use the syntax “msiexec.exe” with adding the necessary installation settings (to get help describing all available commands and installation modes - type i the command line “msiexec.exe / help”). The following are examples of installing the client module using the command line:

- “**msiexec.exe /i TrustViewerPro.msi INSTALLSERVER=192.168.1.10:8443**” – install the client module on the computer in the limited functionality mode, with the indication of the local address of the «TrustServer» server
- “**msiexec.exe /quiet /i TrustViewerPro.msi INSTALLFLAGS=6 INSTALLSERVER=Test:123456@youservername.com:8443**” – install the client module on the computer in quiet mode (“**/quiet**”), only for one computer user (“**INSTALLFLAGS=6**”), with authorization of the computer on the server “**youservername.com:8443**” with the login “**Test**” and password “**123456**” (mode of full functionality of the client module)
- “**psexec \\«computer» -u «domain\username» -p «password» cmd /c «msiexec /i /quiet /norestart TrustViewerPro.msi INSTALLSERVER=192.168.1.10:8443»**” – install the client module over the network in the domain structure (here **«computer»**

is the name of the computer on the network, **«domain\username»** is the domain name / user name, **«password»** is the user password)

Attention! Uninstalling the client module can also be performed using the command line, and this can be done using the product identifier without the TrustViewerPro.msi file. For example, the “**msiexec / quiet / uninstall {6ACADD67-B767-466C-BB68-81D32401DC86}**” command will perform an uninstall in silent mode. Moreover, if you add the parameter “UNINSTALLMODE=partial”, it will be partially uninstalled without removing personal settings.

4.2.5 Running of the portable version of the «TrustViewerPro» client module

The TrustViewerPro client module supports portable mode (i.e. without installation on the computer), but, its functionality will be limited. Moreover, if the TrustViewerPro client module and the TrustServer server are located in a common local network, it is enough to simply run the file “TrustViewerPro.exe” and all settings will be received from the server automatically. Otherwise, for example, if the TrustViewerPro client module connects to the TrustServer server over the Internet, then after running the file “TrustViewerPro.exe” – it is necessary in the network settings of the program to specify the server address: open the menu advanced network settings (“Menu” → “Settings” → “Connections” → “TrustServer”), uncheck “Automatic server detection” and enter in the fields “Server” and “Port” respectively, the values of the host and port of the server TrustServer.

4.2.6 Setting up the operation of «TrustViewer» in compatibility mode with «TrustViewerPro»

The TrustViewer program can be configured to work in the TrustViewerPro compatibility mode – it is enough to specify the address of the TrustServer server in the network settings, and select it as a coordinating server (respectively, the "Server” and “Port” fields, as well as the "Use TrustServer as a coordinating server” checkbox on the “Menu" → “Settings” → “Connections” → “TrustServer”). In this case, some settings, such as branding settings – will be downloaded from the server automatically, however, in this case, the operator mode for the TrustViewer client module will not be available.

4.2.7 Configuring a stand-alone client module for instant remote support

The TrustViewerPro client module, as well as the TrustViewer program, support a special portable mode of operation to provide instant support immediately after downloading the executable file from the Internet, without the need for preliminary configuration. The preferred option is to use your own branded distributions (see the paragraph “Generation of your own distributions signed by the developer's EDS”, in the “Administration of the TrustServer” section of this manual).

An alternative option is to use special public URL links, the part name of which indicates the address of the coordinating server of the organization "TrustServer". If the external port and hostname of the TrustServer server are correctly specified in the startup parameters (for parameters –whost and –wport, see “Installing TrustServer server” for details), then download distribution links TrustViewer and TrustViewerPro will be created automatically and indicated on the “Settings” -> ”General” tab of the server control panel (also, in the “Portable client name” field, here you can specify the name of the program that will be displayed at startup). For example, if you specified the external port and server host name as “myserver.com:443”, then the links to the TrustViewer and TrustViewerPro distributions will be “http://trustviewer.com:443/client/TrustViewerQS_myserver.com_443.exe” and “http://trustviewer.com:443/pro/TrustViewerQS_myserver.com_443.exe”.

Similarly, you can place any versions and distributions on your own servers, just rename the required executable file as “TrustViewerQS_myserver.com_443.exe”.

4.2.8 Running and installing the "TrustViewerPro" client module in the GNU/Linux operating system

Currently, a beta version of the distribution of the client module "TrustViewerPro" with support for the "X Window System" is available for the GNU/Linux operating system on the x86_64 platform. The beta version of the client module for GNU/Linux works in a limited functionality mode, in particular, there is no user interface for changing program settings, so it is recommended to set the connection settings to the coordinating server of the TrustServer organization when generating your own branded distributions. An alternative way to specify the connection settings to the "TrustServer" server is to use special public URL links (see the previous paragraph of this guide), or explicitly specify the parameters when installing the client module using the command line. If the mode of full functionality of the client module was selected, then after its installation it is possible to change all program settings remotely (see the item "Group sending of messages and commands /scripts/settings" in the section "Working with the client module "TrustViewerPro"" of this manual).

An autonomous client module (obtained using special public URL links, or when generating its own branded distributions) is a binary executable file in ELF format that can be run on the user's computer immediately after downloading, and provide access to the computer by ID, without prior configuration and installation.

Attention! To ensure full remote control of the computer, the libraries “**libxinerama-dev**” and “**libxtst-dev**” must be installed in the system.

To install the program on a computer, it is necessary to run an autonomous client module on behalf of a super-user using the command line, specifying the mandatory “install” parameter, as well as, if necessary, additional installation parameters, for example:

- “**sudo ./TrustViewerPro install**” – install the client module on the computer in the limited functionality mode, with default settings
- “**sudo ./TrustViewerPro install Server=youservername.com:8443 InstallForAllUsers=False**” – install the client module on the computer in the limited functionality mode, with the authorization of the computer on the server “**youservername.com:8443**”, only for one computer user (“**InstallForAllUsers=False**”)
- “**sudo ./TrustViewerPro install Server=Test:123456@youservername.com:8443 Dir=/srv/myapp**” – install the client module on the computer, in the folder “**/srv/myapp**” with the authorization of the computer on the server “**youservername.com:8443**” with the login “**Test**” and password “**123456**" (the mode of full functionality of the client module)

The following is a list of installation parameters available for passing as parameters on the command line:

Параметр	Описание
SERVER=<value>	Sets the server address, as well as credentials for authorizing a computer on the server, in the format “login:password@host:port”, where “login:password” respectively the login and password of a group account, and “host:port” is the address of the TrustServer server .
DIR=<value>	Specifies the destination folder where the client module will be installed
InstallForAllUsers= <True/ False>	Sets the flag for program installation for all users (if this parameter is not specified, it is assumed that this option is enabled)
AddIconToDesktop= <True/ False>	Sets the flag for adding an icon to the desktop (if this parameter is not specified, it is assumed that this option is enabled)
AddIconToStartMenu= <True/ False>	Sets the flag for adding an icon to the Start menu (if this parameter is not specified, it is assumed that this option is enabled)

Attention! The client module is also uninstalled using the command line, “**sudo ./TrustViewerPro uninstall**”

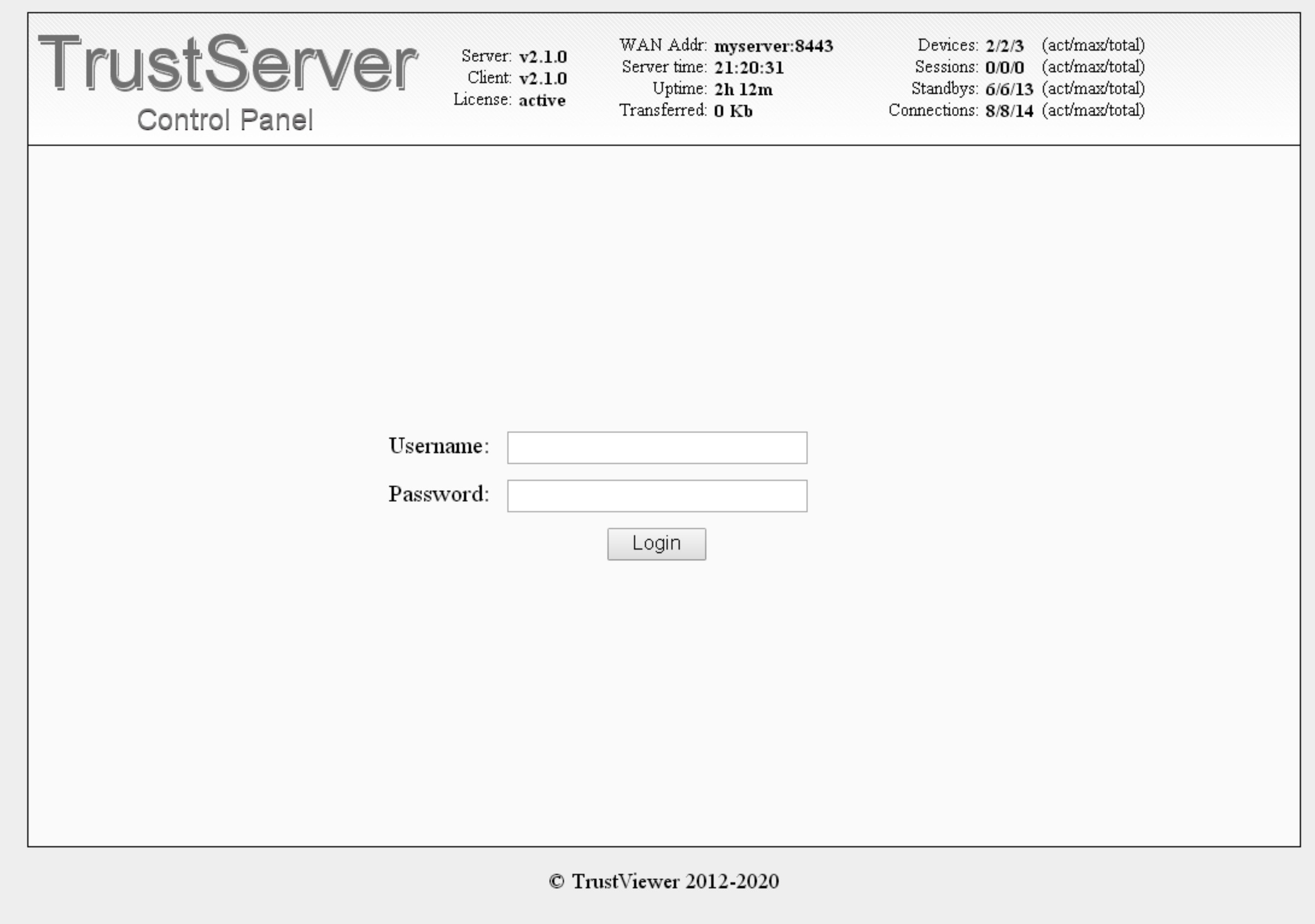
5. Administration of the «TrustServer» server

After installation and initial setup of the server (see the item “Configuring the TrustServer server after installation”, in the “Installation” section of this manual), using the server control panel it is possible to solve the following administrative tasks:

- management of rights and settings of registered users
- management of authorized computer settings
- server settings management

5.1. Server Status Information

Basic information about the status of the server online - you can get on any page of the server control panel, including the authorization page.



Server: v2.1.0
Client: v2.1.0
License: active

WAN Addr: myserver:8443
Server time: 21:20:31
Uptime: 2h 12m
Transferred: 0 Kb

Devices: 2/2/3 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 6/6/13 (act/max/total)
Connections: 8/8/14 (act/max/total)

© TrustViewer 2012-2020

The following is a list of server status options:

Option	Description
Server	Current server version
Client	Current client version
License	License Status: • “active” – license is active • “check” – waiting for license activation online • “wait” – waiting for license activation offline • “error” – activation error
WAN Addr	Declared public server address
Server time	Current server time

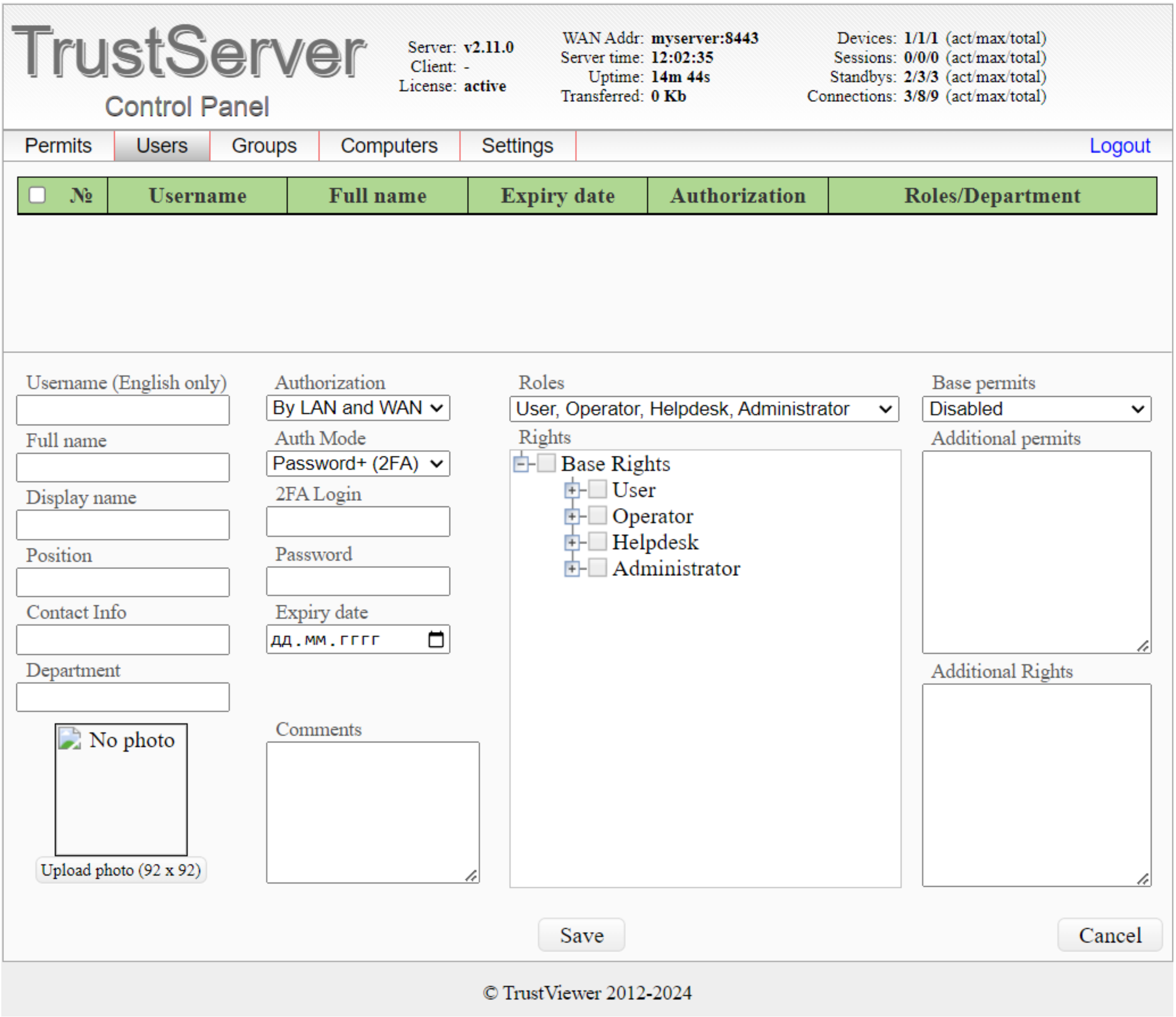
Uptime	Current server uptime
Transferred	Current size of transmitted data in proxy mode
Devices	Information about connected online devices: • “act” – the current number of active online devices • “max" – the maximum number of simultaneously active online devices during server operation • “total” – the total number of different active online devices during server operation
Sessions	Information about the data transfer channels in the proxy server mode: • “act” – the current number of active data channels • “max" – the maximum number of concurrentlyactive data transfer channels during server operation • “total” – total number of active channels during server operation
Standbys	Information about data transmission channels in the coordinating server mode: • “act” – the current number of active data channels • “max" – the maximum number of concurrently active data transfer channels during server operation • “total” – total number of active channels during server operation
Connections	Information about server connections at the socket level: • “act” – current number of active connections • “max" – the maximum number of concurrently connections during server operation • “total” – total number of connections during server operation

5.2. User management

User accounts are primarily used for personal authorization when working with the client module “TrustViewerPro”, in particular, provided that they have the necessary rights, they allow you to connect to remote computers. In addition, user accounts, if they have the necessary rights, are used to access the control panel of the “TrustServer” server.

5.2.1. Editing user profiles

To add a new user, go to the “Users” tab and click the “Add new user” button, then the profile form will open. Fill in the fields and click the “Save” button to save the profile settings (if there are empty / incorrect required fields, the saving procedure will be interrupted, and the fields themselves will be highlighted in red). After adding a new user - you can continue editing his profile later: go to the “Users” tab and left-click on the required account - the profile form will open with the ability to change settings (here you can copy the profile under a different name, for this click “Copy User” button). To delete a user: go to the “Users” tab, tick the required profile and click the “Delete selected” button.



TrustServer
Control Panel

Server: v2.11.0
Client: -
License: active

WAN Addr: myserver:8443
Server time: 12:02:35
Uptime: 14m 44s
Transferred: 0 Kb

Devices: 1/1/1 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 2/3/3 (act/max/total)
Connections: 3/8/9 (act/max/total)

Permits
Users
Groups
Computers
Settings
Logout
☐ № | Username | Full name | Expiry date | Authorization | Roles/Department

Username (English only):
Full name:
Display name:
Position:
Contact Info:
Department:
Authorization: By LAN and WAN
Auth Mode: Password+ (2FA)
2FA Login:
Password:
Expiry date: дд.мм.гггг
Comments:
Roles: User, Operator, Helpdesk, Administrator
Rights:
- ☐ Base Rights
  - ☐ User
  - ☐ Operator
  - ☐ Helpdesk
  - ☐ Administrator

Base permits: Disabled
Additional permits:
Additional Rights:

The following is a list of profile options available for editing:

Option	Description
Username	Unique user login (only in English). This field is required.
Full name	Username. This field is required.
Display name	Username displayed when connected to a remote computer. This field is required.
Position	The user's position is displayed after the end of the communication session with the remote computer. This field is optional.
Contact Info	Arbitrary user contact information is displayed after the end of the communication session with the remote computer. This field is optional.
Department	The name of the department to which the current user belongs. This field is optional.
Authorization	Authorization user rights: • “Disabled (Block User)” – authorization is prohibited (user is blocked) • “By local network only” – authorization is allowed only in the local network • “Both LAN and WAN” – authorization is allowed on the local network and via the Internet • “Super admin” - the user is allowed full access to the server control panel

Auth Mode	Authorization mode: • “Password only” – password authorization • “Cert only” – authorization using a certificate • “Password+ (2FA)” – two-factor authentication (password + confirmation code) • “Cert+ (2FA)” – two-factor authorization (certificate + confirmation code)
Cert	Authorization User Certificate.
2FA Login	User login to send an authorization code (for example, email address or messenger ID).
Password	User Password. This field is required.
Expiry date	The expiration date of the password. This field is optional (leave this field blank to set a password indefinite).
Photo	Sets the user avatar displayed in the client module upon connection. To load a photo, click the “Load photo” button, to delete it, click the “Delete photo” button. This field is optional.
Comments	Comments. This field is optional.
Roles	Rights groups allowed for the user: • User • User, Operator • User, Operator, Helpdesk • User, Operator, Helpdesk, Administrator
Rights	User rights (for a full list of user rights, see in the table below)
Base permits	Template with basic permissions for the current user to access departments / computers (for more information on setting up templates for basic permissions, see the “Permissions to access departments / computers” section, in the “Administration of the TrustServer Server” section of this manual). This field selects one of the templates specified on the “Permits” tab of the server control panel. The value “Disable” means that only the permissions specified in the “Additional permits” field will be applied to the current user.
Additional permits	Additional permissions for access to departments / computers (permissions specified in this field will be added to the permissions specified in the “Base permits” field). If no basic or additional permissions are specified for the user, then the current user will be granted permissions without restrictions (for more information on setting permissions, see “Permissions to access departments / computers” in the “Administration of the TrustServer Server” section of this manual).
Additional rights	Additional user rights (for more information on setting up templates for basic permissions, see the “Additional user rights” section, in the “Administration of the TrustServer Server” section of this manual).

Below is a list of user rights that can be edited:

Option	Description
User	Basic rights of an authorized user • "Use contacts" - allows you to create secure contacts. • "Remote workplaces access (RDP)” – allows connections to remote workplaces over the RDP Protocol. • "View own recordings" - allows you to upload your own session recordings from the server.
Operator	Operator rights to access remote computers on request • "Audio call" - allows audio calls. • The “Video call” – allows video calls. • "Demonstration own desktop” - allows demonstration of your desktop • "View remote desktop” - allows viewing the remote desktop

	• “Mouse/keyboard control” – allows the management of remote desktop • "Full access” - allows full access to the remote computer ○ “Full Clipboard access” – full access to the clipboard ○ “Full File access” – full access to the file system • “Uncontrolled access” – allows uncontrolled access to a remote computer using secure contacts.
Helpdesk	Helpdesk operator rights • “1st support line” – allows accepting applications from users within the 1st helpdesk line • “2nd support line” – allows you to connect to users with operator rights using application tickets within the 2nd helpdesk line
Administrator	Network administrator rights • “View recordings” – allows access to recordings and broadcasts ○ “Recordings of own department” – access to recordings and broadcasts within your Department ○ “Recordings of permitted departments” access to recordings and broadcasts within permitted departments ○ “All recordings” - access to all recordings and broadcasts • “Connections to users on request” – allows access to computers on the network on request, with operator rights • “Administration of computers” - allows access to computers on the network without a request ○ “Desktop access”->”View” – view the desktop ○ “Desktop access”->”Control” – desktop control ○ “Files access”->”Read” – access to files for reading ○ “Files access”->”Write” – access to files for writing • “Sending messages and commands” – allows sending commands and messages to computers on the network ○ “Sending messages to users” – sending messages to users ○ “Sending commands to users” – sending and executing commands on behalf of users ○ “Sending commands to computers” – sending and executing commands on behalf of the system account ○ “Sending WOL” – sending a “Wake on LAN” command to computers • “Sending settings” – allows sending program settings to computers on the network ○ “Connections” – settings on the “Connections” and “Additionally” tabs ○ “TrustServer” – settings on the "TrustServer" tab ○ “Access” – settings on the “Access to this computer" tab ○ “Security” – settings on the "Security" tab ○ “Enable remote settings” – setting "Allow remote modification of program settings” on the “Security" tab” • “Editing computer cards” – allows editing computer cards

5.2.2. Permissions to access departments / computers

Permissions to access departments / computers allow you to specify groups or individual computers that are allowed to access for a given user within his base rights. If permissions are not explicitly set, it is considered that the user is allowed access to all computers, but only within his rights. For example, if the permissions are not explicitly set (and, accordingly, the user is allowed access to all computers), but the user does not have network administrator rights, then this user will not be able to access the computers on the network.

In general, permissions are written as a sequence of rules (one line - one rule), divided into groups by the access rights. In this case, for one sequence of rules several groups can be specified at once, separated by a comma. In addition, if no group is specified for the first rule sequence, then these rules (before the start of the next group) will be applied to all groups of access rights at once. It is also allowed to insert comments anywhere in the text after the characters ***//*** (any text to the end of the line will be considered a comment).

```
// Comment_1
Rule_1
Rule_2
...
Rule_n

<Group_1_name> // Comment_2
Rule_1
Rule_2
...
Rule_n

<Group_name_2>, <Group_name_3>, ... <Group_Name_N>
Rule_1
Rule_2 // comment_3
...
Rule_n

...

<Group_name_n>
Rule_1

Rule_2

...
Rule_n
```

The group name can have the following values:

Group name	Description
<Network>	Rights to access remote computers on the network on demand (corresponds to the “Connections to users on request” permissions of the “Administrator" rights group)
<Admin>	Rights to uncontrollable access to remote computers on the network (corresponds to the “Administration of computers” permissions of the “Administrator” rights group)
<RDP>	Rights for private access to computers on the network via the RDP protocol (corresponds to the “Remote workplaces access (RDP)” permissions of the “Administrator” rights group)
<Helpdesk>	Access rights to helpdesk requests (corresponds to the permissions of the “Helpdesk" rights group)
<Settings>	Access rights to computer settings in the server control panel (corresponds to the “Sending settings” permissions of the “Administrator" rights group)
<Recordings>	The right to view recordings of communication sessions (corresponds to the “Recordings of permitted departments” permissions of the “Administrator" rights group)

There are two possible types of rules: “Allow access” and “Deny access”. The rule type defines the first special character in the rule entry line: “**+**” - “Allow access”, “!” Or “**-**” - “Deny access”.

Moreover, if a special character is not specified, it is considered that the type of such a rule is “Allow access”. After the special character, the scope of the rule is specified, which can take the following values:

Recording format	Description
*	Access to all computers (for the current group of access rights)
DepartmentName	Access to a group of computers by department name, where DepartmentName is the full or partial name of the department.
“LabelName”	Access to a computer (group of computers) by the label name, where LabelName is the full name of the computer label.
[MAC]	Access to a computer by its MAC address, where MAC is the MAC address of the computer.
ActiveDirectory	Access to computers belonging to AD (within their AD administrator rights), where ActiveDirectory is a reserved name (identifiers with this name, including the name of departments, are prohibited).

When specifying the name of a department in the properties of a computer, the composite name of the department, consisting of sub-departments separated by a dot is allowed, of the general form “Branch_1.Section_1. Subdivision_1 .. Subdivision_N”. Moreover, a partial indication of the name of the department in the scope of the rule is allowed, for example, here the format of the entry “Branch_1. Department_1.” Will mean access to all computers of the department “Division_1” of the branch “Branch_1”. Also, a partial indication of the department name is allowed, using the mask symbol “*”, for example, here the recording format “* Division_1. *” Will mean access to all computers of the department “Division_1” in all branches.

Consider the examples of permissions for access to computers located in different departments and branches (for a user who has all the necessary rights). For example, we have 3 branches (“Moscow”, “London”, “Beijing”), 3 departments in each branch (“Accounting”, “Secretariat”, “ACS”), two terminal servers (“Terminal_1”, “Terminal_2”) from the subgroup “Servers.Terminal”, 1 file server (“Exchange_1”) from the subgroup “Servers.Exchange”, and 9 workstations with the following description:

Label (“Label” field)	MAC address (“MAC” field)	Department / Group (Department field)
Computer_1	00-00-00-00-00-01	Moscow.Accounting
Computer_2	00-00-00-00-00-02	Moscow.Secretariat
Computer_3	00-00-00-00-00-03	Moscow.ASU
Computer_4	00-00-00-00-00-04	London.Accounting
Computer_5	00-00-00-00-00-05	London.Secretariat
Computer_6	00-00-00-00-00-06	London.ASU
Computer_7	00-00-00-00-00-07	Beijing.Accounting
Computer_8	00-00-00-00-00-08	Beijing.Secretariat
Computer_9	00-00-00-00-00-09	Beijing.ASU
Terminal _1	00-00-00-00-00-A1	Servers.Terminal
Terminal _2	00-00-00-00-00-A2	Servers.Terminal
Exchange_1	00-00-00-00-00-A3	Servers.Exchange

Example 1. Allow access with all rights to all computers in the branch “Moscow”:

```
Moscow.
```

Example 2. Allow access with all rights to all computers on the network except the “Accounting” department:

```
*                    // This rule gives access to all computers.
!*.Accounting* // Excludes computers included in the “Accounting” subgroup
```

Example 3. Allow access with all rights to all computers on the network, except servers:

- Method 1 (the most optimal)

  ```
  *
  !Servers
  ```

- Method 2 (suitable only if new server groups are not added in the future)

  ```
  *
  // Enumerate server subgroups to exclude
  !Servers.Terminal
  !Servers.Exchange
  ```

- Method 3 (suitable only if no new servers are added in the future)

  ```
  *
  // Enumerate the labels of the computers to be excluded.
  !”Terminal_1”
  !“Terminal_2”
  !“Exchange_1”
  ```

- Method 4 (suitable only if no new servers are added in the future)

  ```
  *
  // Enumerate the MAC addresses of the computers to be excluded
  ![00-00-00-00-00-A1]
  ![00-00-00-00-00-A2]
  ![00-00-00-00-00-A3]
  ```

- Method 5 (suitable only if there are no new departments added in the future)

  ```
  // List the departments that need to be resolved
  Moscow.
  Lonnon.
  Beijing.
  ```

- Method 6 (the most non-optimal)

  ```
  // Enumerate the subdivisions, labels and MAC addresses that need to be resolved
  Moscow.Accounting
  Moscow.Secretariat
  Moscow.ASU
  “Computer_4”
  “Computer_5”
  “Computer_6”
  [00-00-00-00-00-07]
  [00-00-00-00-00-08]
  [00-00-00-00-00-09]
  ```

Example 4. Allow access to all computers on the network, with all rights except the right of uncontrolled access:

```
* // This rule gives access to all computers for all groups of access rights.
<Admin> // Rights group for uncontrolled access
```

```
!* // This rule excludes all computers for the current group
```

Example 5. Allow access to all computers in the network with RDP only:

```
!* // This rule excludes access to all computers for all groups of access rights
<RDP> // Group of rights for private access via the RDP protocol
* // This rule gives access to all computers for the current group.
```

Example 6. Allow access only to terminal servers and only with private access rights via the RDP protocol:

```
<RDP> // Group of rights for private access via the RDP protocol
Servers.Terminal // Access to all terminal servers for the current group
```

Example 7

- Allow RDP access to the terminal server with the label “Terminal _1” and the workstation with the MAC address “00-00-00-00-00-04”
- Allow access with rights to view all computers on the network, except servers (with the exception of the “Exchange_1” server, to which you also allow access)
- Allow access to applications of the 1st support line received from all departments, except for the ACS department, from all branches, except for the London branch
- Allow uncontrolled access, as well as the ability to manage settings of computer in the server control panel, for all computers of the Moscow branch, except for the computer labeled “Computer_3”

```
<RDP>
“Terminal _1”
[00-00-00-00-00-04]

<Network>
*
!Servers
“Exchange_1”

<Helpdesk>
*
!*. ACS*
!London

<Admin>, <Settings>
Moscow
! ”Computer_3”
```

Attention! Permissions for a specific user consist of the basic permissions specified in the template and additional permissions specified in the user profile. Moreover, additional permissions have a higher priority than base ones, i.e. Additional permissions can not only supplement the base permissions, but also cancel them.

Example 8. To prohibit uncontrolled access to the “ACS” department on the basis of a template in which uncontrolled access to all computers of the “Moscow” branch is provided:

- Basic permissions specified in the template

```
<Admin>
Moscow
```

- Additional permissions for user

```
<Admin>
!*.ACS*
```

Example 9. Allow the operator access only to computers belonging to AD (within their AD administrator rights):

```
ActiveDirectory
```

Example 10. Allow the operator access only to computers belonging to AD (within their AD administrator rights) and also to all accounting computers located in Moscow:

```
ActiveDirectory
Moscow.Accounting
```

Example 11. Allow the operator access on request to all computers, and allow full access only to computers belonging to AD (within their AD administrator rights):

```
<Network>
*

<Admin>
ActiveDirectory
```

5.2.3. Additional user rights

Additional user rights allow you to specify groups or individual computers that are allowed access with rights other than the basic ones (additional root nodes that are editable are added to the rights tree).

In general, permissions are written as a sequence of rules (one line - one rule. It is also possible to insert comments anywhere in the text after the // characters (any text to the end of the line will be considered a comment). In this case, each rule will be presented in the tree rights by a separate node available for editing. In addition, using the characters “<>” rules can be combined into named groups, in this case each group will be represented in the rights tree by a separate node available for editing.

```
// Comment_1
Rule_1
Rule_2

<Group_1>
Rule_3
Rule_4

…
Rule_N
```

The syntax of additional user rights is a simplified version of the syntax for permissions to access departments / computers: here you can also specify a group of computers by the name of the department, or specify individual computers by the name of the label or MAC address, but special groups cannot be used here (<Network>, ... <Recordings>).

Example 1. Add to the rights tree an additional node “Moscow.” (at the same time, access to all computers included in the Moscow branch for this user will be determined by these rights, and not basic):

```
Moscow.
```

Example 2. Add an additional node “My servers” to the rights tree that sets the same rights for two selected computers:

```
<My servers>
“Terminal _1”
[00-00-00-00-00-A2]
```

Attention! For a given user, rights from only one root node can be assigned to each of the computers on the network. Moreover, in the tree of rights, the highest priority is for the most recent (lower) node.

Example 3. Add two additional nodes “Moscow.” To the rights tree and “Computer_1”, at the same time, the rights from the “Computer_1” node will be assigned for the computer “Computer_1”, the rights from the “Moscow.” node will be assigned for other computers belonging to the Moscow branch, for all remaining computers the basic ones will be applied rights from the Base Rights node:

```
Moscow.
“Computer_1”
```

Attention! Additional rights apply only to authorized departments / computers. This property can be used for flexible setting of rights together with access permissions.

Example 4. Allow the user access to computers in the departments "Moscow.ACS", "Moscow.Accounting", "London.ACS", while for all computers located in the branch "Moscow" to determine special rights that are different from the basic ones:

- Permissions (“Additional permissions" field)

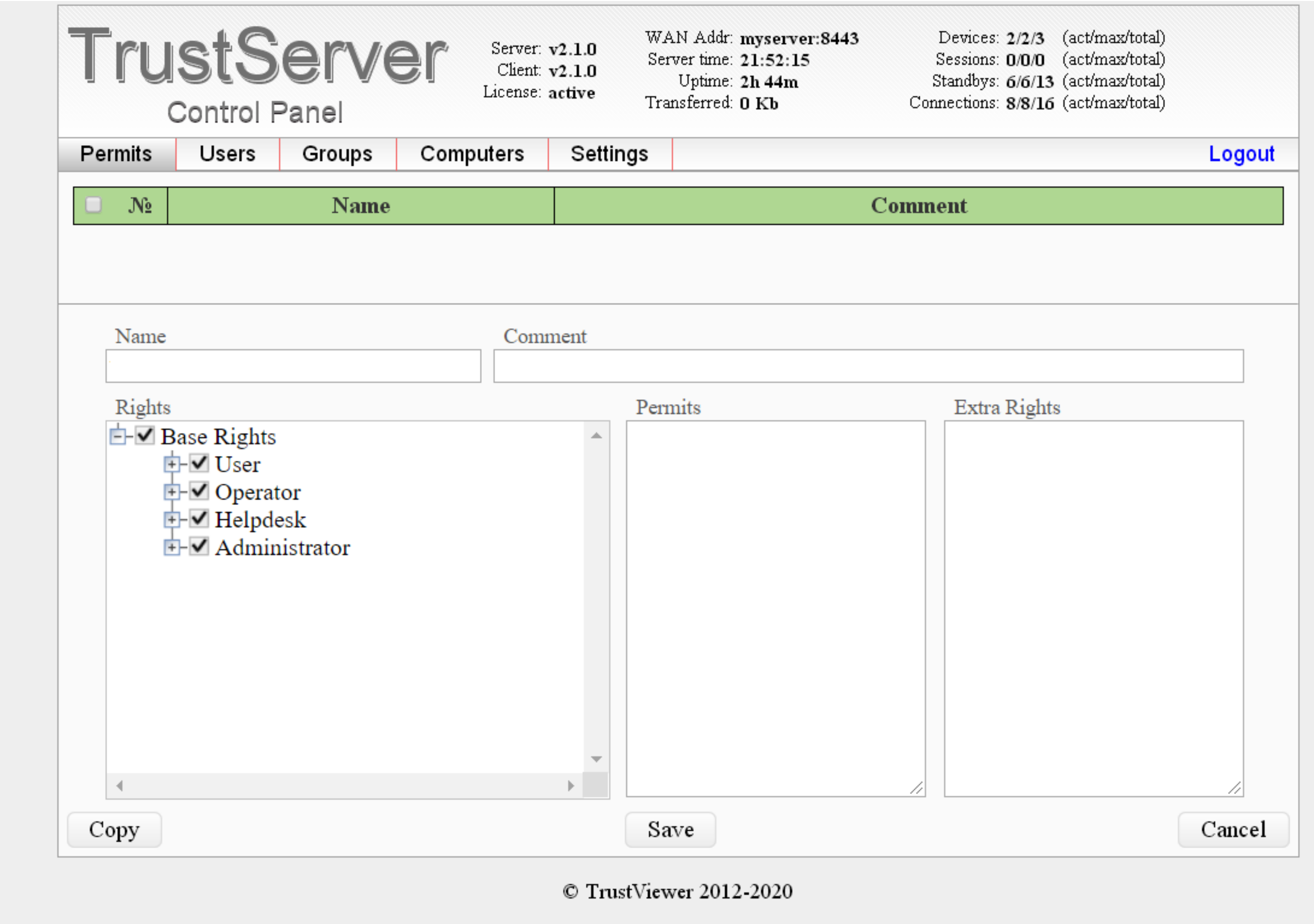
  ```
  <Admin>
  Moscow.ACS
  Moscow.Accounting
  London.ACS
  ```

- Additional rights

  ```
  Moscow.
  ```

5.2.4. Permitted Divisions/Computers Templates

To add a new template for permitted departments / computers, go to the “Permits” tab and click the “Add” button, after which the template form will open. Fill in the fields and click the “Save” button to save the template settings (if there are empty / incorrect required fields, the saving procedure will be interrupted, and the fields themselves will be highlighted in red). After adding a new template - you can continue editing it later: go to the “Permits” tab and left-click on the desired entry - the template form will open with the ability to change settings (here you can copy the template under a different name, to do this, click “Copy”). To delete a template: go to the “Groups” tab, tick the required template and click the “Delete selected” button.



Server: v2.1.0
Client: v2.1.0
License: active

WAN Addr: myserver:8443
Server time: 21:52:15
Uptime: 2h 44m
Transferred: 0 Kb

Devices: 2/2/3 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 6/6/13 (act/max/total)
Connections: 8/8/16 (act/max/total)

☐ №	Name	Comment

- ☑ Base Rights
  - ☑ User
  - ☑ Operator
  - ☑ Helpdesk
  - ☑ Administrator

The following is a list of template options available for editing:

Option	Description
Name	The name of the template. This field is required.
Comment	Comment.
Rights	Base rights.
Permits	List of permissions.
Extra Rights	Additional rights.

5.2.5. Importing user accounts

The first line of the file is an enumeration of the names of the columns, the subsequent lines are the enumeration of the values of the corresponding columns, and the order and number of columns are arbitrary, but the “UserName” column must be present. Both columns and values are separated by either a comma (,) or a semicolon (;). The value can be enclosed in double quotes (“), in which case it can contain characters (,)(;), and if you need to insert a double quote character inside the value, then it must be supplemented with a second double quote (for example, the text ***This "Text" in quotation marks!*** should be written as ***"This ""Text"" in quotation marks!"***).

Attention! If there is only one value in the file line corresponding to the “UserName” column, then such a user will be deleted.

The examples below are identical in terms of results:

- 1)

```
UserName;FullName;DisplayName
Aleks;Aleks B.;Aleks (Admin)
```

- 2)

```
UserName;DisplayName;FullName
Aleks;Aleks (Admin);Aleks B.
```

- 3)

```
UserName;FullName;DisplayName;Position;ContactInfo
Aleks;Aleks B.;Aleks (Admin)
```

- 4)

```
UserName;Position;ContactInfo;FullName;DisplayName
“Aleks”;;;”Aleks B.”;”Aleks (Admin)”
```

All available column names are listed below:

Option	Description
UserName	Unique user login (only in English).
FullName	Username.
DisplayName	Username displayed when connected to a remote computer.
Position	The user's position is displayed after the end of the communication session with the remote computer.
ContactInfo	Arbitrary user contact information is displayed after the end of the communication session with the remote computer.
Department	The name of the department to which the current user belongs.
Comments	Comments.
AuthCB	Authorization user rights. Can take the following values: • “0” – authorization is prohibited (user is blocked) • “1” – authorization is allowed only in the local network • “2” – authorization is allowed on the local network and via the Internet • “3” – the user is allowed full access to the server control panel
Password	User Password. The value is written as an md5 hash.
ExpiryDate	The expiration date of the password. The value is written in the format yyyy-mm-dd
Photo	Sets the user avatar displayed in the client module upon connection. The value is written as a base64 string containing a binary file in .bmp format
RolesCB	Rights groups allowed for the user. Can take the following values: • “1” - User • “2” - User, Operator • “3” - User, Operator, Helpdesk • “4” - User, Operator, Helpdesk, Administrator
Rights	The value is written as a sequence of names separated by a comma, and if there is a “+” sign before the name, then the corresponding right is allowed, and if there is a “-” sign, then it is prohibited. The table below lists all

	available names.
BasePermits	Template with basic permissions for the current user to access departments / computers. The template name is specified on the “Permits” tab.
AddPermits	Additional permissions for access to departments / computers (permissions specified in this field will be added to the permissions specified in the “Base permits” field). The value is written as strings separated by a semicolon (;)
AddRights	Additional user rights. The value is written as group names separated by a semicolon (;), while a string with rights can be specified after the group name (similar to the “Rights” parameter)

Below is a list of names for the "Rights" column:

Option	Description
UserContacts	allows you to create secure contacts
UserRDP	allows connections to remote workplaces over the RDP Protocol
UserRecordings	allows you to upload your own session recordings from the server
OperatorAudioCall	allows audio calls
OperatorVideoCall	allows video calls
OperatorOwnDesktop	allows demonstration of your desktop
OperatorViewDesktop	allows viewing the remote desktop
OperatorControl	allows the management of remote desktop
OperatorClipboard	full access to the clipboard
OperatorFiles	full access to the file system
OperatorUncontrolled	allows uncontrolled access to a remote computer using secure contacts
Helpdesk1line	allows accepting applications from users within the 1st helpdesk line
Helpdesk2line	allows you to connect to users with operator rights using application tickets within the 2nd helpdesk line
AdminDepRecordings	access to recordings and broadcasts within your Department
AdminPerRecordings	access to recordings and broadcasts within permitted departments
AdminAllRecordings	access to all recordings and broadcasts
AdminUsers	allows access to computers on the network on request, with operator rights
AdminDesktop	Allows access to computers on the network without prompting in desktop view mode
AdminControl	Allows access to computers on the network without prompting in desktop control mode
AdminFilesRead	Allows access to computers on the network without prompting in read-only file access mode
AdminFilesWrite	Allows access to computers on the network without prompting in file-write mode
AdminUsersMessages	Allows sending messages to users
AdminUsersCommands	Allows sending and executing commands on behalf of users
AdminComputersCommands	Allows sending and executing commands on behalf of the system account
AdminComputersWOL	Allows computers to send wake-up commands (Wake on LAN)
AdminConnections	Allows computers on the network to send application settings on the “Connections” and “Advanced” tabs
AdminTrustServer	Allows sending the program settings on the “TrustServer” tab to computers on the network
AdminAccess	Allows sending to computers on the network application settings on the “Access to this computer” tab
AdminSecurity	Allows you to send the application settings on the Security tab to computers on the network
AdminRemoteSettings	Allows sending to computers on the network the setting of the “Allow remote change of application settings” parameter on the “Security” tab
AdminEditCards	allows editing computer cards

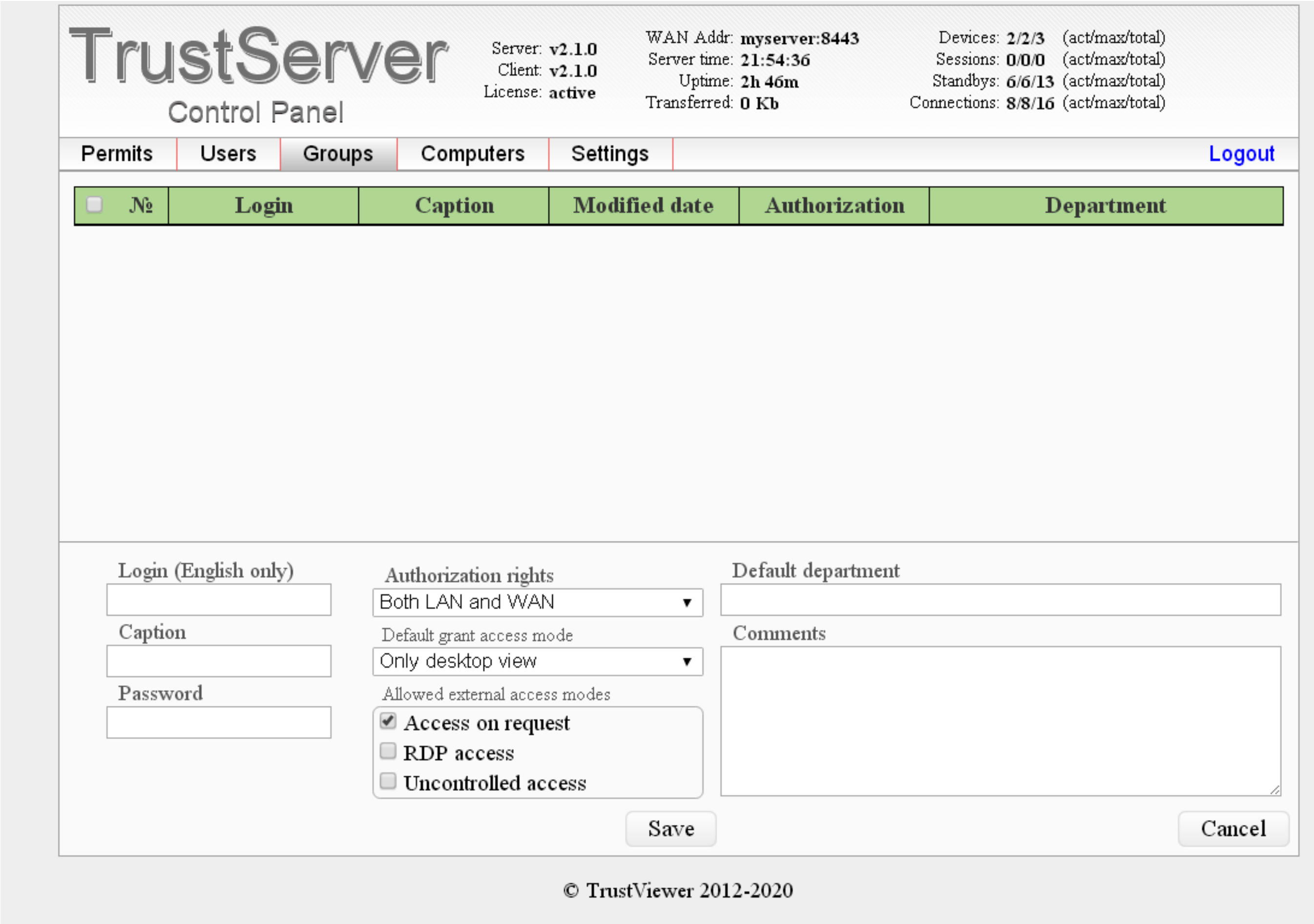
5.3. Computer Management

There are two possible modes of operation of the TrustViewerPro client module: in reduced functionality mode without authorizing a computer on the server (while computers are not displayed in the list on the server and, accordingly, are not available for management), and in full functionality mode - with authorization on the server (computers displayed in the list on the server and are available for management). Authorization of computers is carried out with the help of special group accounts in which initial settings of these computers are set. Moreover, after authorization, the settings settings specified in the group accounts can be overridden for each individual computer. Thus, we can conditionally distinguish two main strategies for setting up workstations:

- Minimum number of group accounts - workstations are conventionally divided into a small number of groups, for example, by the number of branches in cities. In this case, it is assumed that each newly authorized computer requires individual option parameter settings. This option can be handy with a decentralized server administration model: the administrator at the head office manages only group accounts (requires full administrator rights “TrustServer”), administrators at branches - controls only the settings of computers of their branch (the “Computers view only ”).
- Maximum number of group accounts - workstations are conventionally divided into a large number of groups, for example, not only by the number of branches in cities, but also by the number of departments in these cities. It is assumed that the individual configuration of computers after authorization is not required. This option can be handy with a centralized server administration model: “TrustServer” administration rights are available only to the administrator at the head office.

5.3.1. Editing group accounts

To add a new group account, go to the “Groups” tab and click the “Add” button, then the profile form will open. Fill in the fields and click the “Save” button to save the profile settings (if there are empty / incorrect required fields, the saving procedure will be interrupted, and the fields themselves will be highlighted in red). After adding a new group account, you can continue editing its profile later: go to the “Groups” tab and left-click on the required account — the profile form will open with the ability to change settings (here you can copy the profile under a different name, for press the “Copy” button. To delete a group account: go to the “Groups” tab, tick the required profile and click the “Delete selected” button.



Server: v2.1.0
Client: v2.1.0
License: active

WAN Addr: myserver:8443
Server time: 21:54:36
Uptime: 2h 46m
Transferred: 0 Kb

Devices: 2/2/3 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 6/6/13 (act/max/total)
Connections: 8/8/16 (act/max/total)

Login (English only)
Caption
Password

Authorization rights: Both LAN and WAN ▾
Default grant access mode: Only desktop view ▾
Allowed external access modes
☑ Access on request
☐ RDP access
☐ Uncontrolled access

Default department
Comments

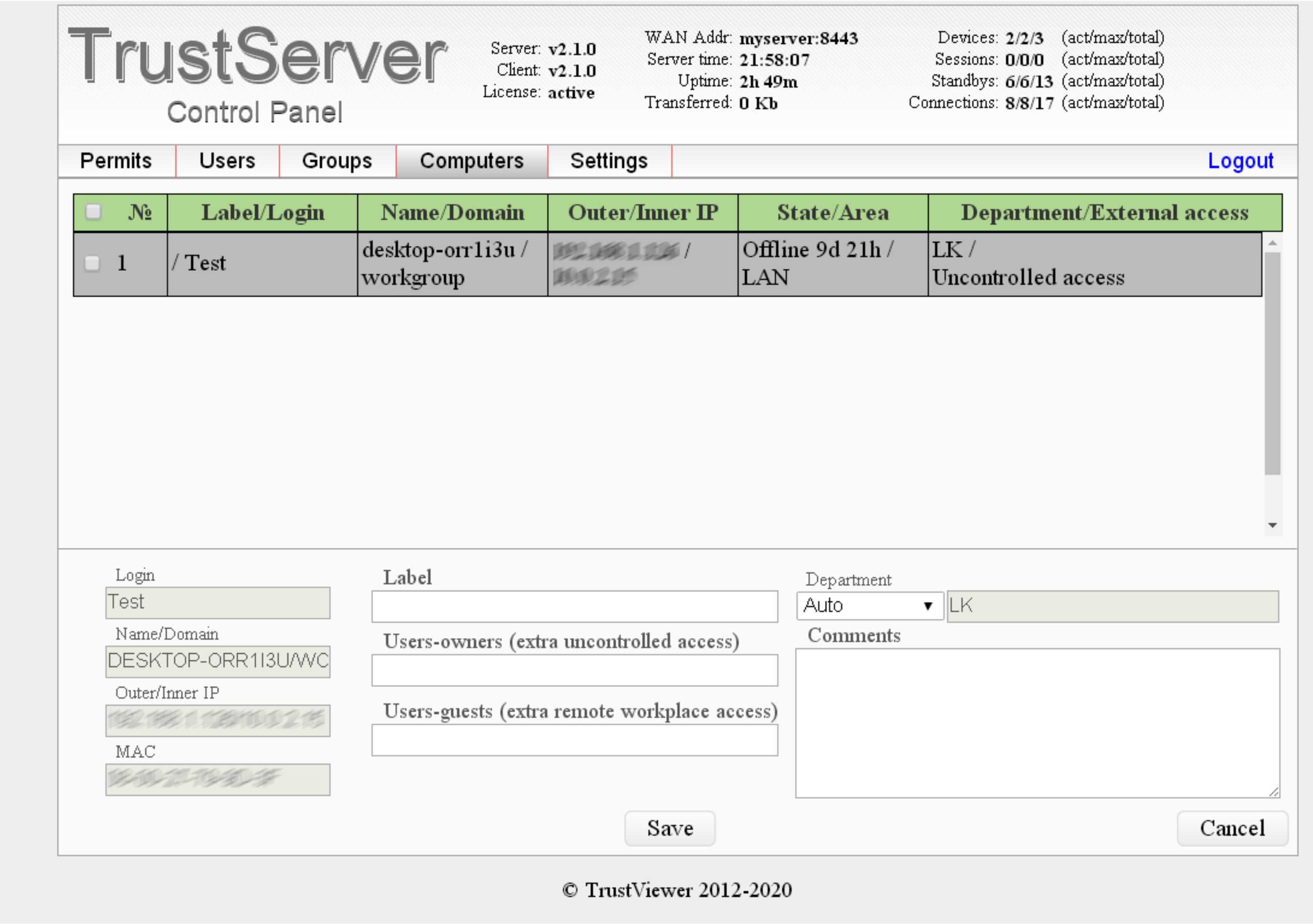
© TrustViewer 2012-2020

The following is a list of profile options available for editing:

Option	Description
Login	Unique account login (only English letters are allowed). This field is required.
Caption	Account name. This field is required.
Password	Account password This field is required.
Authorization rights	Authorization computer rights: • “Disabled (Block Computers)” – authorization is prohibited (all computers authorized with this account are locked) • “By local network only” – authorization is allowed only in the local network • “Both LAN and WAN” – authorization is allowed on the local network and via the Internet
Default grant access mode	The default access mode provided by the user to his computer (when connecting on request): • “Only desktop view (min rights)” – only desktop browsing is allowed • “Joint control” – both desktop view and joint control are allowed • “Unlimited access” – full access to the computer is allowed, including access to the clipboard and the file system without confirmation
Default external access mode	The authorized access modes for the authorized computer, initiated by the operator (this setting can be overridden in the computer card): • “Access on request” – access by request • “RDP access” – RDP access • “Uncontrolled access” – uncontrolled access
Default department	The name of the default department to which the computers authorized with this account belong (this setting can be overridden in the computer card)
Comments	Comments. This field is optional.

5.3.2. Editing computer cards

After authorization, the new computer automatically appears in the list of available computers on the server, with the Options specified by default in its group account. To customize computer settings, go to the “Computers” tab and left-click on the required entry - the computer card form will open with the ability to change settings. To remove unused computers from the list: go to the “Computers” tab, tick the required entry and click the “Delete selected” button.



Server: v2.1.0
Client: v2.1.0
License: active

WAN Addr: myserver:8443
Server time: 21:58:07
Uptime: 2h 49m
Transferred: 0 Kb

Devices: 2/2/3 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 6/6/13 (act/max/total)
Connections: 8/8/17 (act/max/total)

☐	№	Label/Login	Name/Domain	Outer/Inner IP	State/Area	Department/External access
☐	1	/ Test	desktop-orr1i3u / workgroup	[redacted] / [redacted]	Offline 9d 21h / LAN	LK / Uncontrolled access

Login: Test
Name/Domain: DESKTOP-ORR1I3U/WC
Outer/Inner IP: [redacted]
MAC: [redacted]
Label:
Users-owners (extra uncontrolled access):
Users-guests (extra remote workplace access):
Department: Auto ▾ LK
Comments:

© TrustViewer 2012-2020

Following is a list of computer card options available for editing:

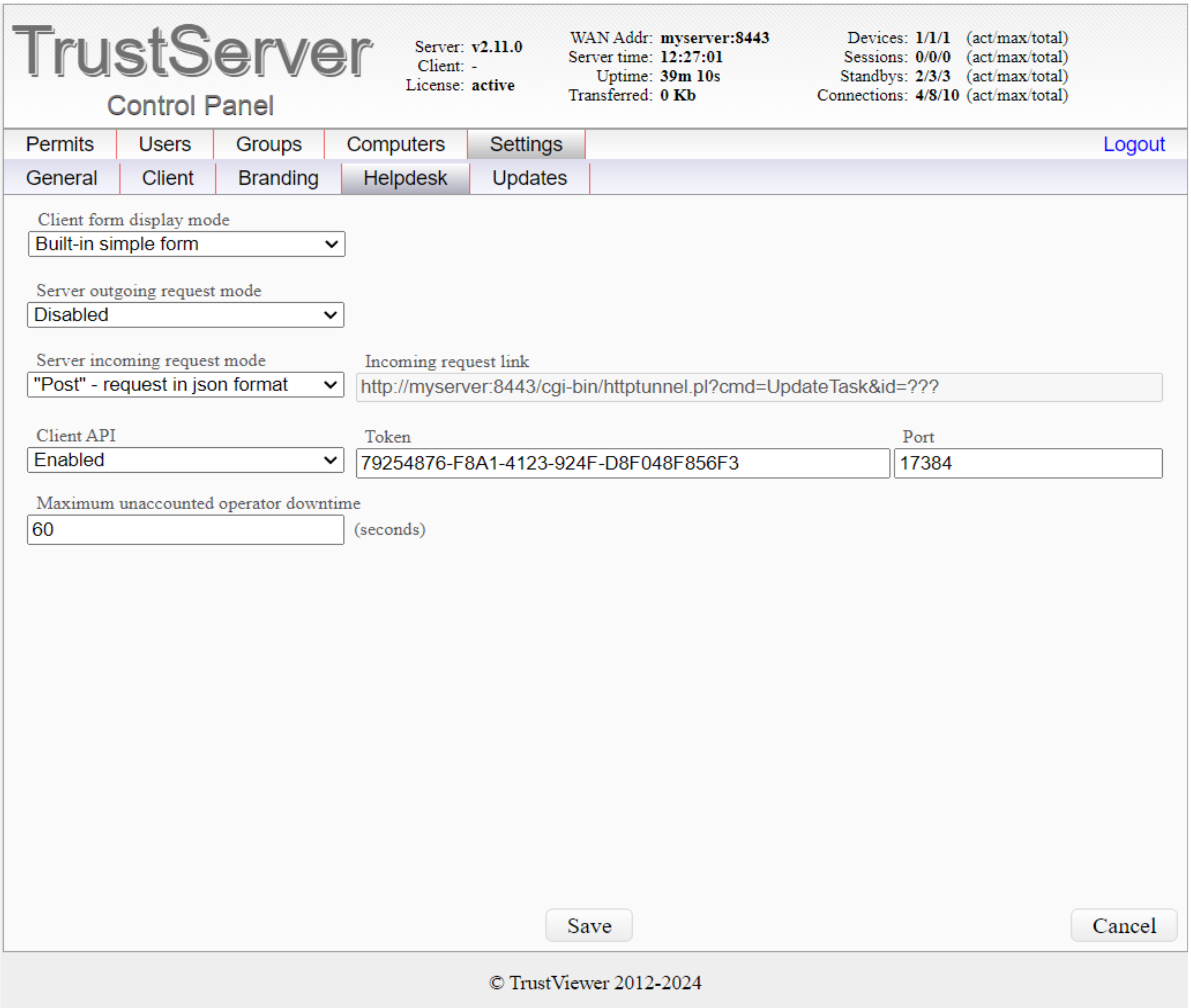
Option	Description
Label	Arbitrary computer tag (used to make computer identification easier)
Users-owners (extra uncontrolled access)	The list of users (user logins are specified, separated by commas), which provide uncontrolled access to this computer in an exclusive priority order (regardless of the rights of the user specified in his profile).
Users-guests (extra remote workplace access)	The list of users (user logins are specified, separated by commas), which provide private access to this computer via the RDP protocol, in an exceptional priority order (regardless of the user's rights specified in his profile).
Department	The name of the department to which the computers authorized with this account belong (by default, this option is set in the group account, to override it, select “Manual” instead of “Auto” from the list)
Comments	Comments.

5.4. Configure integration with Helpdesk / Service desk services

The software “TrustViewerPro” has the ability to integrate with the Helpdesk / Service desk services already deployed in the enterprise using the API, allowing you to connect to remote computers on the basis of application tickets that determine the credentials and the validity period of access. In addition, it is also possible to accept user requests and manage them using the helpdesk with a simplified application form built into the product service. In general, the application is submitted as follows: on the main form of the TrustViewerPro client module, the user clicks the link “Application Helpdesk” with the left mouse button (the link is located under the temporary session identifier number), depending on the server settings it either opens the help form application form in the browser selected by default, or opens the help form application form in the integrated window (the Internet Explorer API is used to display and interact with the form), or the built-in simplified constant form filing. After the application is submitted by the user, processed by the 1st line support operator, and transmitted to the 2nd line support operator for execution - it becomes available for execution in the client module interface (the operator can immediately connect to the remote computer upon request, close the request, or return it to the 1st support line). Thus, work with the helpdesk service can be organized in two main scenarios:

- Using the helpdesk service built into TrustViewerPro: all application management functionality is placed directly in the client module. At the same time, using the server's API, there is the possibility of partial integration with external services, for example, for sending notifications about the change in the status of applications via additional communication channels (mail, corporate chat, etc.).
- Using the Helpdesk / Service desk service already deployed in the enterprise: the web page with the request form opens at the URL specified in the TrustViewerPro server settings, and along with the request to the helpdesk / service desk service server, additional reference data is transmitted that partially automates the completion application, as well as a unique application identifier, which is later used to manage the application by API.

The settings for integration with Helpdesk / Service desk services are managed in the “TrustServer” server control panel, in the “Settings”->”Helpdesk” tab.



Server: v2.11.0
Client: -
License: active

WAN Addr: myserver:8443
Server time: 12:27:01
Uptime: 39m 10s
Transferred: 0 Kb

Devices: 1/1/1 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 2/3/3 (act/max/total)
Connections: 4/8/10 (act/max/total)

Client form display mode: Built-in simple form

Server outgoing request mode: Disabled

Server incoming request mode: "Post" - request in json format
Incoming request link: http://myserver:8443/cgi-bin/httptunnel.pl?cmd=UpdateTask&id=???

Client API: Enabled
Token: 79254876-F8A1-4123-924F-D8F048F856F3
Port: 17384

Maximum unaccounted operator downtime: 60 (seconds)

© TrustViewer 2012-2024

The following is a list of settings for integration with Helpdesk / Service desk services:

Setting	Description
Client form display mode	The mode of displaying the application form in the client module: • “Disabled” – disabled (the link “Helpdesk request” on the main form of the client module will not be available) • “Built-in simple form” – the built-in simplified application form is used • “External form in browser” – the application form is used in the form of a web page opened in the default browser • “External form in window” – the application form is used in the form of a web page opened in the integrated window
Link to external form	URL application form (for “External form in browser” and “External form in window” modes)
WindowWidth	The default width of the integrated application window (for the “External form in window” mode)
WindowHeight	The default length of the inline application window (for the “External form in window” mode)
Server outgoing request mode	API mode for outbound notifications about status changes: • “Disabled” – disabled (notifications will not be sent) • “Post - request in json format” - notifications will be sent as Post-request in JSON format
Outgoing request link	URL to which notifications about status changes will be sent (for the “Post - request in json form” mode)
Server incoming	API mode for incoming notifications about status changes:

request mode	• “Post - request in json format” - notifications will be received as a Post-request in JSON format
Incoming request link	The URL to which notifications will be received regarding the status of requests (instead of “Id = ???”, the identifier of the existing application must be indicated, for example, “Id=792CE139-E197-418B-B98D-E2E2EB8B9968”)
Client API	Client module API for access from the browser: • “Disabled” – disabled • “Enabled” – enabled
Token	Security token used to access the client module API from the browser
Port	Client module port used to access the API from the browser

The object of the request is a JSON structure, in addition to information fields, which also contains fields intended for managing the request. Thus, the request management is reduced to sending a JSON structure to the POST request server indicating the fields to be changed (the request URL corresponds to the “Incoming request link” setting, i.e. the settings need the command name “UpdateTask” and the request ID). Following are the JSON structure fields for managing the ticket.

Field	Description
State (string type)	Application Status: • “Active” – the request is active (this status must be set immediately after successful registration of the application on the support site) • “Cancel” – the request is canceled (set if the user cancels the request) • “Close” – the order is closed (set if the 1st line operator closes the application) • “Complete” – Application completed (set in case of closing (completion) of the application by the 2nd line operator)
Number (string type)	Request number
Priority (string type)	Application priority: • “0” – Low • “1” – Normal • “2” – High • “3” – Maximum
Subject (string type)	Subject of the application
Description (string type)	Application Description
Contacts (string type)	Contact the author of the application
Executor (string type)	The current assigned agent of the application (user login is specified with the rights of the 2nd line operator, or an empty line, in case of return of the application for the 1st line)
Comment (string type)	Comment to the application (can be added by the 1st line operator at the time of appointment appointment, or by the 2nd line operator at the time the application is returned back to the 1st line)

At the moment when the user opens the application form, additional settings are added to the URL (specified in the “Link to external form” field) containing the application ID and reference information for auto-filling of some form fields. The following are the settings passed along with the URL.

Setting	Description
ID	The unique ID of the request (used as a setting when sending a request change command to the server)

Department	The department of the computer from which the application was sent
Login	Username of the user author of the application (empty if it is not authorized)
Group	Login for a group computer account (empty if it is not authorized)
Domain	Computer domain / workgroup name
Computer	Network computer name
User	The username of the computer
Ip	List of computer IP addresses

For security reasons, the server does not provide any request information upon request. However, in case of any changes in the request, the server can send to the service address specified in the “Outgoing request link” field the POST requests containing the actual JSON-structure of the application. Thus, it is possible to track the current status of all requests, which is necessary in the case of partial integration with Helpdesk / Service desk services deployed in the enterprise, when part of the request management operations is performed using services directly Helpdesk / Service desk, and partly using the client module interface TrustViewerPro.

Consider an example of using the API in the case of partial integration with Helpdesk / Service desk services deployed in an enterprise (in the case of full integration).

Step 1. Create an application.

Suppose you configured the following URL for application forms – “https://myserver.com/userform” then at load time of the application form, to the server of the support service will be transferred to the query “https://myserver.com/userform?ID=DA2CAC00-ABD9-4EC3-9268-34BED40AA329& Department=Ulyanovsk.Accounting&Login=Alex&Group=&Domain =WORKGROUP&Computer=PC&User=User&Ip=192.168.1.100”.

Step 2. Activation of the application.

Suppose the TrustServer server can be accessed at 192.168.1.2:8443, then, after the user has successfully created a request, the service must send a POST request to the server of the form“http://192.168.1.2:8443/cgi-bin/httptunnel.pl?cmd=UpdateTask&ID=DA2CAC00-ABD9-4EC3-9268-34BED40AA329”, with the following JSON data:

```
{
  "State": "Active",
  "Number": "001",
  "Priority": "1",
  "Subject": "Driver error",
  "Description": "Scanner does not work: driver error",
  "Contacts": "Alexander"
}
```

Suppose the settings indicate the following URL of the service for monitoring the status of requests - “http://127.0.0.1:8888”; then, having processed the request, the TrustServer server will send a POST request of the form “http://127.0.0.1:8888”, with the following JSON data:

```
{
  "ID": "DA2CAC00-ABD9-4EC3-9268-34BED40AA329"
  "State": "Active",
  "Number": "001",
  "Priority": "1",
  "Subject": "Driver error",
  "Description": "Scanner does not work: driver error",
  "Contacts": "Alexander"
  "Department": "London.Accounting",
  "Login": "Alex",
  "Group": "",
  "User": "User",
  "Domain": "WORKGROUP",
  "Computer": "PC",
  "LocalIp": "192.168.1.100"
}
```

Step 3. Assignment of the application to the operator.

After assigning (or reassigning) the request to the operator, the helpdesk service should send a POST request of the form to the server“http://192.168.1.2:8443/cgi-bin/httptunnel.pl?cmd=UpdateTask&ID=DA2CAC00-ABD9-4EC3-9268-34BED40AA329”, with the following JSON data (indicating the login of the operator to which the application will be assigned, as well as, if necessary, the accompanying comment):

```
{
  "Executor": "Alex",
  "Comment": " Optional comment "
}
```

After processing the request, the TrustServer server will send a POST request of the form “http://127.0.0.1:8888”, with the following JSON data:

```
{
  "ID": "DA2CAC00-ABD9-4EC3-9268-34BED40AA329"
  "State": "Active",
  "Number": "001",
  "Priority": "1",
  "Subject": "Driver error",
  "Description": "Scanner does not work: driver error",
  "Contacts": "Alexander"
  "Department": "London.Accounting",
  "Login": "Alex",
  "Group": "",
  "User": "User",
  "Domain": "WORKGROUP",
  "Computer": "PC",
  "LocalIp": "192.168.1.100",
  "Executor": "Alex",
  "Comment": " Optional comment "
}
```

Step 4. Return the application to the 1st line.

If the request is returned by the 2nd line operator back to the 1st line, the helpdesk service should send to the server a POST request of the form “http://192.168.1.2:8443/cgi-bin/httptunun.pl?cmd=UpdateTask&ID= DA2CAC00-ABD9-4EC3-9268-34BED40AA329 ”, with the following JSON data (with an empty login, as well as, if necessary, an accompanying comment):

```
{
  "Executor": "",
  "Comment": " Optional comment "
}
```

After processing the request, the TrustServer server will send a POST request of the form “http://127.0.0.1:8888”, with the following JSON data:

```
{
  "ID": "DA2CAC00-ABD9-4EC3-9268-34BED40AA329"
  "State": "Active",
  "Number": "001",
  "Priority": "1",
  "Subject": "Driver error",
  "Description": "Scanner does not work: driver error",
  "Contacts": "Alexander"
  "Department": "London.Accounting",
  "Login": "Alex",
  "Group": "",
  "User": "User",
  "Domain": "WORKGROUP",
  "Computer": "PC",
  "LocalIp": "192.168.1.100",
  "Executor": "",
  "Comment": " Optional comment "
}
```

Step 5. Cancellation / closing / completion of the application.

In case of cancellation / closing / completion of the request, the helpdesk service should send a POST request to the server of the form “http://192.168.1.2:8443/cgi-bin/httptunnel.pl?cmd=UpdateTask&ID=DA2CAC00-ABD9-4EC3-9268-34BED40AA329”, with the following JSON data (indicating the corresponding status - “Cancel”, “Close” or “Complete”):

```
{
  "State": "Complete"
}
```

After processing the request, the TrustServer server will send a POST request of the form “http://127.0.0.1:8888”, with the following JSON data:

```
{
  "ID": "DA2CAC00-ABD9-4EC3-9268-34BED40AA329"
  "State": "Complete",
  "Number": "001",
  "Priority": "1",
  "Subject": "Driver error",
  "Description": "Scanner does not work: driver error",
  "Contacts": "Alexander"
  "Department": "London.Accounting",
  "Login": "Alex",
  "Group": "",
  "User": "User",
  "Domain": "WORKGROUP",
  "Computer": "PC",
  "LocalIp": "192.168.1.100",
  "Executor": "Alex",
  "Comment": " Optional comment "
}
```

The client module API allows you to obtain clarifying information about the client computer for use in external application forms. For example, a request

```
http://localhost:17384/cgi-bin/api.pl?tid=79254876-F8A1-4123-924F-D8F048F856F2&cmd=getinfo
```

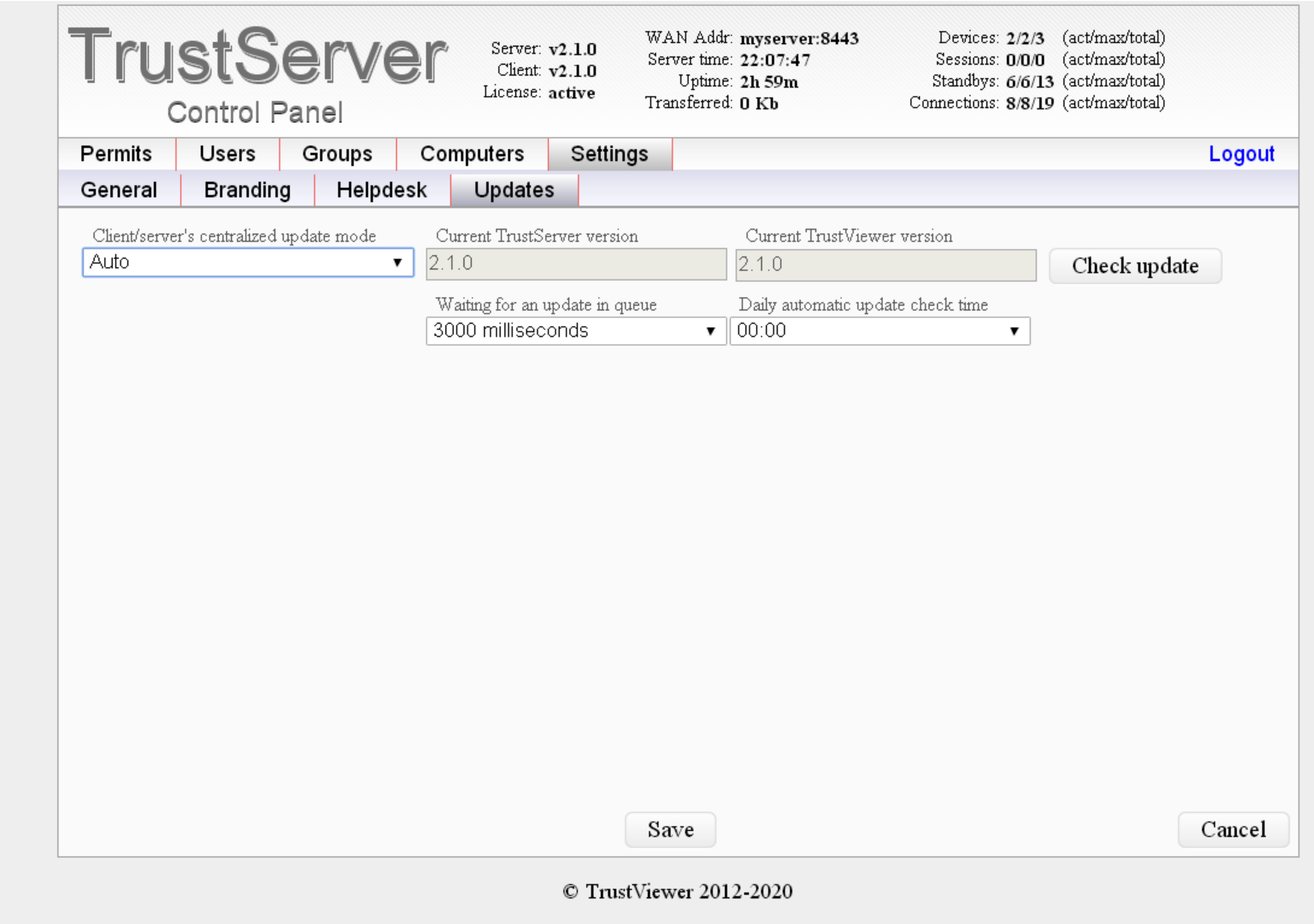
will return the following data in JSON format:

```
{"Domain": "WORKGROUP", "Computer": "TV10", "LocalIp":
"192.168.56.1;192.168.0.106", "ExternalIp": "192.168.56.1", "MAC": "0A-00-28-00-
00-0D;B4-2E-90-EE-75-90", "CPU": "AMD Ryzen 5 PRO 4650G with Radeon Graphics (12
units)", "RAM": "32163 Mb RAM (25209 Mb available)", "OS": "Windows 10
(PROFESSIONAL, 64 bit)", "Uptime": 11886, "SystemId": "C1F4C2A2-D722-7516-2605-
BEE6956E59F4"}
```

5.5. Update Management "TrustViewerPro"

TrustServer also serves as an update server, allowing you to keep current versions of both the client modules and the server itself. For the update procedure, a special file is used that contains the update package for all variants of the builds, both the server (Windows, Linux 32/64) and the client module (“TrustViewer”, “TrustViewerPro”). In this case, the download of the update package is possible both in the automatic mode according to the schedule and in the manual mode. Thus, the operation of TrustServer as an update server is possible both in public networks and in private networks without access to the Internet.

Updates are managed in the “TrustServer” server control panel, in the “Settings”->“Updates” tab.



Server: v2.1.0
Client: v2.1.0
License: active

WAN Addr: myserver:8443
Server time: 22:07:47
Uptime: 2h 59m
Transferred: 0 Kb

Devices: 2/2/3 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 6/6/13 (act/max/total)
Connections: 8/8/19 (act/max/total)

Client/server's centralized update mode: Auto
Current TrustServer version: 2.1.0
Current TrustViewer version: 2.1.0
Waiting for an update in queue: 3000 milliseconds
Daily automatic update check time: 00:00

© TrustViewer 2012-2020

The following is a list of update management options:

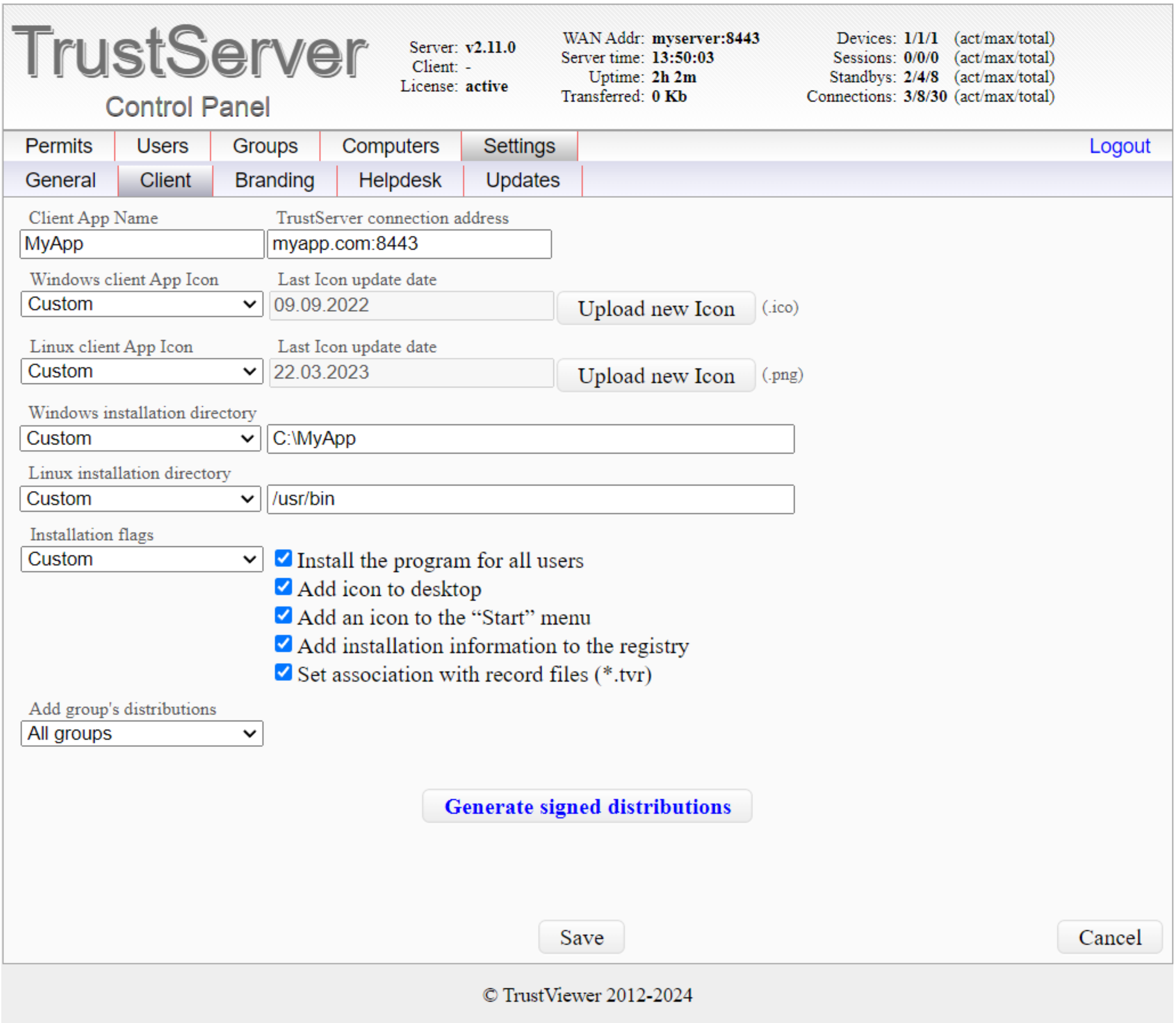
Option	Description
Client/server's centralized update mode	Mode of centralized update of the server and client module: • “Disabled” – disabled (updates will not be installed centrally) • “Manual” – installation of updates manually (you need to download the update package file from the program’s website and upload it to the server) • “Auto” – install updates automatically (the server automatically checks and installs all updates according to the schedule)
Waiting for an update in queue	The estimated time in the queue to wait for an update for one client module, in milliseconds (when receiving a signal to download an update, to prevent server overload – client modules are queued to wait for the download of the update)
Daily automatic update check time	Automatic daily check time and install updates.

5.6. Branding settings

As part of branding, it is possible to generate distribution kits of the client module signed with the EDS of the developer, indicating their own name and program icon. In addition, at any time it is possible to change the logo and wallpaper of the main form (static image of arbitrary size), as well as customize the display of your banner (flash movie, gif-animation, or static image with optimal size 468x120px), with the ability to follow the link (link will be opened in the default browser.)

5.6.1. Generation of own distributions signed by the developer's EDS

Generation of own distributions signed by the developer's EDS are managed in the TrustServer server control panel, in the “Settings”->”Client” tab.



Server: v2.11.0
Client: -
License: active

WAN Addr: myserver:8443
Server time: 13:50:03
Uptime: 2h 2m
Transferred: 0 Kb

Devices: 1/1/1 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 2/4/8 (act/max/total)
Connections: 3/8/30 (act/max/total)

Client App Name: MyApp
TrustServer connection address: myapp.com:8443
Windows client App Icon: Custom
Last Icon update date: 09.09.2022 (.ico)
Linux client App Icon: Custom
Last Icon update date: 22.03.2023 (.png)
Windows installation directory: Custom C:\MyApp
Linux installation directory: Custom /usr/bin
Installation flags: Custom

- ☑ Install the program for all users
- ☑ Add icon to desktop
- ☑ Add an icon to the “Start” menu
- ☑ Add installation information to the registry
- ☑ Set association with record files (*.tvr)

Add group's distributions: All groups

Below is a list of distribution generation options:

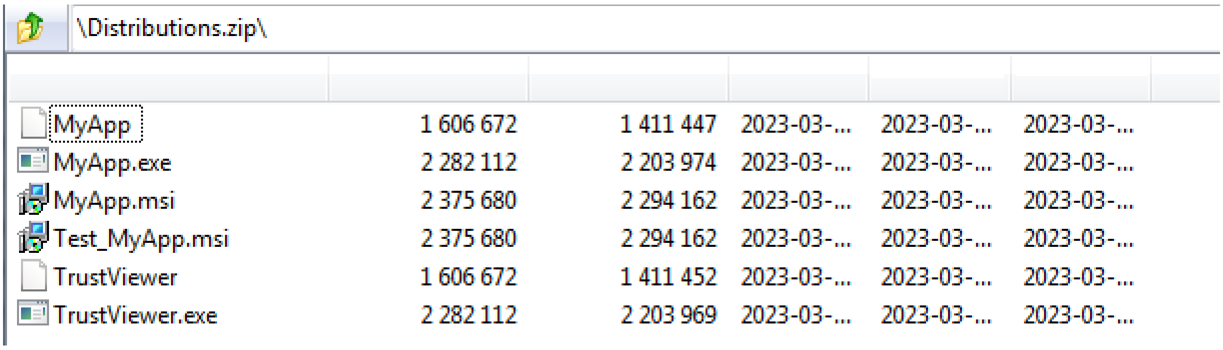
Option	Description
Client App Name	Custom program name (set to “TrustViewerPro” to use the default name).
TrustServer connection address	trustserver address.
Windows client App Icon	Custom program icon for Windows OS (set to “Default” to use the default icon).
Linux client App Icon	Custom program icon for Linux OS (set to “Default” to use the default icon).
Windows Installation directory	Custom program installation directory Linux OS (set to “Default” to use the default directory).
Linux Installation directory	Custom program installation directory Windows OS (set to “Default” to use the default directory).
Installation flags	Installation options (set to “Default” to use default options): • “Install the program for all users” – install the program for all users • “Add icon to desktop” – add icon to desktop • “Add an icon to the “Start” menu” – add an icon to the start menu • “Add installation information to the registry” – add installation information

	to the Windows registry. • “Set association with record files (*.tvr)” – set association with recording files (*.tvr)
Add group's distributions	Generating additional distributions for group accounts: • “Disabled” – distributions for group accounts will not be generated • “All groups” – distributions will be generated for all group accounts • “Custom group” – a distribution package will be generated for the selected account

After all the necessary parameters have been set and saved, you must click on the “Generate signed distributions” button. After processing the request, you will be prompted to download the archive with distributions.

Attention! To process the request, you need access to the Internet.

Below is an example of an archive structure with distributions, where “MyAppe” and “MyApp.exe ” – portable versions of the client module for Linux and Windows OS, “MyApp.msi” – msi-client module package, “Test_MyApp.msi” – msi-client module package without EDS, specifically for installation in full functionality mode using the login and password of the “Test” group account (as many distributions will be generated as there are group accounts registered on the server), “TrustViewer” “TrustViewer.exe ” - portable versions of the regular (non-professional) TrustViewer program for Linux and Windows, which can be used for compatibility.

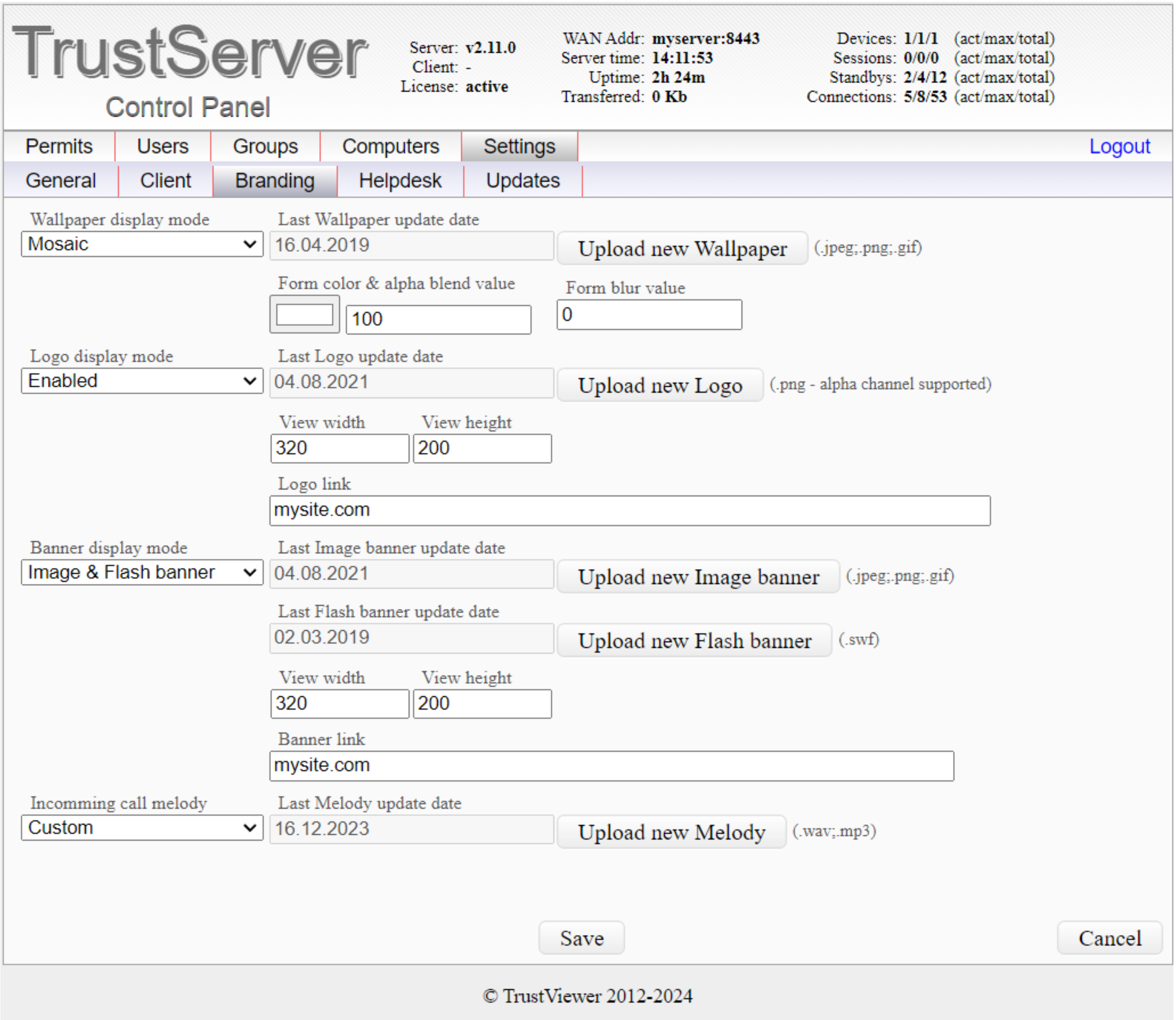


\Distributions.zip\

MyApp	1 606 672	1 411 447	2023-03-...	2023-03-...	2023-03-...
MyApp.exe	2 282 112	2 203 974	2023-03-...	2023-03-...	2023-03-...
MyApp.msi	2 375 680	2 294 162	2023-03-...	2023-03-...	2023-03-...
Test_MyApp.msi	2 375 680	2 294 162	2023-03-...	2023-03-...	2023-03-...
TrustViewer	1 606 672	1 411 452	2023-03-...	2023-03-...	2023-03-...
TrustViewer.exe	2 282 112	2 203 969	2023-03-...	2023-03-...	2023-03-...

5.6.2. Banner, logo and wallpaper management

Banner, logo and wallpaper are managed in the TrustServer server control panel, in the “Settings”->”Branding” tab.



Server: **v2.11.0**
Client: -
License: **active**

WAN Addr: **myserver:8443**
Server time: **14:11:53**
Uptime: **2h 24m**
Transferred: **0 Kb**

Devices: **1/1/1** (act/max/total)
Sessions: **0/0/0** (act/max/total)
Standbys: **2/4/12** (act/max/total)
Connections: **5/8/53** (act/max/total)

Wallpaper display mode: Mosaic
Last Wallpaper update date: 16.04.2019 (.jpeg;.png;.gif)
Form color & alpha blend value: 100
Form blur value: 0

Logo display mode: Enabled
Last Logo update date: 04.08.2021 (.png - alpha channel supported)
View width: 320
View height: 200
Logo link: mysite.com

Banner display mode: Image & Flash banner
Last Image banner update date: 04.08.2021 (.jpeg;.png;.gif)
Last Flash banner update date: 02.03.2019 (.swf)
View width: 320
View height: 200
Banner link: mysite.com

Incomming call melody: Custom
Last Melody update date: 16.12.2023 (.wav;.mp3)

© TrustViewer 2012-2024

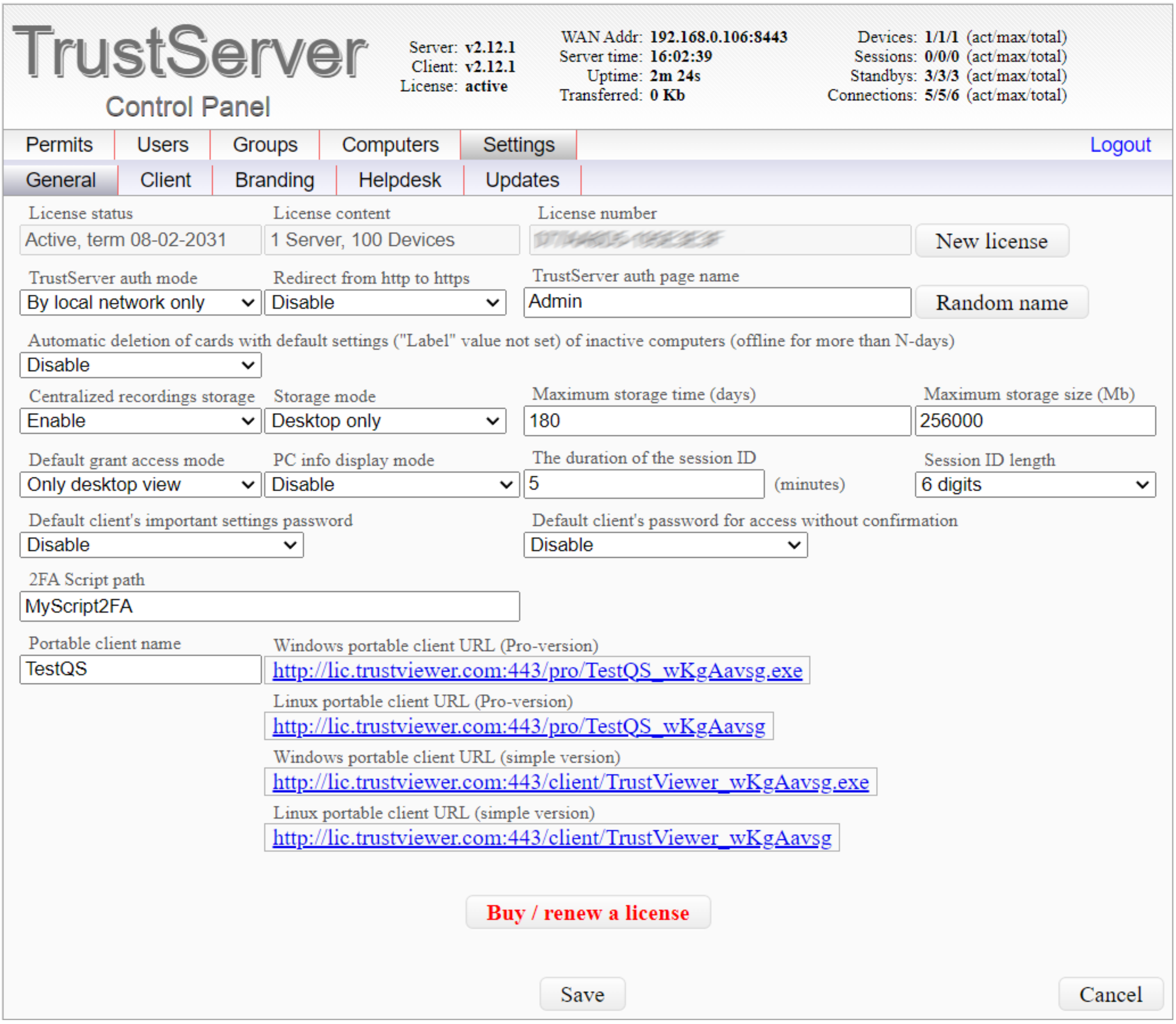
Following Below is a list of options for managing wallpaper, banner and logo:

Option	Description
Wallpaper display mode	Wallpaper display mode: • “Default” – the preset wallpaper will be displayed • “Mosaic” – custom wallpapers will be displayed in “fill” mode • “Stretch” – custom wallpapers will be displayed in “stretch” mode
Form color & alpha blend value	Color and transparency level
Form blur value	Blur level
Logo display mode	Logo display mode: • “Disabled” – disabled (the logo will not be shown) • “Enabled” – enabled (logo will be shown)
Logo View width & View height	The width and height of the logo when displayed
Logo link	Logo URL (leave this field blank if no link is required).
Banner display mode	Banner display mode: • “Disabled” – disabled (banner will not be shown) • “Image banner only” – enabled (only static banner or gif-animation will be shown) • “Image & Flash banner” – enabled (the flash movie will be shown if possible, either a static banner or a gif-animation)

Banner View width & View height	The width and height of the banner when displayed
Banner link	Banner URL-link (leave this field blank if the link is not required).
Incomming call melody	Режим проигрывания мелодии для входящих звонков: • “Default” – использование мелодии по умолчанию • “Custom” – использование пользовательской мелодии

5.7. Main server settings

The main server settings are made in the “TrustServer” server control panel, in the “Settings”->”General” tab.



Server: v2.12.1
Client: v2.12.1
License: active

WAN Addr: 192.168.0.106:8443
Server time: 16:02:39
Uptime: 2m 24s
Transferred: 0 Kb

Devices: 1/1/1 (act/max/total)
Sessions: 0/0/0 (act/max/total)
Standbys: 3/3/3 (act/max/total)
Connections: 5/5/6 (act/max/total)

License status: Active, term 08-02-2031
License content: 1 Server, 100 Devices
License number: [redacted]

TrustServer auth mode: By local network only
Redirect from http to https: Disable
TrustServer auth page name: Admin

Automatic deletion of cards with default settings ("Label" value not set) of inactive computers (offline for more than N-days): Disable

Centralized recordings storage: Enable
Storage mode: Desktop only
Maximum storage time (days): 180
Maximum storage size (Mb): 256000

Default grant access mode: Only desktop view
PC info display mode: Disable
The duration of the session ID: 5 (minutes)
Session ID length: 6 digits

Default client's important settings password: Disable
Default client's password for access without confirmation: Disable

2FA Script path: MyScript2FA

Portable client name: TestQS
Windows portable client URL (Pro-version): http://lic.trustviewer.com:443/pro/TestQS_wKgAavsg.exe
Linux portable client URL (Pro-version): http://lic.trustviewer.com:443/pro/TestQS_wKgAavsg
Windows portable client URL (simple version): http://lic.trustviewer.com:443/client/TrustViewer_wKgAavsg.exe
Linux portable client URL (simple version): http://lic.trustviewer.com:443/client/TrustViewer_wKgAavsg

5.7.1. License activation

Unregistered copy of “TrustViewerPro” has restrictions on the number of connections to the server, so product registration is required to complete the work. At the same time, product registration is possible both in automatic mode via the Internet and in manual mode without access to the Internet. Thus, the full-fledged work of “TrustServer” is possible both in public networks and in private networks without access to the Internet.

Product registration is carried out in the TrustServer server control panel, in the “Settings”->”General” tab. To activate a new license, click the “New license” button, then enter the license number in the “License number” field, and click the “Apply” button. If Internet access is available, the registration will be performed automatically; otherwise, a link to the license file will be created, which will need to be manually downloaded from a computer with Internet access, and then uploaded to the server (“Upload license file” button). To cancel the registration, click the “New license” button, and then immediately click the “Apply” button (the “License number” field should be empty).

Attention! You can repeatedly register a product with the same license number, incl. and on different servers. However, activation of two or more different servers at the same time is prohibited (in this case, the license will be active only for the last activated server), so it is strongly recommended to unregister before performing license activation on another server.

Attention! The product “TrustViewerPro” is distributed on a subscription basis. This means that after the expiration of the license - the program will be limited. To exclude interruptions in work, please renew your license in a timely manner.

Attention! Automatic license renewal (after timely payment) - is possible only if the server has Internet access, otherwise - it is necessary to re-register the product manually.

5.7.2 Main settings

Management of additional settings is carried out in the server control panel “TrustServer”, on the “Settings”->”General” tab.

Following is a list of advanced settings options:

Option	Description
TrustServer auth mode	Authorization mode in the server management panel: - “By local network only” – authorization is allowed only in the local network - “Both LAN and WAN” – authorization is allowed on the local network and the Internet
Redirect from http to https	Configuring the redirect of the control panel page from the HTTP protocol to the HTTPS protocol (you need to configure the use of an SSL certificate, for more details, see “Installation of the «TrustServer» server” section of this manual): - “Disabled” – redirect is disabled - “By WAN only” – redirect is enabled only for Internet connections to the server - “Both LAN and WAN” – redirect is enabled for both local and Internet connections to the server
TrustServer auth page name	The name of the server authorization page (to generate a random name - click the “Random name” button)
Automatic deletion of cards with default settings ("Label" value not set) of inactive computers (offline for more than N-days)	The mode of automatic deletion of cards of unused computers (a computer is considered unused if its field does not contain the “Label” field, and also if it was offline for a specified number of days, ie it was not connected to the server): - “Disabled” - disabled (unused contacts cards will not be automatically deleted) - “Enabled” - enabled (cards of unused contacts will be automatically deleted)
Centralized	Centralized storage of session recordings:

recordings storage	- "Disabled" – disabled (recordings will not be saved on the server) - "Enabled" – enabled (all recordings will be saved on the server)
Storage mode	The mode of preservation of records: - "Desktop only" – only desktop recordings will be made - "Desktop and Audio" – only desktop recordings and audio calls will be made - "Full (Desktop, Audio and Video)" – will be recorded desktop and audio and video calls
Maximum storage time (days)	Time limit for storing records on the server, in days
Maximum storage size (Mb)	Limit on the total size, on storage of records on the server, in megabytes
Default grant access mode	The default access mode provided by the user to his computer (when connecting on request to unauthorized computers, including to the "TrustViewer" client modules, in which authorization is not provided): - "Only desktop view (min rights)" – only desktop view is allowed - "Joint control" – both desktop view and joint control are allowed - "Unlimited access" – full access to the computer is allowed, including access to the clipboard and the file system without confirmation
PC info display mode	The mode of displaying reference information about the computer on the main form of the client module - "Disabled" – disabled (reference information will not be shown) - "Net name only" – enabled (only the network name of the computer will be shown) - "IP only" – enabled (only the IP address of the computer will be shown) - "Net name & IP" – enabled (both the IP address and the network name of the computer will be shown)
The duration of the session ID	Limit the duration of the session identifier in the client module in idle mode (in minutes)
Session ID length	The number of digits in the session ID.
Default client's important settings password	Default password to access important settings of the client module (in the settings of the client module, on the "Security" tab, the "Protecting important settings with a password" flag must be unchecked, and the "Allow remote modification of program settings" flag must be set)
Default client's password for access without confirmation	The default password for access to the computer without confirmation (in the settings of the client module, on the "Security" tab, the "Default password for access without confirmation" flag must be unchecked, and the "Allow remote modification of program settings" flag must be set)
2FA Script path	Path to the script for processing the request to send a verification code as part of two-factor authentication. The request is executed by passing five parameters to the command line like "MySrcipt $1 $2 $3 $4 $5", the first two of which are mandatory ("$1" is the authorization code, "$2" is the 2FA login) and three more are clarifying ("$3" is the login user, "$4" is the user's full name, "$5" is the user's display name)
Portable client name	The name of the program that will be displayed when the portable client module is launched in instant remote support mode
Windows portable client URL (Pro-version)	Automatically generated link to the stand-alone TrustViewerPro client module in instant remote support mode, for Windows OS
Linux portable client URL (Pro-version)	Automatically generated link to the stand-alone TrustViewerPro client module in instant remote support mode, for Linux OS
Windows portable client URL (simple version)	Automatically generated link to the TrustViewer portable program in instant remote support mode, for Windows OS
Linux portable client URL (simple version)	Automatically generated link to the TrustViewer portable program in instant remote support mode, for Linux OS

6. Work with the client module «TrustViewerPro»

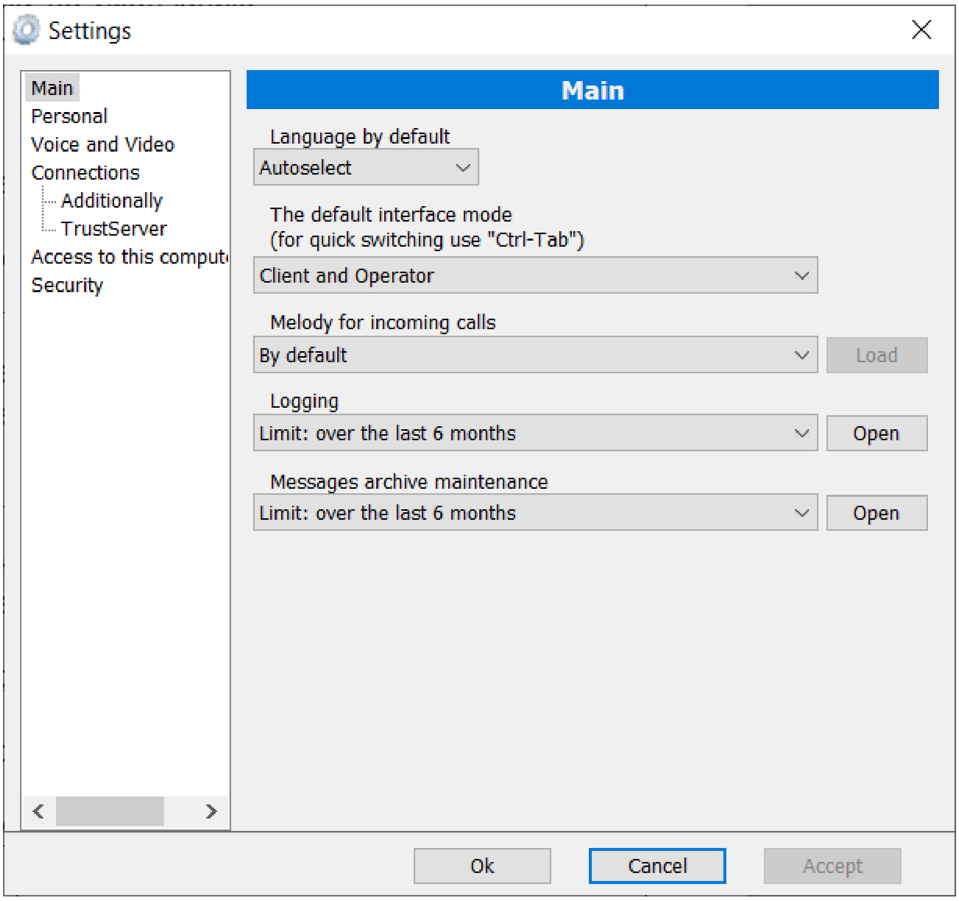
Once installed on the computer, the TrustViewerPro client module can be used both to provide remote access to your computer (client mode) and to connect to other remote computers (operator / administrator mode). At the same time, working in the operator / administrator mode is possible only after the user is authorized on the “TrustServer” server, and also if he has the appropriate rights and permissions. Two authorization options are possible:

- “Temporary authorization” - is performed from the main form of the program (where it can also be canceled) and is valid for the duration of the program until restarting it.
- “Permanent authorization” - is performed automatically when the program is started, with the credentials specified in the personal settings (“Menu” → “Settings” → “Personal”).

6.1. Settings of the client module «TrustViewerPro»

To open the client module settings form - click the “Menu” button on the main form of the program (or right-click on the program icon in the tray), and select “Settings”. Note: in addition to the “Settings” menu item, the “Language” items are also available (to temporarily change the current interface language) and “About the program” (to display information about the program and license status).

6.1.1. “Main” settings page



Language by default: Autoselect

The default interface mode (for quick switching use "Ctrl-Tab"): Client and Operator

Melody for incoming calls: By default

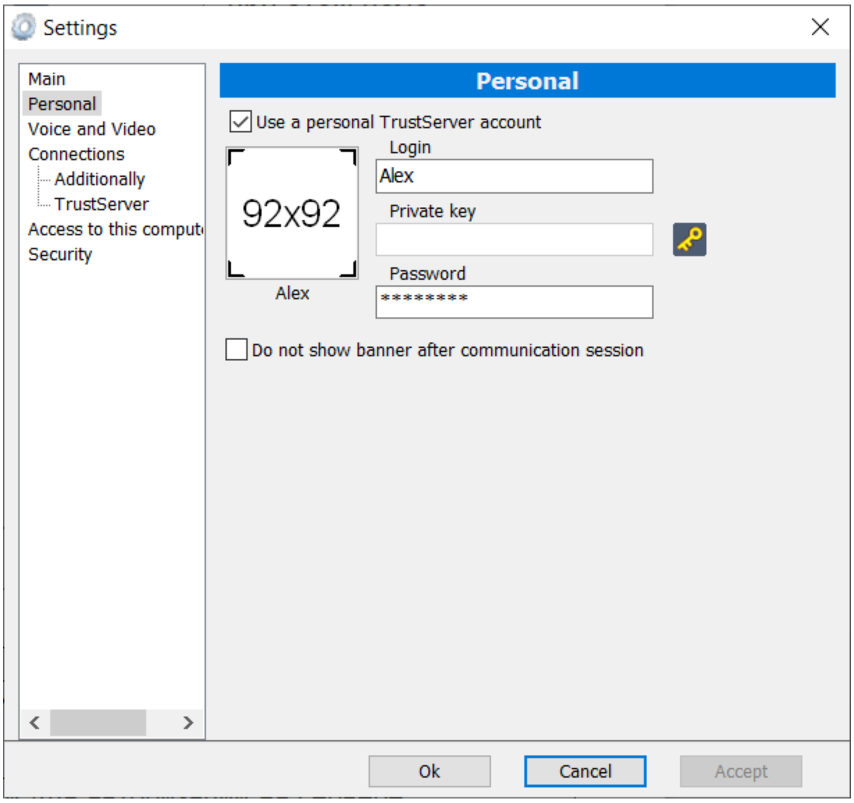
Logging: Limit: over the last 6 months

Messages archive maintenance: Limit: over the last 6 months

On this you can change the main settings of the program.

Setting	Description
Default language	Program interface language: • “Autoselect” - when the program is started, the interface language will be automatically selected, depending on the system settings (if the language defined in the system is not supported by the program, then English will be selected by default) • “List of languages” - selection from the list of available interface languages in the program.
Default interface mode	Defines the default interface mode: • "Client and Operator" - on the main form of the program, the interface of both the client and the operator is available (subject to user authorization) • "Client only” – only the client interface is available on the main form of the program • "Operator only" – only the operator interface is available on the main form of the program (subject to user authorization)
Melody for incoming calls	Defines the ringtone for incoming calls: • “Do not use” – the melody will not be played • “Default” – the default melody will be played • “Custom” – a custom melody will be played
Keeping a journal	Time limit for program logging: • “Forbid” - the log will not be kept • “Limit: within the last month” - the magazine will be limited to one month • “Limit: over the last 6 months” - the journal will be limited to half a year • “Limit: over the last year” - the magazine will be limited to one year • “Unlimited” - the magazine will not be limited in time.
Archiving of messages	Restriction of maintaining archive of messages in time: • “Forbid” - the archive will not be kept • “Limit: within the last month” - the archive will be limited to one month • “Limit: over the last 6 months” - the archive will be limited to half a year • “Limit: over the last year” - the archive will be limited to one year • “Unlimited” - the archive will not be limited in time.

6.1.2. Personal Settings Page



☑ Use a personal TrustServer account

Login: Alex

Private key:

Password: ********

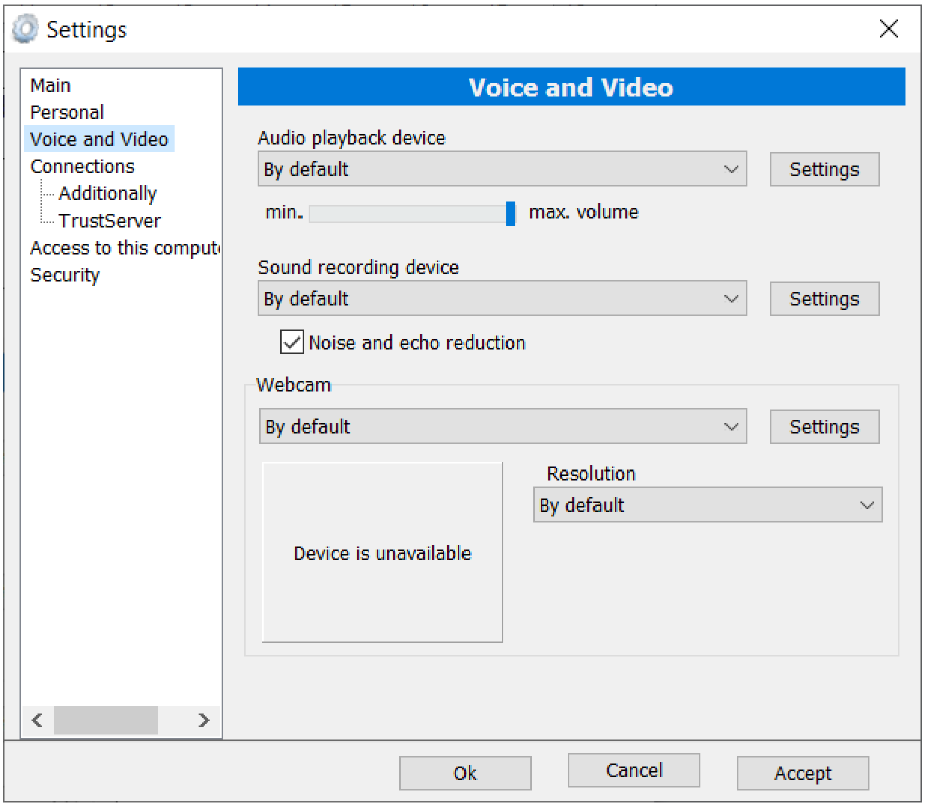
☐ Do not show banner after communication session

If user authorization is required - the login and password of the “TrustServer” account are indicated on this page, while the “Display Name” field and also “Photo” are loaded automatically. Also, for authorized users, you can disable the display of the banner after the end of the session.

Setting	Description
Use a personal TrustServer account	Determines whether the TrustServer personal account will be used, i.e. whether authorization is required on the server.
Login	Login of the account for authorization on the server
Private key	RSA key for authorization on the server using a certificate
Password	Password of the account for authorization on the server
Display Name	Display user name when connecting to a remote computer
A photo	User photo
Do not show banner after session	Determines whether the banner will be displayed after the session

6.1.3. “Voice and Video” settings page

On this page you can select a webcam, as well as playback and sound recording devices that will be used in the program, including for video calls.



Audio playback device: By default

Sound recording device: By default

☑ Noise and echo reduction

Webcam: By default

Device is unavailable

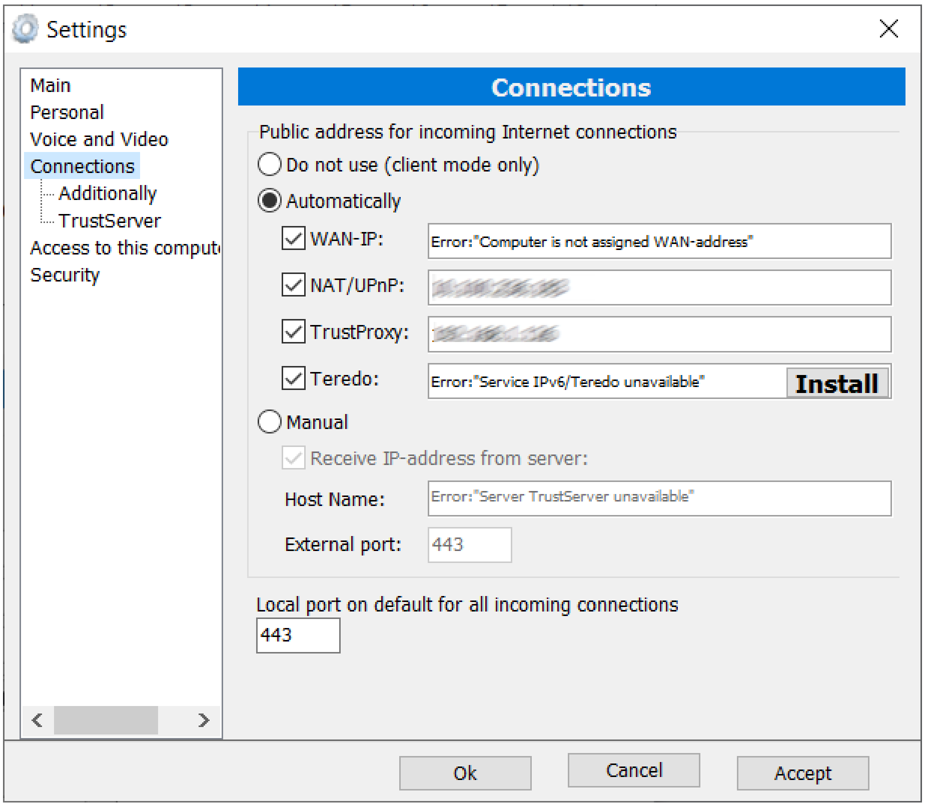
Resolution: By default

Setting	Description
Audio playback device	Defines the audio playback device used in the program: • “Default” - the device specified in the system will be used • “Device List” - select from the list of available devices in the system
Volume	Specifies the default volume level for audio playback
Sound recording device	Defines the sound recorder used in the program: • “Default” - the device specified in the system will be used. • “Device List” - select from the list of available devices in the system.
Noise and echo reduction	Determines if noise and echo reduction is required when recording audio
Webcam	Defines the webcam used in the program: • “Default” - the default webcam will be used in the system • “Device List” - select from the list of available webcams in the system

Resolution	Defines the video stream resolution for the webcam. • “Default” - the resolution set for the default webcam will be used • “Permissions List” - select from the list of permissions available for the webcam

6.1.4. “Connections” settings page

On this page, you can change the settings for incoming connections (computer administrator rights are required).



Connections

Public address for incoming Internet connections

○ Do not use (client mode only)

● Automatically

☑ WAN-IP: Error:"Computer is not assigned WAN-address"

☑ NAT/UPnP: [redacted]

☑ TrustProxy: [redacted]

☑ Teredo: Error:"Service IPv6/Teredo unavailable" Install

○ Manual

☑ Receive IP-address from server:

Host Name: Error:"Server TrustServer unavailable"

External port: 443

Local port on default for all incoming connections

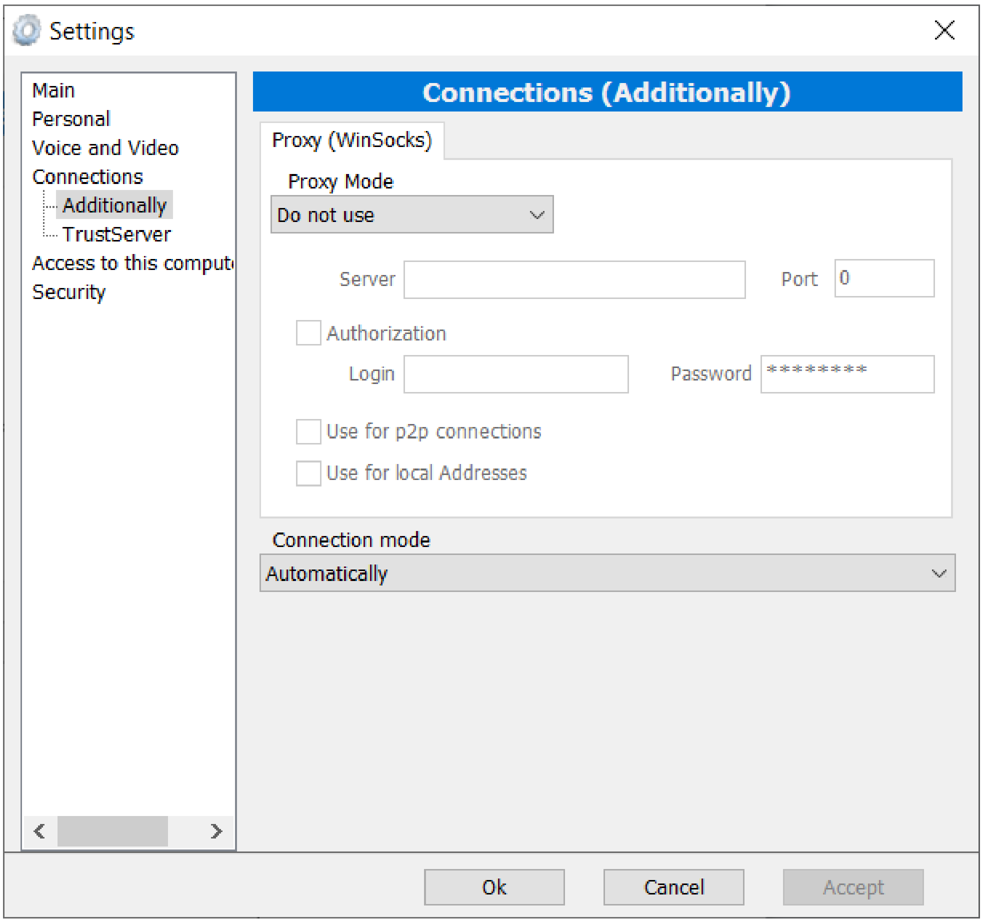
443

Attention! Automatic detection of all possible types of incoming connections allows to improve the efficiency of routing optimization when connecting to a remote computer, however, in some cases, the process of optimizing routing may take a longer time.

Setting	Description
Do not use (client mode only)	Determines whether incoming internet connections will be allowed
Automatically	Automatic configuration of incoming Internet connections • “WAN-IP” - determines if the computer’s “WAN-IP” address will be used • “NAT / UPnP” - determines whether the protocol “NAT / UPnP” will be used to obtain the public address of the computer • “TrustProxy” - determines whether the TrustServer server’s IPA will be used (in proxy mode) to get the public address of the computer • “Teredo” - determines whether the “Teredo” service will be used - to get the public address of the computer
Manual	Manual setting of the public address of the computer for incoming Internet connections • “Reseive IP-address from server” - determines whether you need to specify the host name and port number manually, or the host name can be automatically determined using the public server

	“TrustServer” • “External port” - external port number for incoming Internet connections
Local port on default for all incoming connections	Computer's default port for all local and internet connections

6.1.5. “Additionally” settings page



Proxy Mode: Do not use

Port: 0

Password: ********

☐ Authorization

☐ Use for p2p connections

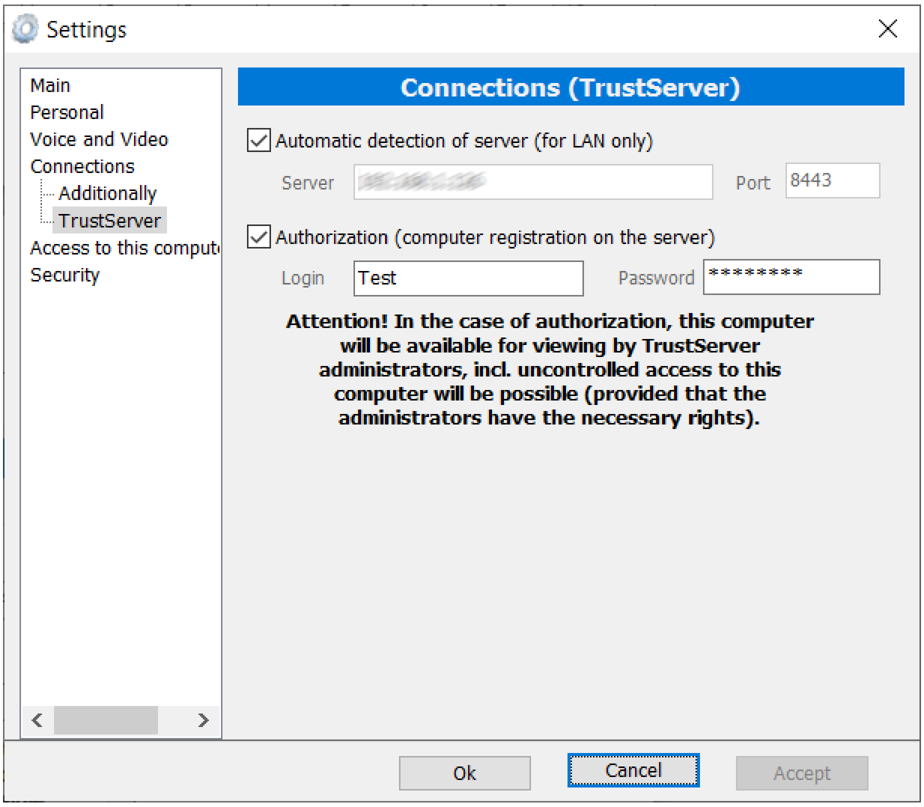
☐ Use for local Addresses

Connection mode: Automatically

On this page, you can change additional connection settings (computer administrator rights are required).

Setting	Description
Proxy (WinSocks)	Proxy settings (for WinSocks only, for WinInet, proxy settings are determined by the system): • “Proxy mode” - defines the proxy mode (“HTTP / HTTPS”, “SOCKS 4/5”) or cancels the use of a proxy (“Do not use”) • “Server / Port” - the host name and port number of the proxy server • “Authorization” - determines whether authorization is required on the proxy server • “Login / Password” - the login and password of the account for authorization on the proxy server • “Use for p2p connections” - determines whether you need to use a proxy server for p2p connections • “Use for local Addresses” - determines whether to use a proxy server for local addresses
Connection mode	Connection mode: • “Автоматически” – the optimal connection mode will be selected automatically • “TrustSocks” – secure connection using the TrustSocks protocol • “Https (WinSSPI)” – secure connection using the Https (WinSSPI) protocol • “Https (WinInet)” – secure connection using the Https (WinInet) protocol

6.1.6. Settings page “TrustServer”



Connections (TrustServer)

☑ Automatic detection of server (for LAN only)

Server Port 8443

☑ Authorization (computer registration on the server)

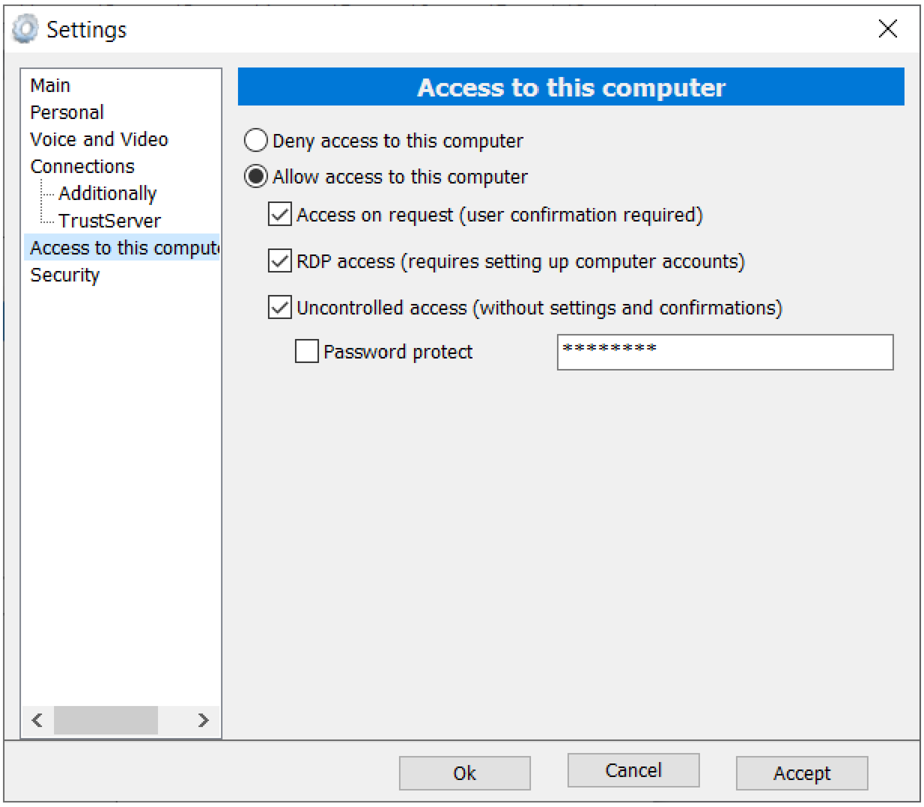
Login Test Password ********

Attention! In the case of authorization, this computer will be available for viewing by TrustServer administrators, incl. uncontrolled access to this computer will be possible (provided that the administrators have the necessary rights).

On this page you can change the server connection settings (computer administrator rights are required).

Параметр	Описание
Automatic detection of server	Determines whether the server will be detected automatically (only for the local network), or the server address must be set manually • “Server / Port” - the host name and port number of the server
Authorization	Determines whether authorization of the computer on the server is required (full functionality of the client module) • “Login / Password” - a group account login and password for authorizing a computer on the server

6.1.7. Settings page “Access this computer”



Access to this computer

○ Deny access to this computer

● Allow access to this computer

☑ Access on request (user confirmation required)

☑ RDP access (requires setting up computer accounts)

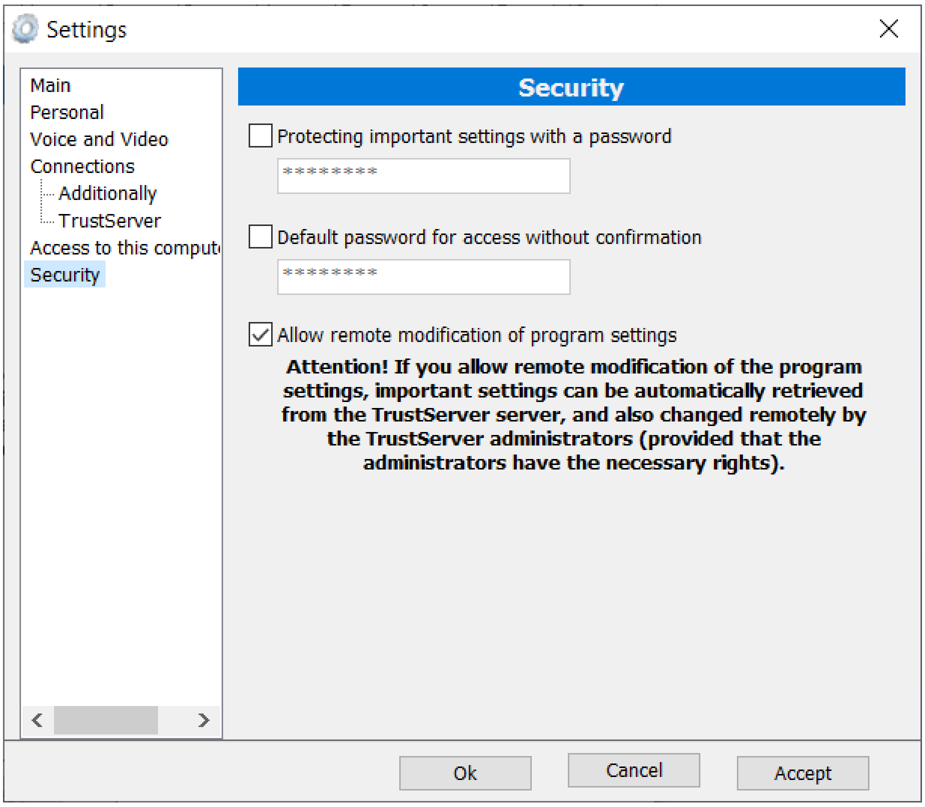
☑ Uncontrolled access (without settings and confirmations)

☐ Password protect ********

On this page, you can change the settings of the permanent access to the computer without an invitation (you need computer administrator rights, as well as authorization of the computer on the TrustServer server)

Setting	Description
Deny access to this computer	Denies permanent access to a computer without an invitation.
Allow access to this computer	Allows continuous access to a computer without an invitation: • “Access on request (user confirmation required)” - allows constant access to the computer with the need to confirm the request for access • “RDP access (requires setting up computer accounts)” - allows continuous private access to a computer using RDP sessions • “Uncontrolled access (without settings and confirmations)” - allows constant uncontrollable access to a computer without restrictions • “Password protect” - determines whether an additional password should be used in case of uncontrolled access to this computer • “Password” - an additional password in case of uncontrolled access to this computer“Пароль” – additional password in case of uncontrolled access to this computer

6.1.8. Settings page “Security”



☐ Protecting important settings with a password

****

☐ Default password for access without confirmation

****

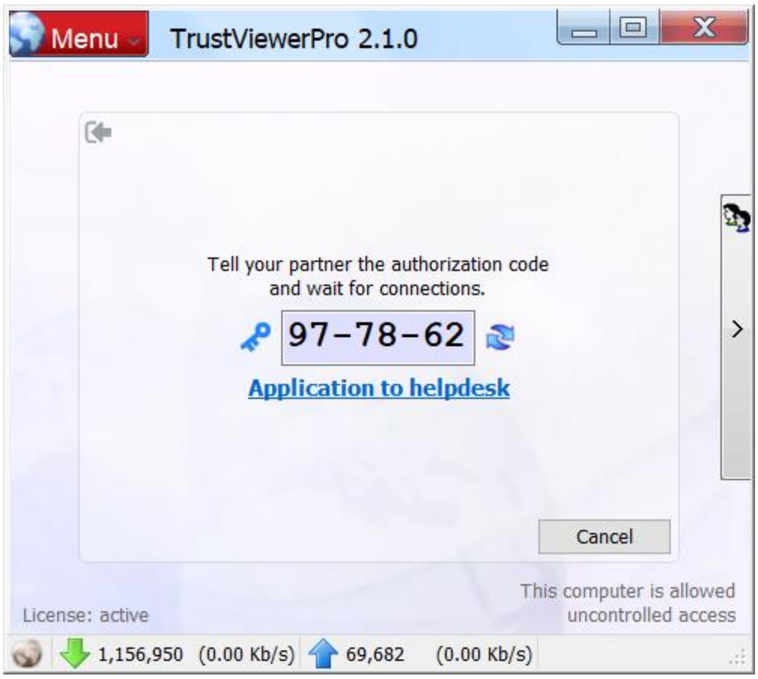
☑ Allow remote modification of program settings

Attention! If you allow remote modification of the program settings, important settings can be automatically retrieved from the TrustServer server, and also changed remotely by the TrustServer administrators (provided that the administrators have the necessary rights).

On this page, you can change the settings related to the security of using the program (requires computer administrator rights).

Setting	Description
Protecting important settings with a password	Specifies the password used to access important program settings (“Connections”, “Access this computer” and “Security”)
Default password for access without confirmation	Sets the default password for accessing the computer without confirmation when granting access using a temporary ID
Allow remote modification of program settings	Разрешает удаленное изменение всех важных настроек программы администраторами TrustServer (при условии наличия у администраторов необходимых прав)

6.2. Work with the «TrustViewerPro» client module in client mode



Tell your partner the authorization code
and wait for connections.

97-78-62

Application to helpdesk

License: active

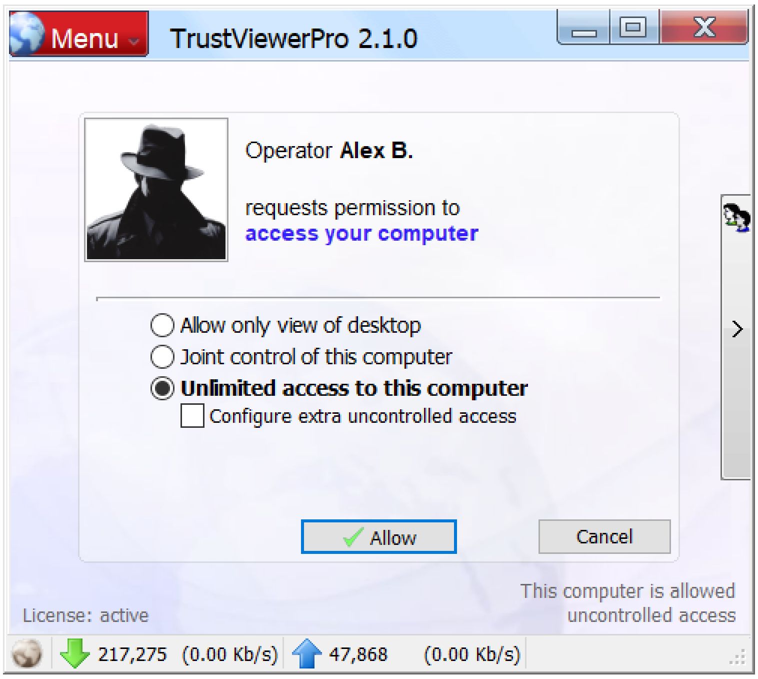
This computer is allowed
uncontrolled access

1,156,950 (0.00 Kb/s) 69,682 (0.00 Kb/s)

Any user, even unauthorized, can initiate a connection to his computer: create an invitation to access using a temporary ID, or apply for helpdesk service. To provide access to your computer, the user should open the main form of the program (by launching the corresponding icon on the desktop, or by clicking the left mouse button on the program icon in the tray), this will display a temporary session ID that needs to be communicated to the operator, as well as a link to open application forms for the helpdesk. While waiting for a connection to his computer - the user can minimize the program window, while the current session will not be interrupted. However, if the user clicks the “Cancel” button, the current session will be terminated.

Attention! Here the user can also allow temporary access to his computer without confirmation, for this purpose it is necessary to click on the icon with the image of the key (to the left of the ID field), set an arbitrary password, and report it along with the ID to the operator. Also, the password for access without confirmation can be set by default in the program settings on the “Security " tab.

6.2.1. Granting access using a temporary ID



Operator **Alex B.**

requests permission to
access your computer

○ Allow only view of desktop
○ Joint control of this computer
● **Unlimited access to this computer**
☐ Configure extra uncontrolled access

License: active

This computer is allowed
uncontrolled access

217,275 (0.00 Kb/s) 47,868 (0.00 Kb/s)

After the operator has received a session ID from the user, and with its help initiated a connection to a remote computer, a confirmation form will open on the user’s side, where you can select the access granting mode.

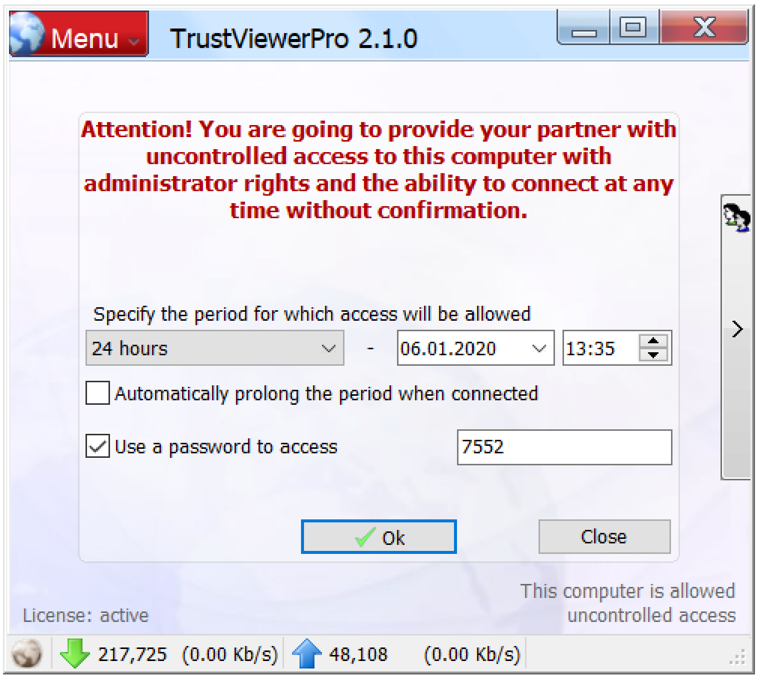
The following are the possible modes of providing access to a computer.

Access mode	Description
Allow only view of desktop	The operator will only be able to observe the actions of the user of the remote computer, he will not be able to control the computer himself.
Joint control of this computer	Both the operator and the user can control the computer at the same time, however, for the operator to perform operations related to the files and the clipboard, confirmation from the user is required.
Unlimited access to this computer	The operator gets full access to the computer, including access to the file system and the clipboard without the need for confirmation from the user.

Attention! It uses a temporary ID unique for each new communication session. In case of expiration of the identifier, it is necessary to initiate a new communication session, and, accordingly, inform the operator of the new temporary identifier.

Attention! Using the TrustServer server control panel, you can limit the level of access to remote computers for each individual operator. In this case, depending on the access level of the operator, here some modes of providing access to the computer will be blocked. In addition, the server can also set the default access mode, both for all unauthorized users, and for certain groups of authorized users (specified in the properties of the group account).

In addition, in the case of a user-selected mode of unrestricted access to your computer, here you can configure the provision of temporary uncontrolled access to the computer to the current operator. In this case, after the end of the current communication session, the operator will be able to temporarily connect to the computer without the need for confirmation from the user, including managing the computer after a reboot. To configure uncontrolled access - the user must tick the “Configure uncontrolled access” checkbox and click the “Accept” button, after which the corresponding setup form will be displayed.



Attention! You are going to provide your partner with uncontrolled access to this computer with administrator rights and the ability to connect at any time without confirmation.

Specify the period for which access will be allowed

24 hours - 06.01.2020 13:35

☐ Automatically prolong the period when connected

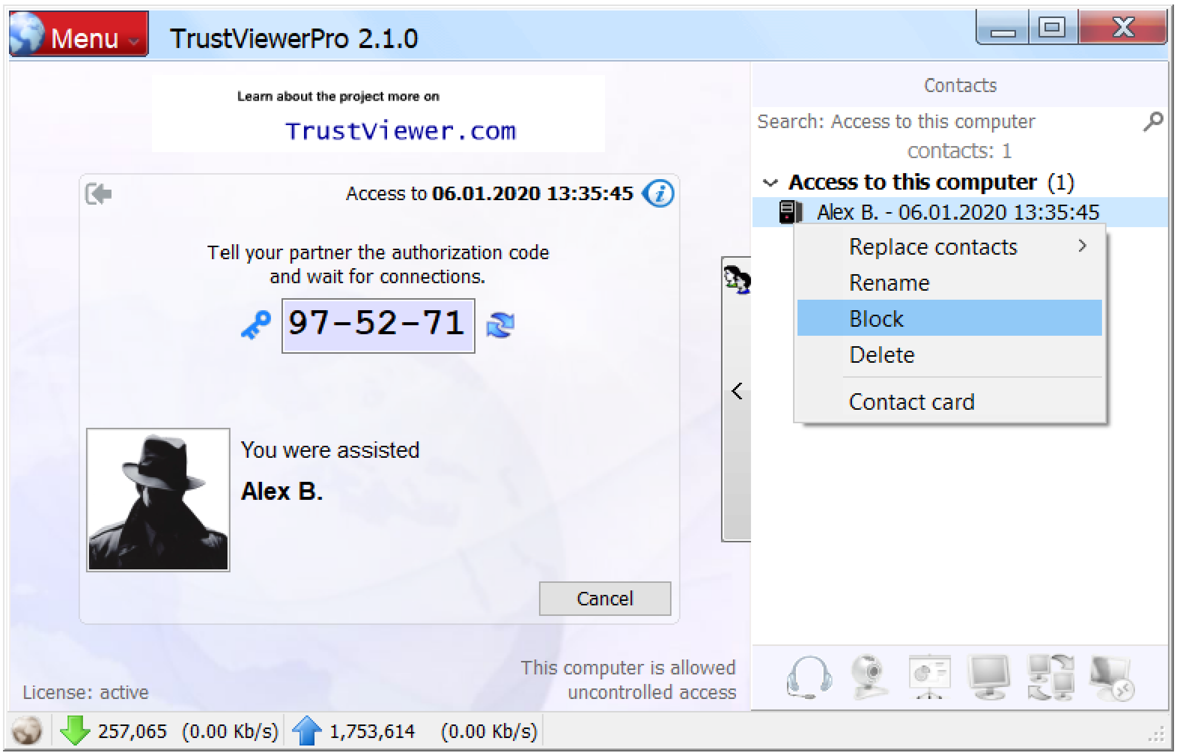
☑ Use a password to access 7552

License: active

This computer is allowed uncontrolled access

217,725 (0.00 Kb/s) 48,108 (0.00 Kb/s)

Here you need to specify the period for which access will be granted, as well as, if necessary, set a password for access to the computer. If the “Automatically prolong the period when connected" flag is not selected, then after the expiration date - uncontrolled access for the current operator will be automatically blocked. In addition, the user can cancel access at any time manually, to do this, display the contacts panel (click the button on the right side of the main form of the program), expand the “Access to this computer” group, find and highlight the required operator (for one computer can simultaneously several uncontrolled accesses for different operators can be provided), right-click the context menu, and click “Block” or “Delete”.



Learn about the project more on TrustViewer.com

Access to **06.01.2020 13:35:45**

Tell your partner the authorization code and wait for connections.

97-52-71

You were assisted

Alex B.

This computer is allowed uncontrolled access

License: active

257,065 (0.00 Kb/s) 1,753,614 (0.00 Kb/s)

Search: Access to this computer

contacts: 1

Access to this computer (1)

Alex B. - 06.01.2020 13:35:45

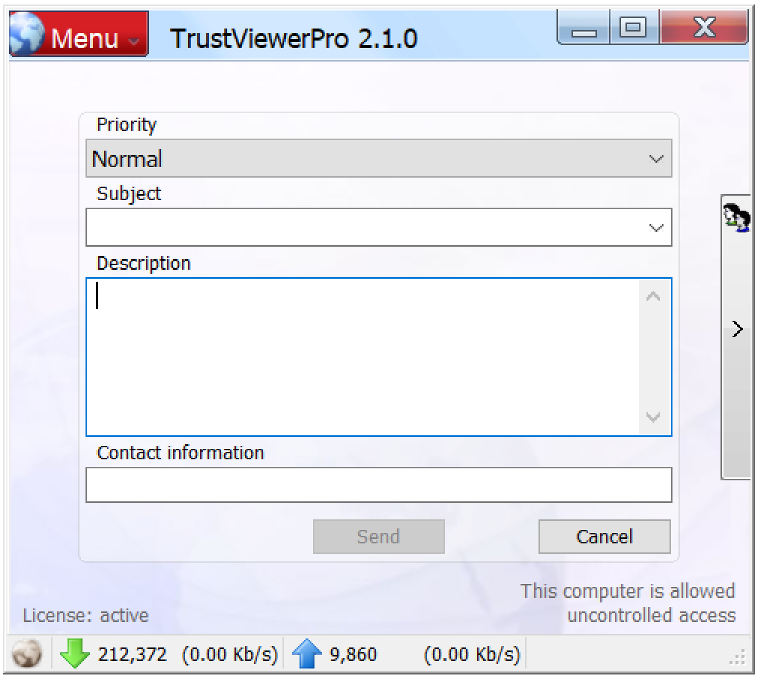
Attention! After the end of the session, the old session ID is still valid, so it is possible to easily reconnect without having to tell the operator a new ID. To end the current session and assign a new ID, click the “Cancel" button here.

6.2.2. Providing access through the application to the helpdesk service

Attention! To enable the user to submit an application to the helpdesk service, the corresponding settings must be made on the TrustServer server (for more details, see “Configure integration with Helpdesk / Service desk services” in the “Administration of the TrustServer server” section of this manual)

Attention! To submit an application to the helpdesk service, the operators (if they have the appropriate rights) can request access to the remote computer during the entire lifetime of the active application.

To submit an application to the helpdesk service, the user must click on the link “Application to helpdesk” located under the temporary identifier field on the main form of the program. At the same time, depending on the TrustServer server settings, either the built-in simplified application form will open, or a window with the form of the configured helpdesk service, or a page in the default browser with the corresponding form. Following is a variant of using the built-in simplified application form.



Priority: Normal

Subject

Description

Contact information

This computer is allowed uncontrolled access

License: active

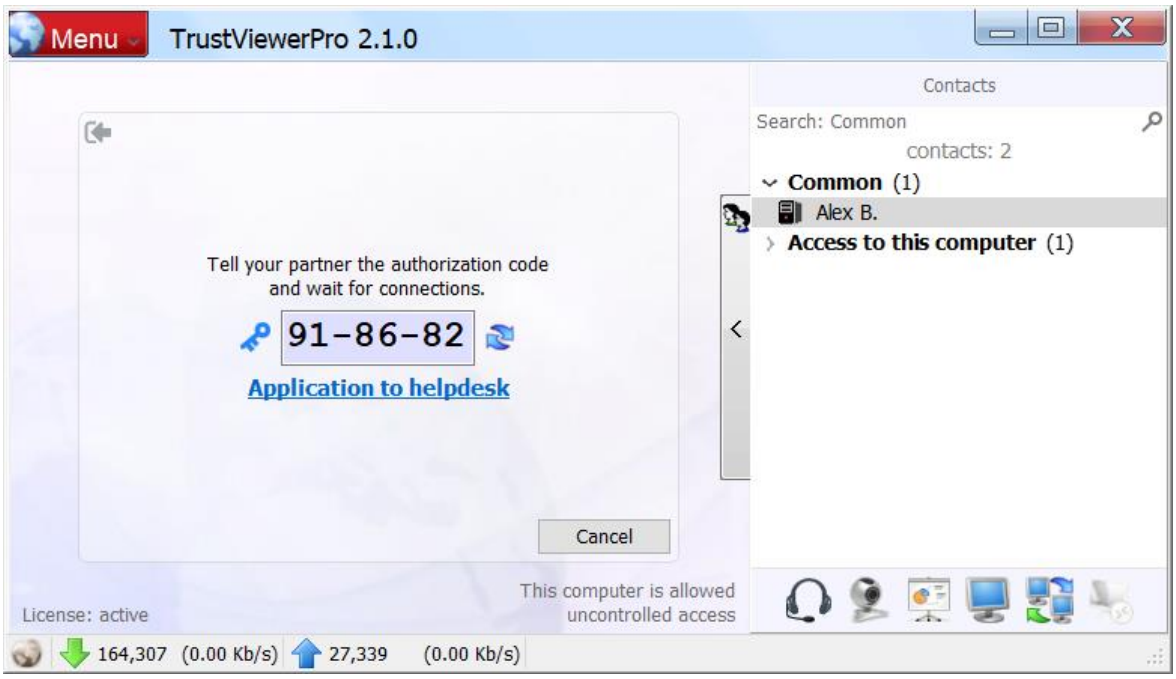
Here you need to specify the priority of the request (choose from the list one of the options - “Low”, “Normal”, “High” or “Maximum”), fill in the “Subject” field (enter a new value or select from the list of saved), fill in the “Description” ”(In case the“ Subject ”field was chosen from the list of saved, this field will also be filled automatically), as well as the“ Contact information ”field (this field will be automatically filled with the value from the previous application). After filling in all the fields of the form, you must click the “Send” button and wait for the connection to be established by the operator (before connecting, as well as in the case of providing access by ID - the confirmation form will be opened, where you can choose the mode of providing access).

Attention! Since the application submitted provides access to the user's computer without time limit (access is given for the duration of the application, i.e., until it is processed or revoked), for security reasons, it can be open for each user at the same time Only one active application. Check the fact of the presence of an active open application, as well as cancel the current application - the user can at any time on the main form of the program.

6.2.3. Providing access using the contact list

During an active communication session, established with a temporary ID or request to the helpdesk service, the user and the operator can exchange contact information (create contact cards). In this case, the user can at any time send an invitation to access your computer using the contact card of the operator, you need to display the contact panel (click on the button on the right side of the main form of the program), find and select the desired operator, wait for a positive response from the remote computer (in the access panel should be activated buttons for appropriate requests), click on the “desktop Demonstration” (icon presentation), and wait for the connection operator. Here the user can block or delete the contact of the operator, for this you need to select the desired operator, call the right mouse button context menu, and click “Lock” or “Delete”

Attention! In the “Desktop demonstration” access mode, the operator will only be allowed to view the desktop, without being able to control the remote computer, however, during a communication session, the operator can request an increase in access level.



Tell your partner the authorization code and wait for connections.

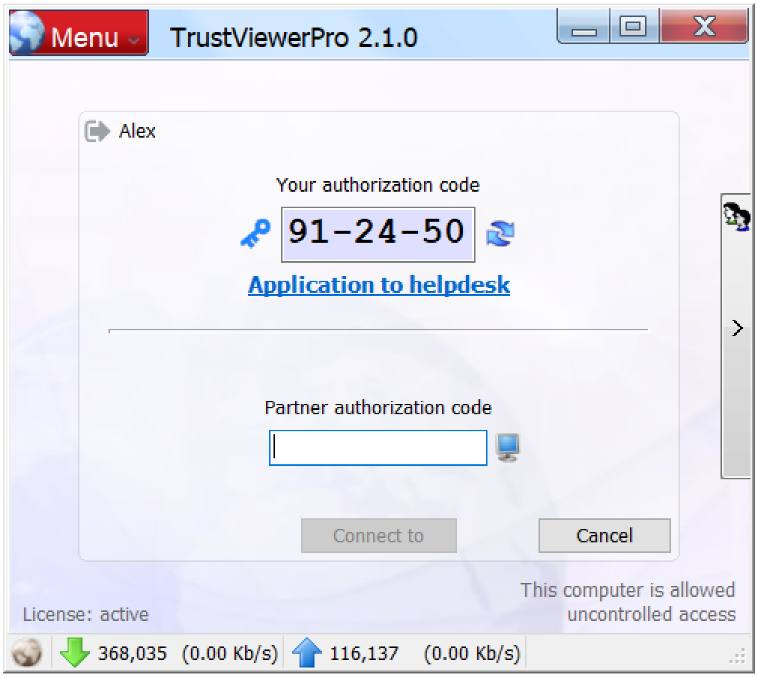
91-86-82

Application to helpdesk

License: active

This computer is allowed uncontrolled access

6.3. Work with the «TrustViewerPro» client module in the operator mode



Your authorization code

91-24-50

Application to helpdesk

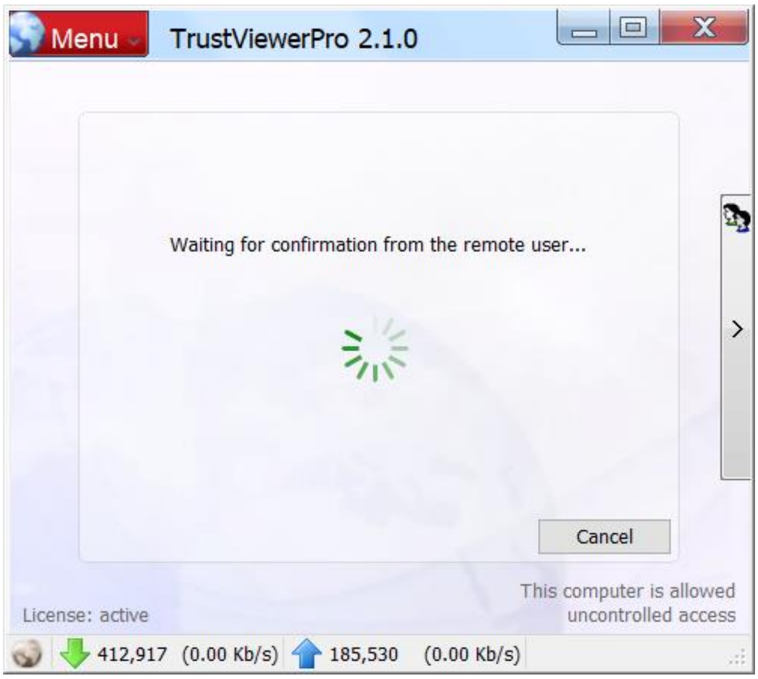
Partner authorization code

License: active

This computer is allowed uncontrolled access

An authorized user with operator rights can connect to remote computers using the temporary session ID given to him, to do this, open the main form of the program (by launching the corresponding icon on the desktop, or by left-clicking the program icon in the tray), enter the session ID and click button “Connect”.

Attention! In addition to the default session mode “Remote Desktop” - the operator here can also select an additional session mode (“Voice”, “Video call”, “Desktop demo”, “File and folder sharing”) for To do this, click the button to the right of the identifier entry field, and select the required mode in the drop-down list.



Waiting for confirmation from the remote user...

This computer is allowed uncontrolled access

After that, a form of waiting for confirmation of connection from the user's side of the remote computer will open, on which the operator, if necessary, can send an instant message to the user. Also, if the remote user has set an access password without confirmation, you can enter the access password here and immediately start a communication session.

After confirming the connection by the user of the remote computer, depending on the mode of access granted, the session will start either with the ability to only view the remote desktop, or with the possibility of joint control of the computer, or in the mode of unlimited access to the computer.

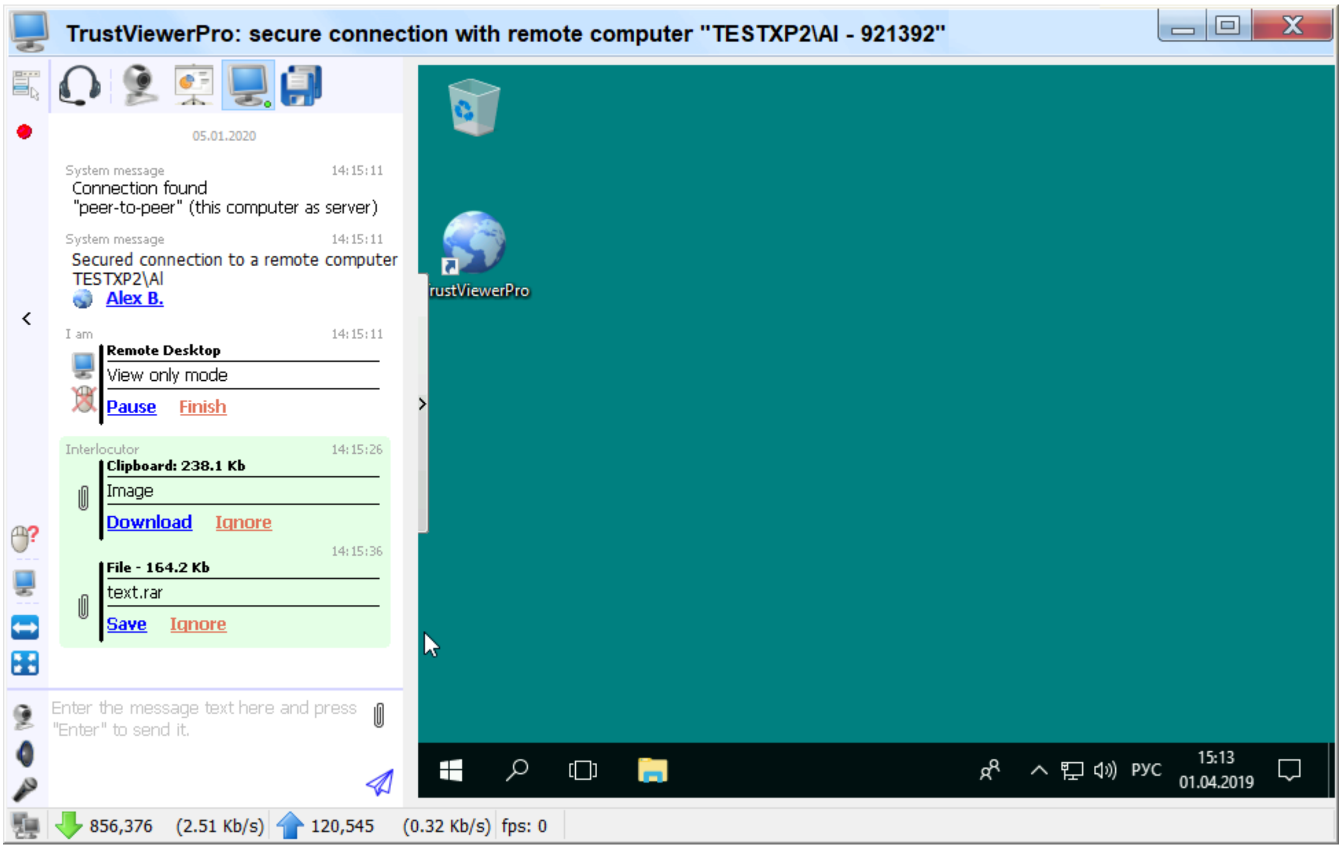
Attention! The level of access to a remote computer at each new session is selected directly by the user of this computer during the confirmation of the request for access. Moreover, during a communication session, the operator may request an increase in the access level, however, in any case, the user of the remote computer cannot select the access level to his computer above the value specified in the operator profile card (for the “Operator rights to remote control” setting, see in the “User Management”, in the “Administration of the TrustServer Server” section of this manual).

After a successful connection, in addition to direc control the remote computer, both for the operator and the user, additional modes of interaction will be available. In general, the interface with the remote computer is implemented in the “single window” version, with the ability to quickly switch between the active presentation modes: “Video call”, “Desktop demo”, “Remote desktop”, “File sharing and folders” (there is also a “Voice communication” mode, which does not have a separate presentation and works together with the other modes, i.e., the initiated audio call will be active during the entire communication session regardless of the current presentation mode). To switch between active modes, just click on the corresponding button (the active mode is indicated by a green circle in the lower right corner of the corresponding button). In addition, when you hover the mouse over the mode button, a context menu is displayed in which, depending on the type and status of the marked mode, you can perform the following actions: send invitation (request for activation of the mode requires confirmation from the partner, except in the case of unlimited access to the computer), pause/end the action of the mode, and also, for the mode “Sharing of files and folders” - add/cancel sharing of files and folders.

In the event that the parties exchanged contacts during a communication session, the operator may at any time send an access request to the user of the remote computer using the contacts panel. In addition, if the operator was provided with temporary uncontrolled access, then using the contact panel, the operator can also connect to a remote computer, but without confirmation from the user.

6.3.1. Communication session in desktop view only

In the desktop view only mode, the operator cannot control the remote computer using the mouse and keyboard, and file and clipboard operations require confirmation from the user of the remote computer.



TrustViewerPro: secure connection with remote computer "TESTXP2\AI - 921392"

05.01.2020

System message 14:15:11
Connection found
"peer-to-peer" (this computer as server)

System message 14:15:11
Secured connection to a remote computer
TESTXP2\AI
Alex B.

I am 14:15:11
Remote Desktop
View only mode
Pause Finish

Interlocutor 14:15:26
Clipboard: 238.1 Kb
Image
Download Ignore

14:15:36
File - 164.2 Kb
text.rar
Save Ignore

Enter the message text here and press "Enter" to send it.

856,376 (2.51 Kb/s) 120,545 (0.32 Kb/s) fps: 0

The following are the button assignments on the session control panel in the desktop view only mode.

Button	Description
Menu	Opens the session management menu: • "Information on onnection" - displays the current connection information • "System Information" - displays information about the system of local and remote computers • "Messages archive" - displays the archive of messages • "Create contact" - opens the contact card creation dialog • "Request for uncontrolled access" - sends a request for uncontrollable access to a remote computer user • "New connection" - initiates a new communication session without closing the current • "End session connection" - ends the current connection
●	Start recording a session (not available if centralized recording is enabled on the server, in which case recording will start automatically)
Voice communication	Audio Call Control
Video call	View Switching / Video call mode control
Desktop demo	View Switching / Desktop Demo Mode Control
Remote Desktop	View Switching / Remote Desktop Control
Sharing files and folders	View Switching / Manage file and folder sharing mode
Hide / Show Chat	Hides / displays chat panel

< Panel	
Management Request	Sends a remote access request to a remote computer user (permission to share control or unlimited access)
Settings	Setting the options for transferring images of a remote desktop (monitor selection, compression algorithm, fps, etc.)
On / Off fit size	Toggles the display mode of the remote desktop image: true size or fitted size
On / Off full screen	Toggles the interface display mode: full screen or windowed mode
Camera settings	Opens the webcam control menu, with the ability to select the active device, as well as settings for additional options defined by the system
Speaker settings	Opens the control menu of the audio playback device, with the possibility of selecting the active device, as well as setting additional options defined by the system
Microphone settings	Opens the control menu of the sound recorder, with the possibility of selecting the active device, as well as setting additional options defined by the system
Send clipboard or files	Opens a menu with the ability to send files or clipboard contents to a remote computer, as well as enable / disable compression mode during data transfer
➢	Sends the message entered in the chat

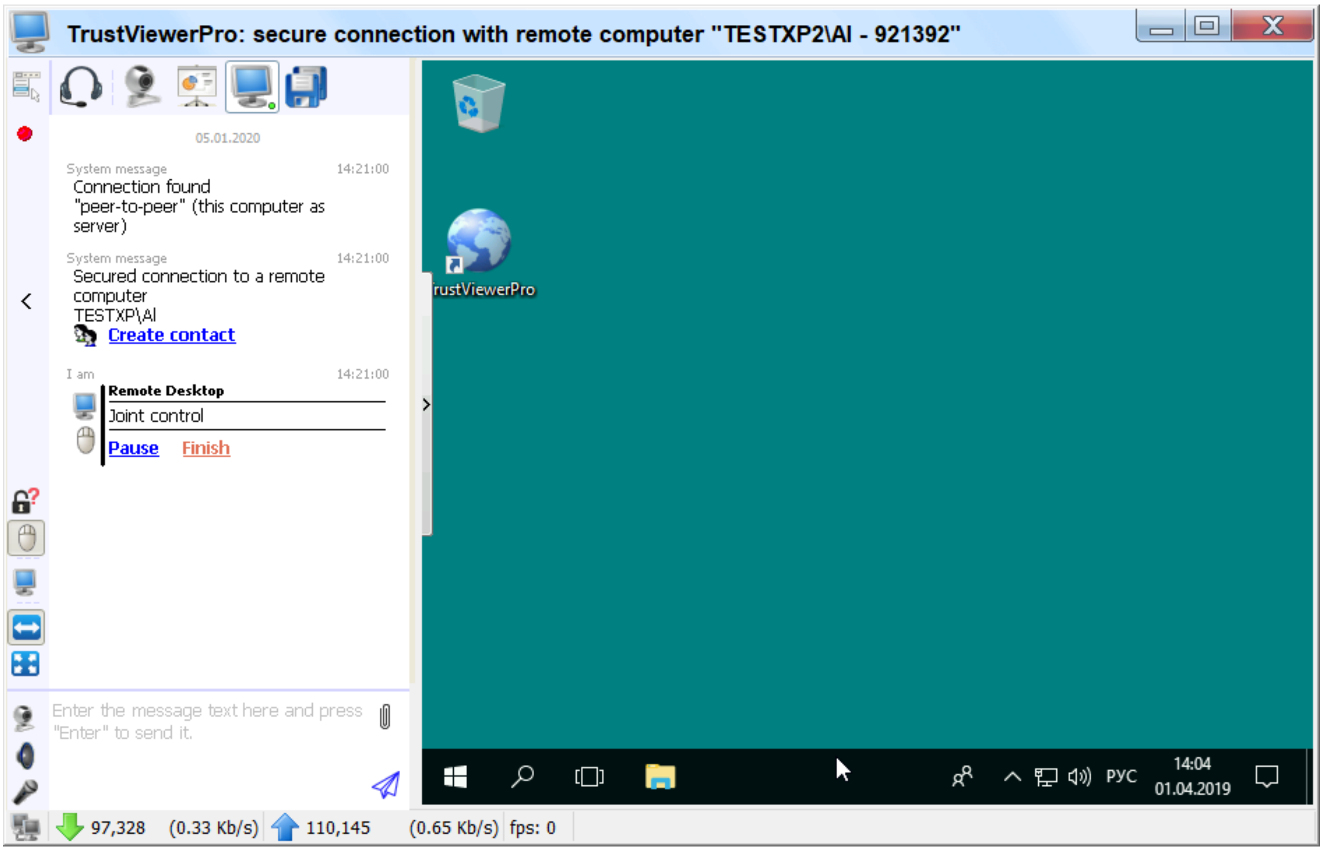
To transfer favorite files or clipboard contents from a remote computer to the operator’s computer - the user of the remote computer must open the chat panel (by pointing the cursor on the arrow button on the left side of the screen, or clicking the tray icon on the presentation icon), click the “Send clipboard or files” (with a paperclip image) and select“ Send clipboard ”or“ Send files and folders ”accordingly. After that, the corresponding entries will appear in the operator's chat with information about the downloaded files or the contents of the clipboard. To load the contents of the clipboard - the operator must first click “Download” on the corresponding record, and then “Put in the clipboard” (it is possible to repeatedly place the previously downloaded clipboard contents of the remote computer into the buffer). To download files and folders - the operator must click “Save” on the corresponding chat entry, after which the dialog for selecting the destination folder will open, and when it is closed, the files will be downloaded to the specified folder. Transfer of selected files and clipboard contents from the operator’s computer to the remote computer is carried out in a similar way. In addition, to transfer files in both directions - you can use the “File and folder sharing” view mode, in which both the user and the operator can provide access to their selected files / folders / drives or the entire file system at once, as in read-only mode, and with the possibility of making changes (for more details, see the “View mode “File and folder sharing” section, see the “Work with the client module «TrustViewerPro»” section of this manual).

Attention! During a session, the previously used session ID is still valid, so it can be shared with another operator for viewing/control the remote desktop (the current valid ID is displayed in the view window header).

Attention! If centralized record storage is enabled on the server, a special seven-digit broadcast ID is specified in the chat, as well as in the header of the view window, which can be used by other operators to view the current communication session (the specified broadcast ID must be entered on the main form of the program instead of the usual session ID).

6.3.2. Communication session in the joint computer control mode

In the joint control mode, the operator can control the remote computer using the mouse and keyboard, but operations related to files and the clipboard, as well as in the case of connection in the desktop view only mode, require confirmation from the user of the remote computer.



TrustViewerPro: secure connection with remote computer "TESTXP2\AI - 921392"

05.01.2020

System message 14:21:00
Connection found "peer-to-peer" (this computer as server)

System message 14:21:00
Secured connection to a remote computer TESTXP\AI
Create contact

I am 14:21:00
Remote Desktop
Joint control
Pause Finish

Enter the message text here and press "Enter" to send it.

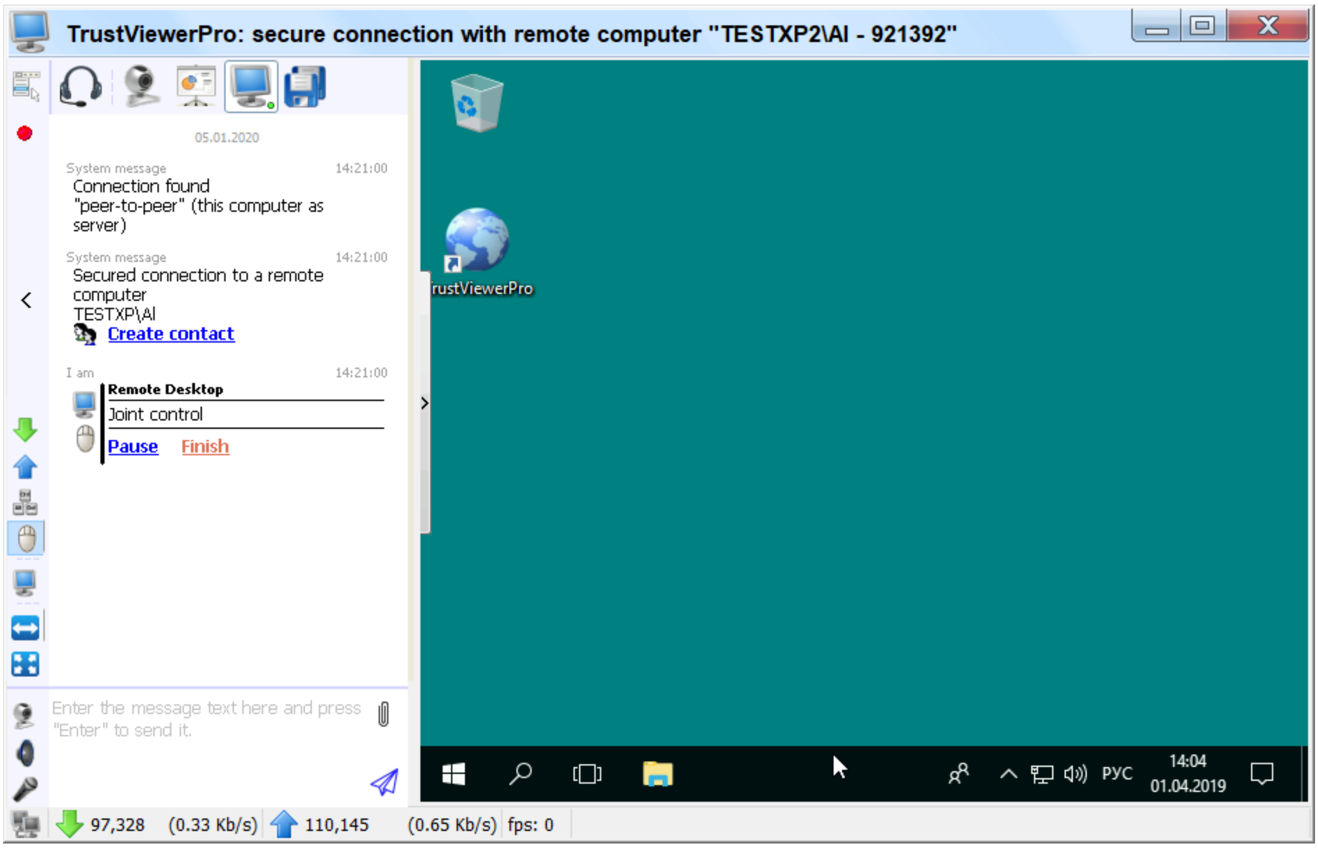
97,328 (0.33 Kb/s) 110,145 (0.65 Kb/s) fps: 0

The arrangement and purpose of the buttons on the control panel of a communication session in the joint control mode are the same as in the mode of viewing the desktop only, with the exception of two buttons:

Button	Description
On / off control	Enables / disables remote computer control with a mouse and keyboard.
Request for full access	Sends a request to increase the access level to a remote computer user (permission for unlimited access)

6.3.3. Communication session in the mode of full access to the computer

In the full access mode, the operator can not only control the remote computer using the mouse and keyboard, but also perform operations related to files and the clipboard without confirmation from the user of the remote computer.



TrustViewerPro: secure connection with remote computer "TESTXP2\AI - 921392"

05.01.2020

System message 14:21:00
Connection found "peer-to-peer" (this computer as server)

System message 14:21:00
Secured connection to a remote computer TESTXP\AI
Create contact

I am 14:21:00
Remote Desktop
Joint control
Pause Finish

Enter the message text here and press "Enter" to send it.

97,328 (0.33 Kb/s) 110,145 (0.65 Kb/s) fps: 0

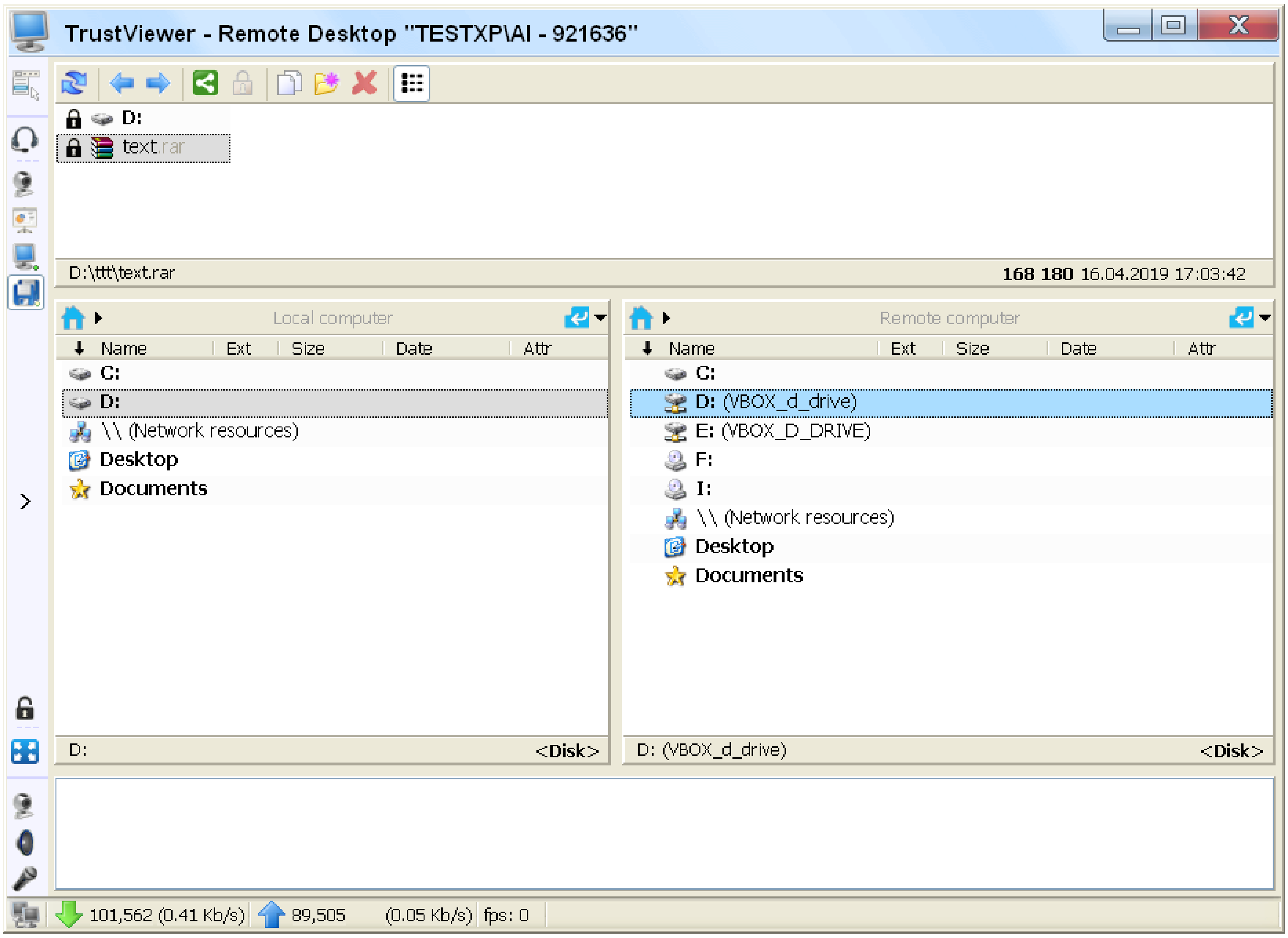
The location and purpose of the buttons on the control panel of a communication session in the full access mode are the same as in the joint control mode, with the exception of three buttons:

Button	Description
⬇ Download clipboard or files	Loads the current clipboard content from a remote computer (if the clipboard contains files, the file saving dialog will be called)
⬆ Send clipboard or files	Sends the current clipboard content to the remote computer (if the clipboard contains files, the file saving dialog will be called on the computer remotely)
Send Ctrl-Alt-Del	Sends a Ctrl-Alt-Del keyboard shortcut to a remote computer

Attention! In case of granting full access, the operator also automatically gets full access to the entire file system of the remote computer using the “File and folder sharing” view mode.

6.3.4. View mode “File and folder sharing”

In the “File and Folder Sharing” view, both the operator and the user of the remote computer can provide access to their favorite files / folders / drives or the entire file system at once, both in read-only mode and with making changes. To switch from the “Remote Desktop” view mode to the “File and Folder Sharing” mode and back, simply click on the corresponding button on the control panel of the communication session. Visually, the file and folder sharing management interface is divided into four parts: the top one contains a common control and navigation panel, as well as a panel with a list of all current public objects of the local computer, the left one is a panel for navigating through the local computer file system, the right one - to navigate through the file system of a remote computer, the bottom - displays a queue of transmitted objects.



Following are the descriptions of the buttons on the navigation / control panel.

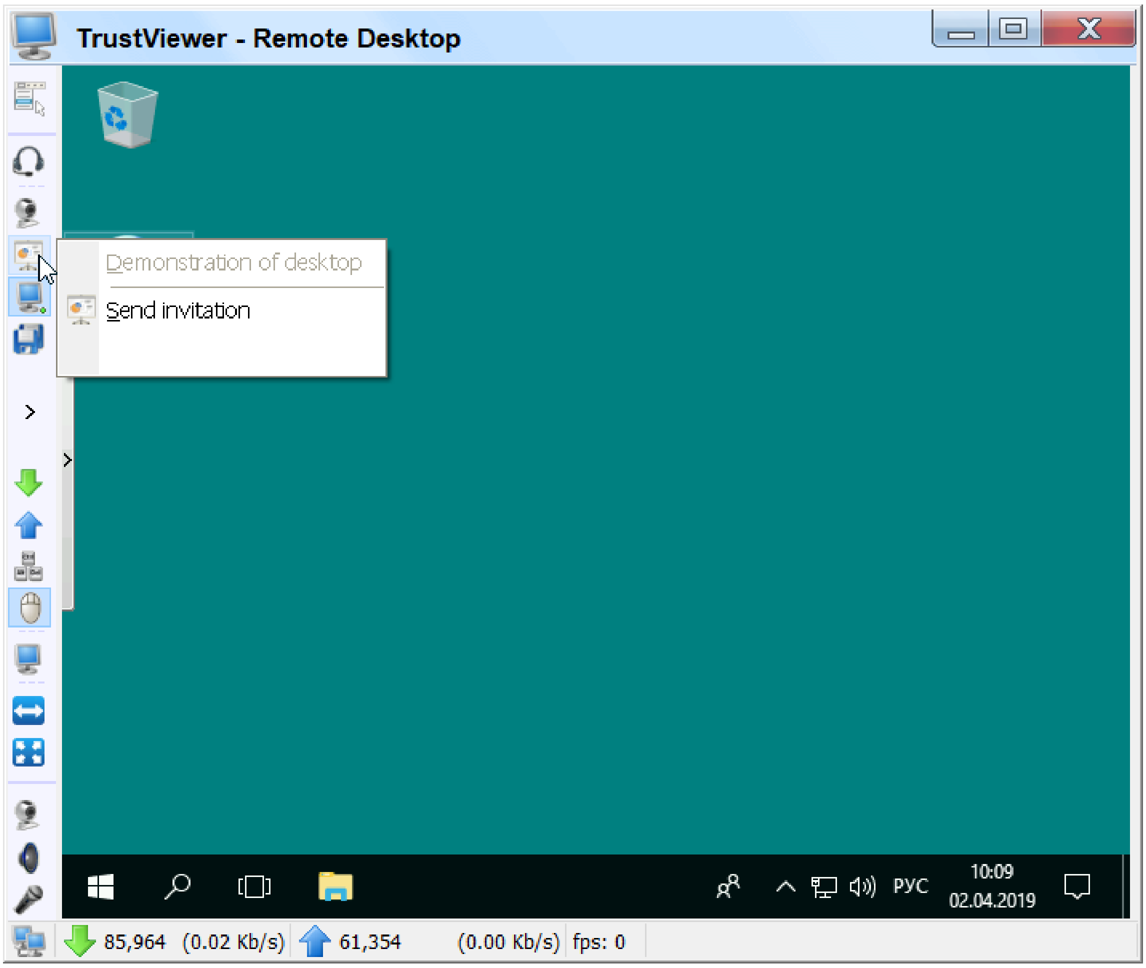
Button	Description
Update panel content	Updates the contents of the current active panel.
Forward	Move to the previous folder of the navigation history of the current active panel.
Back	Move to the next folder in the navigation history of the current active panel.
Shared access	Opens a dialog to select files / folders / disks of the local computer that will become publicly available (if you select the “This computer” object, access will be open to the entire file system, and if the “Add with read-only rights” checkbox is not selected, then full access, with the possibility of making changes).
Read Only Access	Enables / disables the read-only mode for the currently selected shared object.
Transfer to another computer	Copies marked objects from local to remote, or from remote to local computer, depending on the currently active panel.
Create a new folder	Creates a new folder on a local or remote computer.
Delete	Removes marked objects on a local or remote computer.
Detailed view	Turns on / off a detailed view of the display for the current active panel.

In addition, in the “File and Folder Sharing” view mode, an additional button has been added to the session control panel:

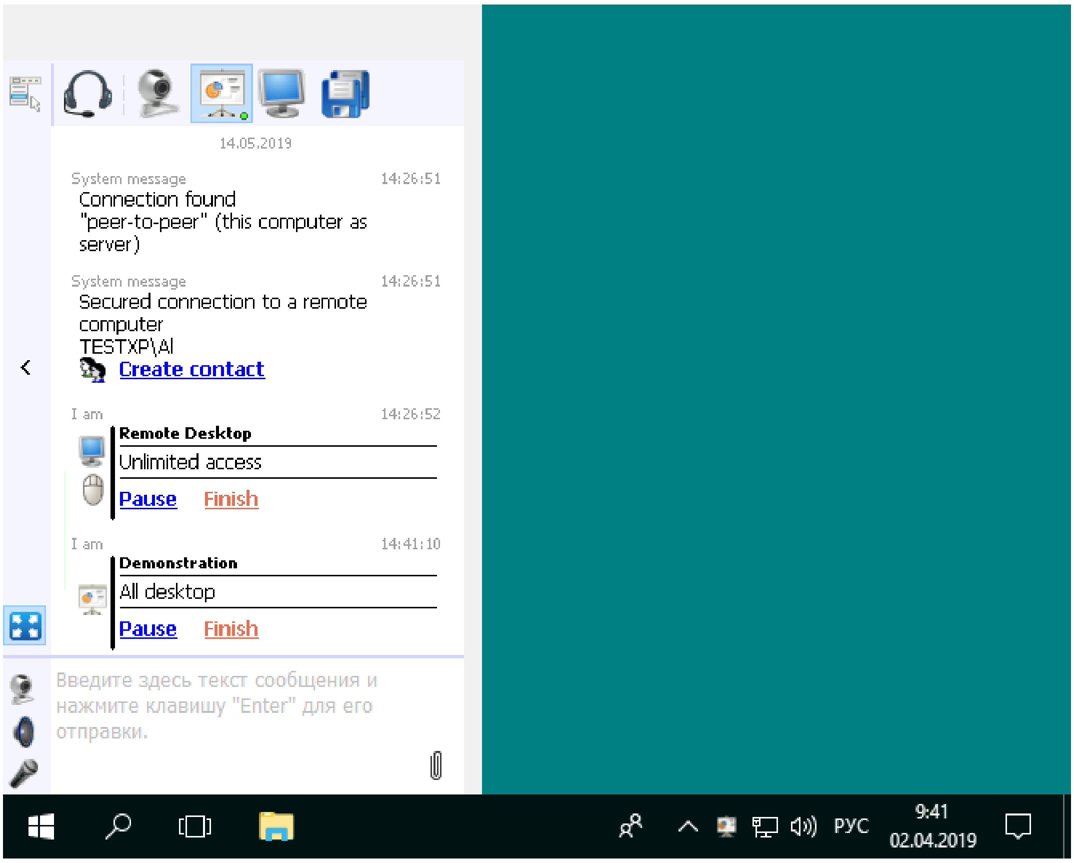
Button	Description
On / Off full file access	Enables / disables full access to the entire file system of the local computer with the ability to make changes (this mode is enabled by default on the remote computer when connected to it in a session with full access rights).

6.3.5. Presentation mode “Desktop demonstration”

In the “Desktop demonstration” view mode, an operator can show his desktop to a remote computer user without having to initiate a new communication session. To start demonstration of your desktop, in the control panel of the communication session, move the mouse cursor over the “Desktop demonstration” button (with the presentation image), select “Send invitation” and wait for confirmation from the user of the remote computer (in the case of a full access session) - confirmation from the user is not required).



To switch from the “Remote Desktop” view mode to the “Desktop Display” mode and back, just click the corresponding button on the communication session control panel (to display the control panel, you must hover the mouse cursor over the button on the left of the screen).



14.05.2019

System message 14:26:51
Connection found
"peer-to-peer" (this computer as server)

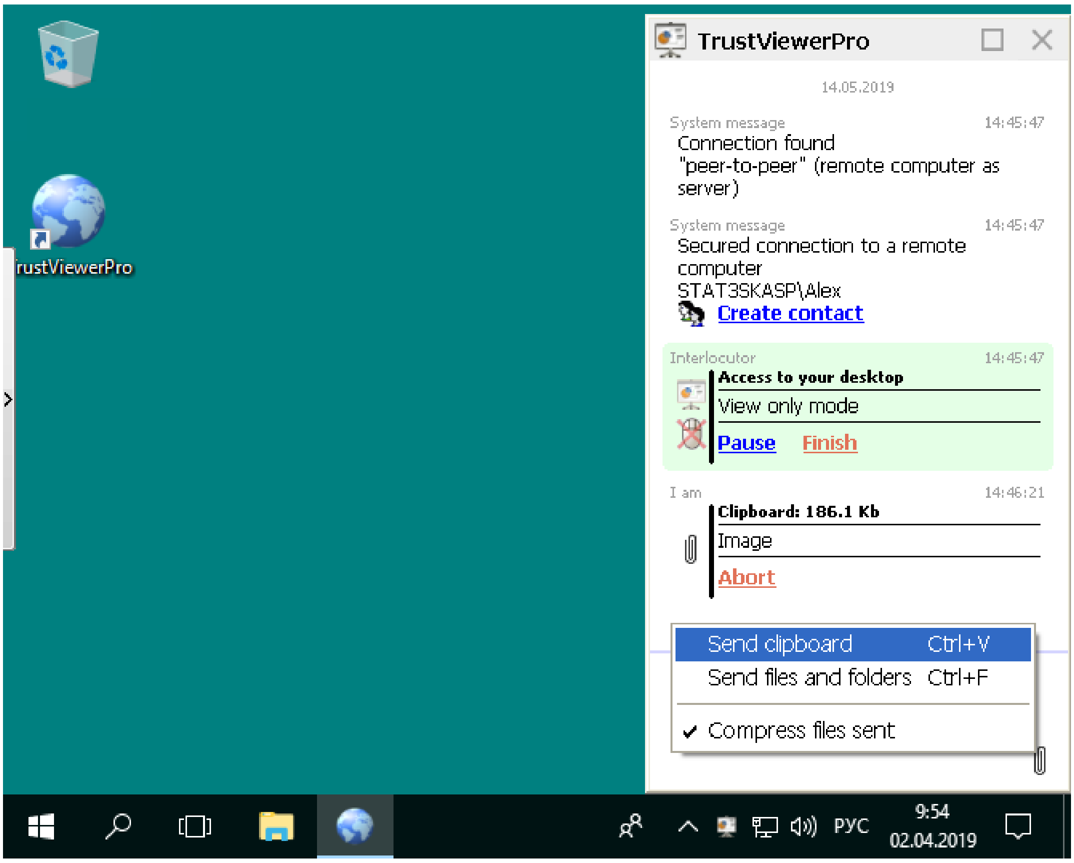
System message 14:26:51
Secured connection to a remote computer
TESTXP\Al

I am 14:26:52
Remote Desktop
Unlimited access

I am 14:41:10
Demonstration
All desktop

Create contact
Pause
Finish
Pause
Finish
Введите здесь текст сообщения и нажмите клавишу "Enter" для его отправки.
РУС
9:41
02.04.2019

To send messages, files or clipboard content to a remote computer - the operator can also use an additional chat window displayed when clicking on the tray presentation icon.



14.05.2019

System message 14:45:47
Connection found
"peer-to-peer" (remote computer as server)

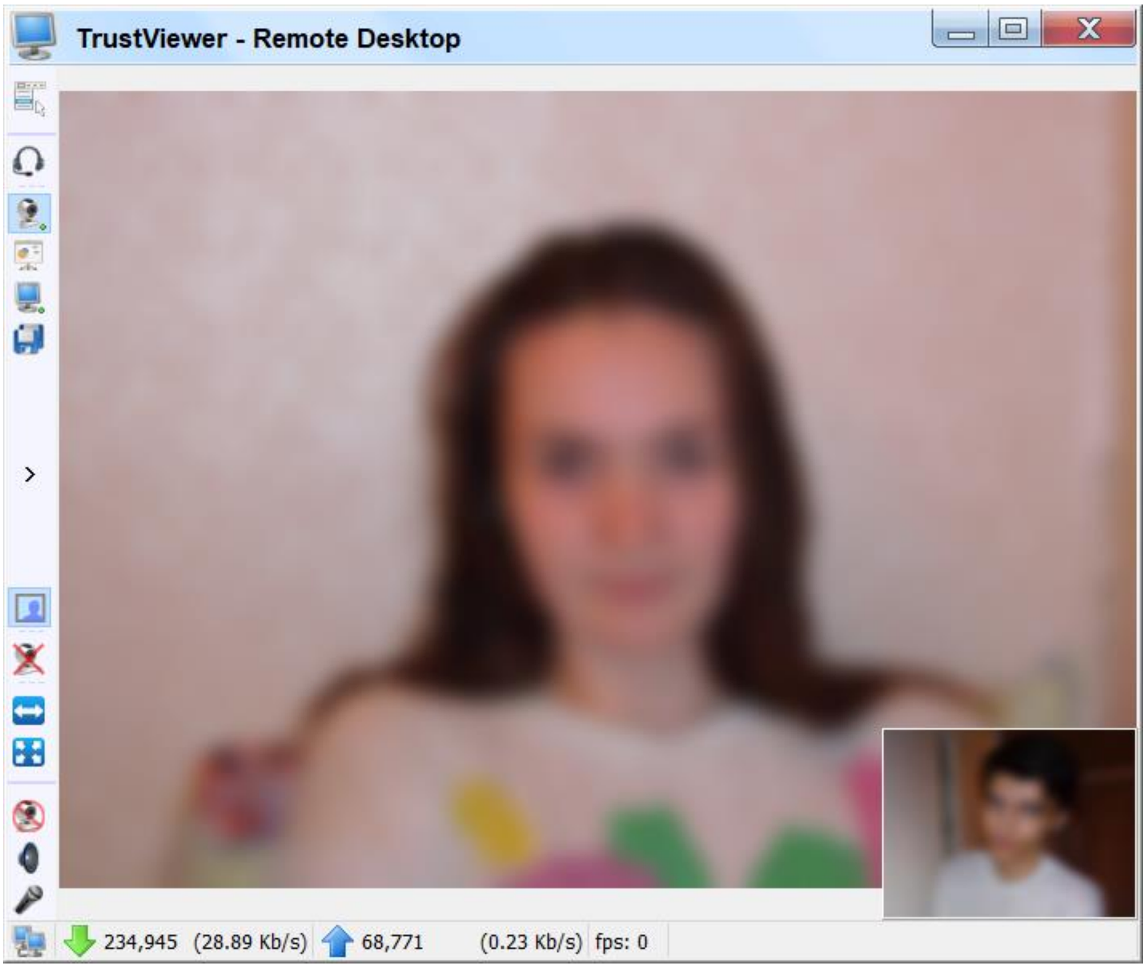
System message 14:45:47
Secured connection to a remote computer
STAT3SKASP\Alex

Interlocutor 14:45:47
Access to your desktop
View only mode

I am 14:46:21
Clipboard: 186.1 Kb
Image

6.3.6. View mode “Video call”

In the “Video call” view mode, the operator and the user of the remote computer can communicate via video connection. To start a video call - in the control panel of a communication session, hover the mouse over the “Video call” button (with a webcam image), select “Send invitation” and wait for confirmation from the user of the remote computer. To switch from the “Remote Desktop” view mode to the “Video Call” mode and back, just click on the corresponding button on the communication session control panel.



The location and purpose of the buttons on the session control panel in the video call view are the same as in the remote desktop view, with the exception of two buttons:

Button	Description
👤 On / off preview	Enables / disables the local webcam image preview
📷	Setting options for transferring images of a remote webcam (resolution, fps, etc.)
◢	Volume control for audio signal transmitted from a remote computer.
🔈	Setting the transmission options of the audio signal transmitted from a remote computer (use of additional audio signal processing algorithms)

6.3.7. Voice mode

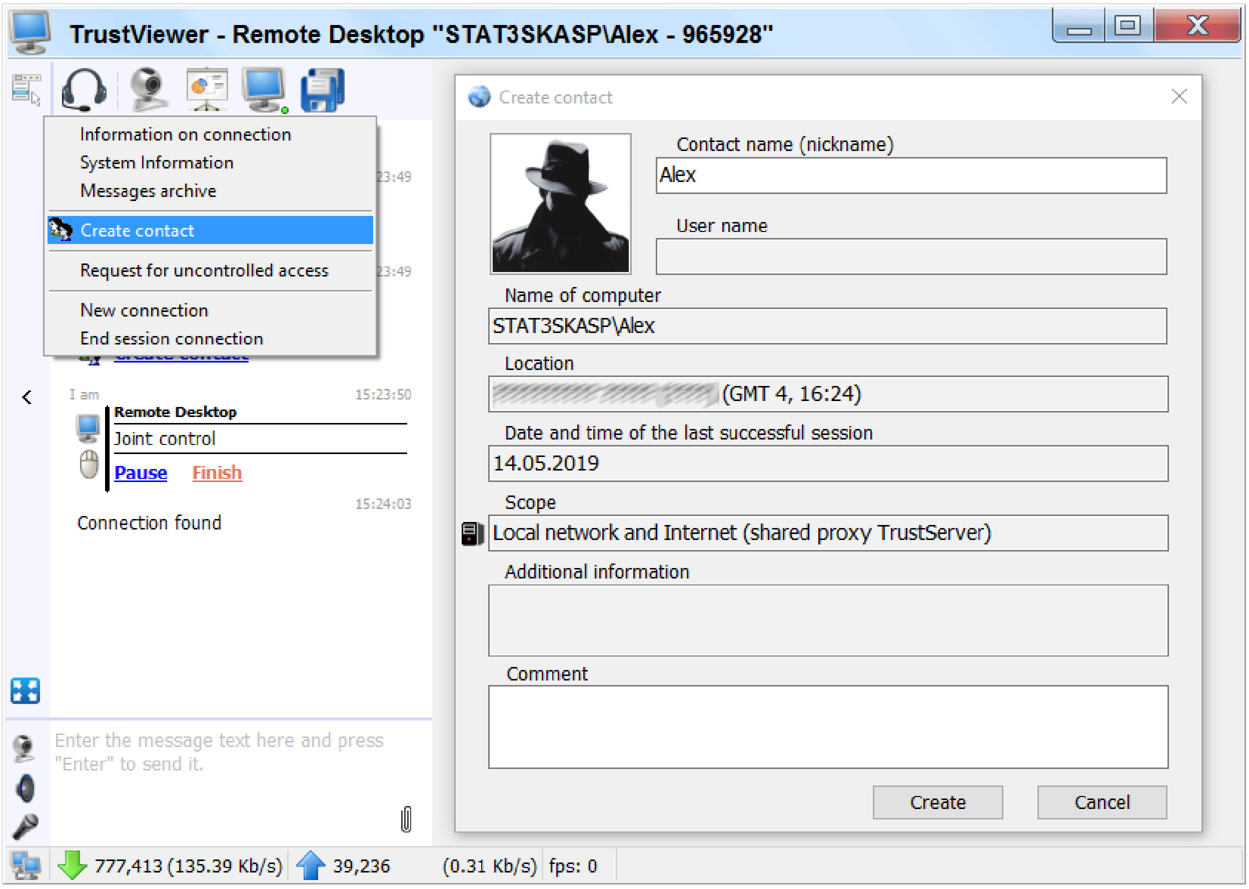
The “Voice communication” mode is intended for communication between the operator and the user of the remote computer via an audio call. The “Voice Communication” mode does not have a separate presentation and operates in parallel with the other modes (i.e., the initiated audio call will be active during the entire communication session regardless of the current presentation mode). To start an audio call, in the control panel of a communication session, move the mouse cursor over the Voice button (with a headset image), select “Send invitation” and wait for confirmation from the user of the remote computer. In the audio call mode, in the session control panel in each view, additional buttons are added:

Button	Description
◢	Volume control for audio signal transmitted from a remote computer.
🔈	Setting the transmission options of the audio signal transmitted from a remote computer (use of additional audio signal processing algorithms)

6.3.8. Connecting to a remote computer using the contact list

In addition to connection by ID, the operator can also connect to a remote computer using the “safe contacts”. Such contacts can be created only during a trusted communication session, they are protected by asymmetric keys associated with the computer hardware and the profile of the Windows system user account, and automatically updated after each communication session. Such contacts cannot be forged and even copied to another computer, so they are safe to use even in compatibility mode with the “TrustViewer” software product that uses public servers to connect.

To exchange contact data (create contact cards) - the operator must select “Create contact” in the session management menu (or click on the corresponding entry in the chat following the system notification of successful connection to the computer) during a normal communication session, then a new contact card form will open, in which you need to fill in the “Contact Name” field (you can also fill in the optional “Comment” field), and click the “Create” button. After creating a contact on the operator’s side, the same form will open on the user’s side of the remote computer, which must be filled out and confirmed in the same way.


TrustViewer - Remote Desktop "STAT3SKASP\Alex - 965928"
Information on connection
System Information
Messages archive
Create contact
Request for uncontrolled access
New connection
End session connection
23:49
23:49
Create contact
Pause
Finish
Enter the message text here and press "Enter" to send it.
Create
Cancel

I am 15:23:50
Remote Desktop
Joint control

15:24:03
Connection found

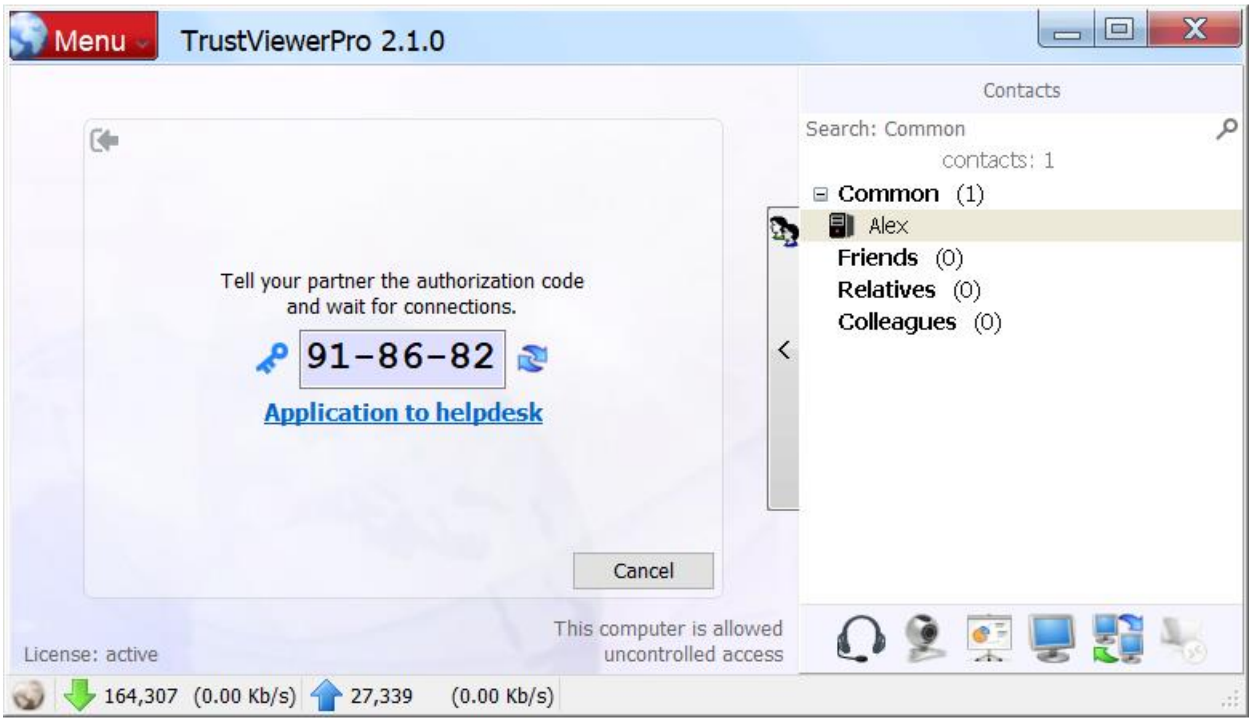
Create contact

Contact name (nickname): Alex
User name:
Name of computer: STAT3SKASP\Alex
Location: [redacted] (GMT 4, 16:24)
Date and time of the last successful session: 14.05.2019
Scope: Local network and Internet (shared proxy TrustServer)
Additional information:
Comment:

777,413 (135.39 Kb/s) 39,236 (0.31 Kb/s) fps: 0

In the case of granting the operator temporary uncontrolled access (for details, see "Granting access using a temporary ID" in the section "Work with the client module «TrustViewerPro»" of this manual) – temporary secure contacts are created automatically and additional actions on the part of the operator and the user of the remote computer are not required.

After a successful exchange of contacts and the completion of the current communication session - the operator can at any time initiate a new communication session using the user's contact card. A new contact is created by default in the “General” group in the contacts pane, but later it can be transferred to another group (to create a new group, right-click on the free space on the panel and select “Add group” in the context menu). The required contact can be quickly found using the search panel: just start typing the name of the contact, and the list of matches will be immediately displayed in the group of search results. To connect to a remote computer, you need to find and select the desired user, wait for a positive response from the remote computer (buttons for the corresponding requests should be activated in the access panel), click on the button with the required connection mode (“Voice communication”, “Video call”, “Desktop demo”, “Remote desktop” or “Chat, file sharing, etc.”), and wait for the confirmation of the request from the remote user. You can also send a message to the user using the chat panel (when sending a message, the chat form on the remote computer opens automatically). Here, the operator can block or delete the user's contact, to do this, select the desired user, right-click the context menu, and click “Block” or “Delete”.



Tell your partner the authorization code and wait for connections.

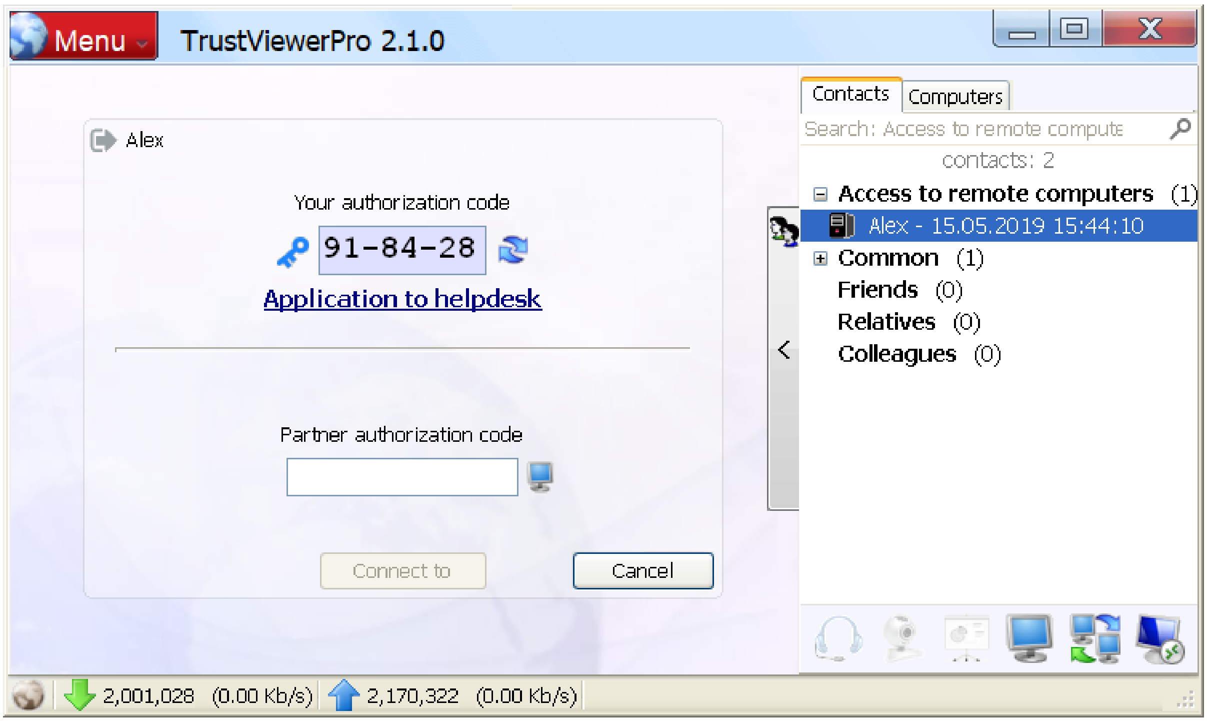
91-86-82

This computer is allowed uncontrolled access

License: active

164,307 (0.00 Kb/s) 27,339 (0.00 Kb/s)

If the operator is provided with temporary uncontrolled access, temporary contacts are created in the “Access to remote computers” group, with the user name and the date and time of the granted access expired (you can later rename the contact by opening the contact card for editing).



Your authorization code 91-84-28

Alex - 15.05.2019 15:44:10

2,001,028 (0.00 Kb/s) 2,170,322 (0.00 Kb/s)

To connect to a remote computer, you need to find and highlight the required entry, wait for a positive response from the remote computer (the buttons for the corresponding requests should be activated in the access panel), click on the button with the required connection mode (“Remote desktop”, “Chat, exchange files, etc.” or “RDP session”), and, if required, enter a password for access. Here, as well as in the case of regular contacts, the operator can block or delete a temporary contact, to do this, select the desired entry, right-click on the context menu, and click “Block” or “Delete”.

6.4. Working with the «TrustViewerPro» client module in network administrator mode

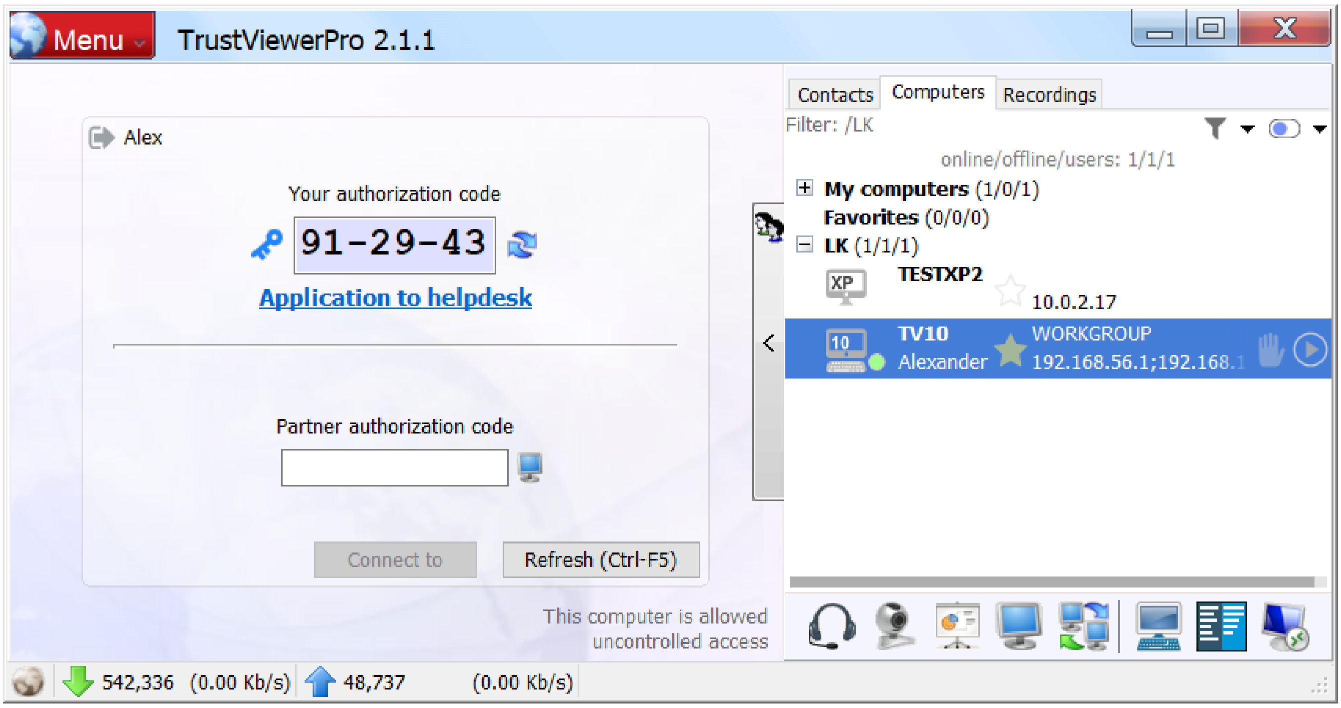
An authorized user with network administrator privileges can at any time connect to remote registered computers without using an identifier, using the control panel of computers or using the quick search mode and connecting to the main form of the program.

Attention! In order for a computer to appear in the network list, in addition to the condition of its authorization by a group account - in the settings of the client module of this computer, it must also be explicitly allowed to access it, indicating the available modes (for details, see the "Settings page “Access this computer”", in the "Work with the client module «TrustViewerPro»" section of this manual).

6.4.1. Computer control panel

Computers available for connection are displayed in the “Computers” panel as a tree structure, where the nodes are departments and subdivisions of computers (the “Department” property in the computer card on the server), and the final nodes are the own computers and current active users of these computers (for identification of users of computers the system accounts of Windows are used). Thus, an administrator can connect to a specific computer user with confirmation of a request to access his desktop (administrator rights not lower than “Connections to users with request” are required) or directly to a computer without confirmation (administrator rights are required “Connections to computers without request”).

Here, the process of connecting to a remote computer is generally similar to connecting using the contacts panel (connecting to the user is similar to connecting to a permanent contact, and connecting to a computer - connecting to a temporary contact with uncontrolled access): to connect to a remote computer, you need to find and highlight required computer or its active user, wait for a positive response from the remote computer (in the access panel, the buttons must be activated to match requests), click on the button with the required connection mode (“Voice communication”, “Video call”, “Desktop demo”, “Remote desktop” or “Chat, file sharing, etc.” - when connected to the active user computer, or “Remote Desktop”, “Chat, file sharing, etc.” or “RDP session” (when connected to the computer itself), and, if required, enter the password for access. Here, in the case of connecting to an active user, as well as in the case of a regular contact - you can send a message to the user using the instant messaging panel.



In the “My computers” group — computers that are allowed individual access for this user are automatically displayed (set on the server in the computer properties, for more details see the section “Editing computer cards”, in the “Administration of the TrustServer server” section of this manual).

For more convenient access to computers - you can add some of them to the “Favorites” group (tick the required computers or entire nodes, right-click the context menu and select “Add to Favorites”). To remove computers from the “Favorites” group, check the required computers in it, call the context menu and select “Delete”. Also, you can control the placement of a computer in the “Favorites” group using its card (the “Add to Favorites” checkbox on the computer card).

You can find the desired computer or user using the search bar: just start typing the query text (you can enter several keywords separated by a space), and the list of matches will be immediately displayed in the search results group.

Attention! When you open a list of computers in one of the groups, the search bar automatically switches to filter mode, where the list of matches is displayed in the current view. You can change the current Search/Filter mode manually at any time using the corresponding button in the search bar.

An advanced search mode is also available that allows you to set complex sampling conditions by using fields, operators, and brackets. To activate the advanced mode - just start typing the expression with the symbol "?". For example, the condition "? ((Ip == 192.168.*) or (label =="Computer 1")) and (department<>*KM*)" will select all computers from the 192.168 network, or with the label "Computer 1", provided that the word "KM" does not appear in the name of the unit. In this case, the operators "==" are used - it is equal, "<>" - is not equal, ">" – greater, ">=" – greater or equal, "<" - less, "<=" – less or equal, the value can be enclosed in quotation marks, and a search mask can also be used (using the symbol "*"). In addition, to simplify the preparation of expressions, you can use the following alternative operators: "=" - similar to the operator "==" with the full mask "*value*" (ie, the expression "?ip=1" selects all computers whose IP address contains the symbol "1"); "! =" - similar to the operator "<>" with the full mask "*value*" (ie, the expression "?ip!=1" will select all computers whose IP address does not contain the symbol "1").

Attention! Using the pop-up list (the "▼" button next to the search button) - you can save/call/delete frequently used expressions.

Attention! Selection records are sorted in ascending order by the fields specified in the expression. For example, the expression "?Label=" (that is, only the field name is specified, without specifying values) - displays the records of all computers and sorts them by the "label" field.

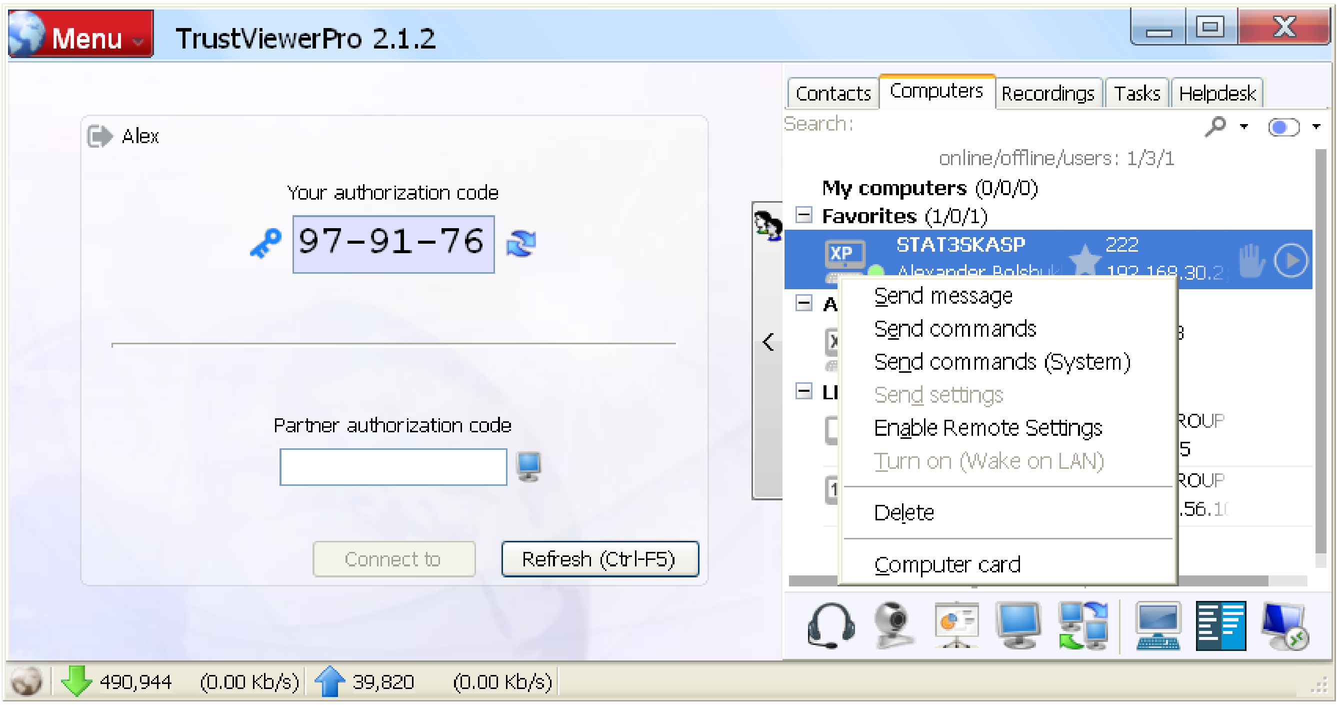
Attention! If the query text is to simply type "?"- then all fields of the card available for composing the expression will be displayed. You can use this property as a quick hint when composing expressions.

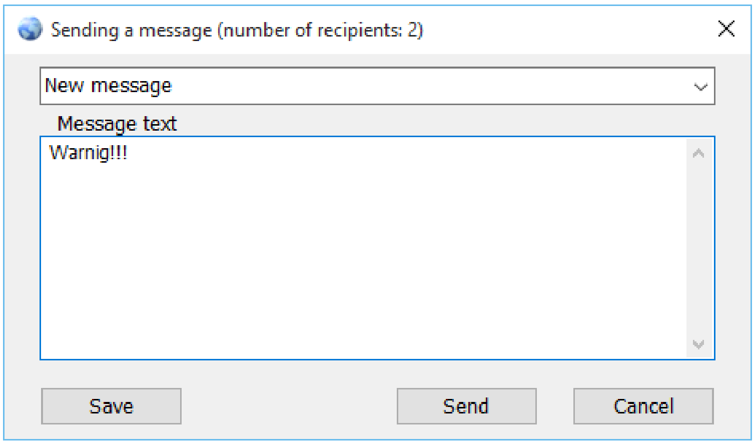
The following is a list of fields available for composing an expression.

Field	Description
Label	Computer label (set in the computer card)
Tag	Additional computer label (set in the computer card)
Computer	Network name of the computer (determined by the system)
Domain	Computer domain / workgroup (determined by the system)
Ip	The list of IP addresses assigned to the computer (determined by the system)
Login	The name of the group account under which the computer was authorized
Department	Department to which the computer belongs (specified in the computer card on the server)
Users	List of current active computer users (Windows system accounts are used to identify computer users)
Online	Number of days of continuous connection to the server (0 if the computer is currently offline)
Offline	Number of days without connecting to the server (0 if the computer is currently online)
Uptime	Days of computer uptime.
Error	Indicates an error in authorizing the computer using a group account (1 – there is an error, 0 – there is no error).
CPU	Processor model
OS	Computer operating system version.
Build	Computer operating system build number.
Version	Client module update version.
FileVersion	Client module distribution version.
Comment	Comment.
ID	Computer ID

6.4.2. Group sending of messages and commands / scripts / settings

Using the computer control panel - you can send messages, as well as remote execution of commands / scripts, both for individual computers and for their groups.



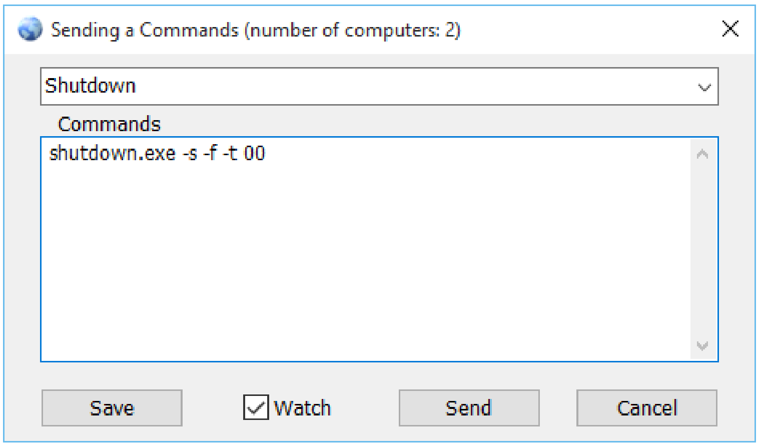


New message

Message text

Warnig!!!

Select the desired nodes (for group selection - use the left mouse button while holding down Ctrl or Shift), and use the right mouse button – call the context menu. To send a message to active users of dedicated computers, select the menu item “Send message”, in the opened form select a previously saved or enter a new message and click the “Send” button (to save the current message - click the “Save” button).



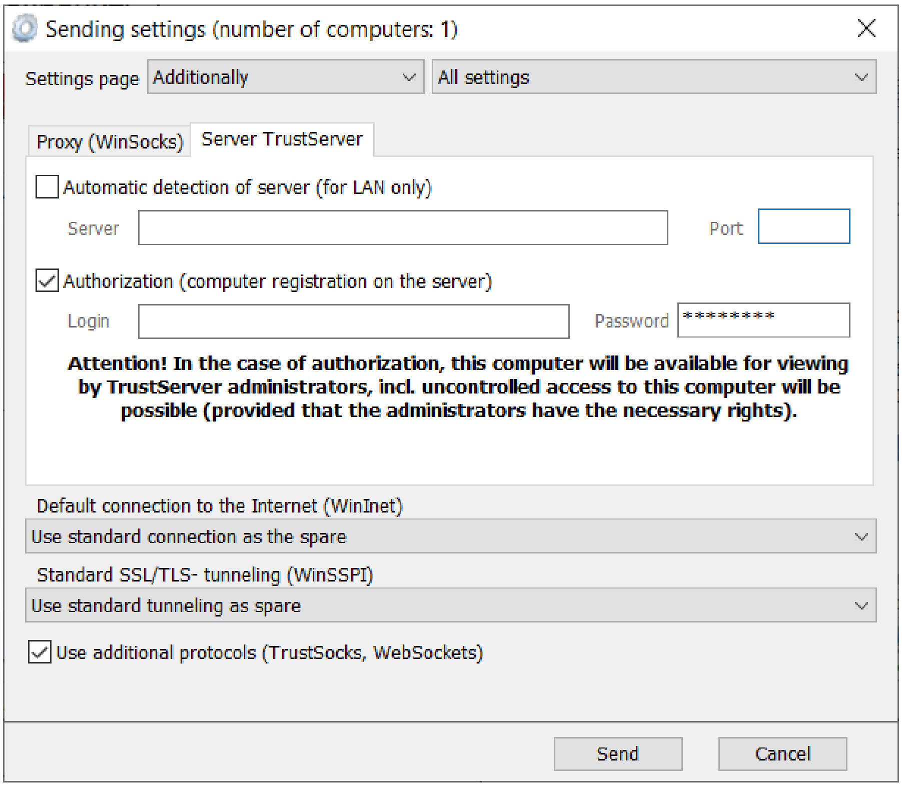
Shutdown

Commands

```
shutdown.exe -s -f -t 00
```

For remote execution of commands/scripts on the selected computers (syntax corresponds to batch (BAT) file) - select “Send commands” in the menu (commands will be executed on behalf of currently active users of these computers) or “Send commands (System) ”(The commands will be executed on behalf of the System account of the System), select the previously saved or enter a new script, check/uncheck the "Watch" checkbox (depending on whether you want to display the results of command execution or not) and click the “Submit” button (to save the current script, click the “Save” button).

Attention! When sending commands, you can also pass a file (any format, but no larger than 10 MB) and use it in the script. To insert a file into the script, select "New script (+file)" from the list on the command sending form)"



Settings page: Additionally | All settings

☐ Automatic detection of server (for LAN only)

Server: Port:

☑ Authorization (computer registration on the server)

Login: Password: *********

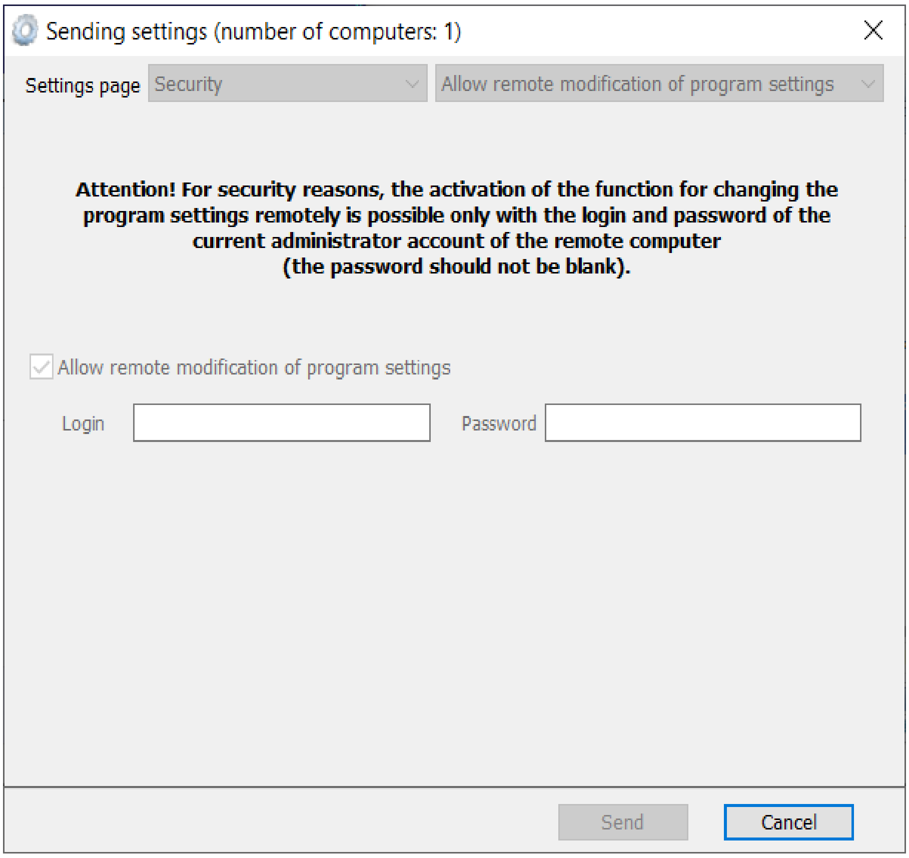
Attention! In the case of authorization, this computer will be available for viewing by TrustServer administrators, incl. uncontrolled access to this computer will be possible (provided that the administrators have the necessary rights).

Default connection to the Internet (WinInet): Use standard connection as the spare

Standard SSL/TLS- tunneling (WinSSPI): Use standard tunneling as spare

☑ Use additional protocols (TrustSocks, WebSockets)

To send settings to selected computers (on the “Security” tab, the “Allow remote modification of program settings” flag should be checked in the settings of the remote computers program) - select “Send settings” from the menu, select the desired settings page, select the desired setting (or “All settings”), specify the settings and click “Send”.



Settings page: Security | Allow remote modification of program settings

Attention! For security reasons, the activation of the function for changing the program settings remotely is possible only with the login and password of the current administrator account of the remote computer (the password should not be blank).

☑ Allow remote modification of program settings

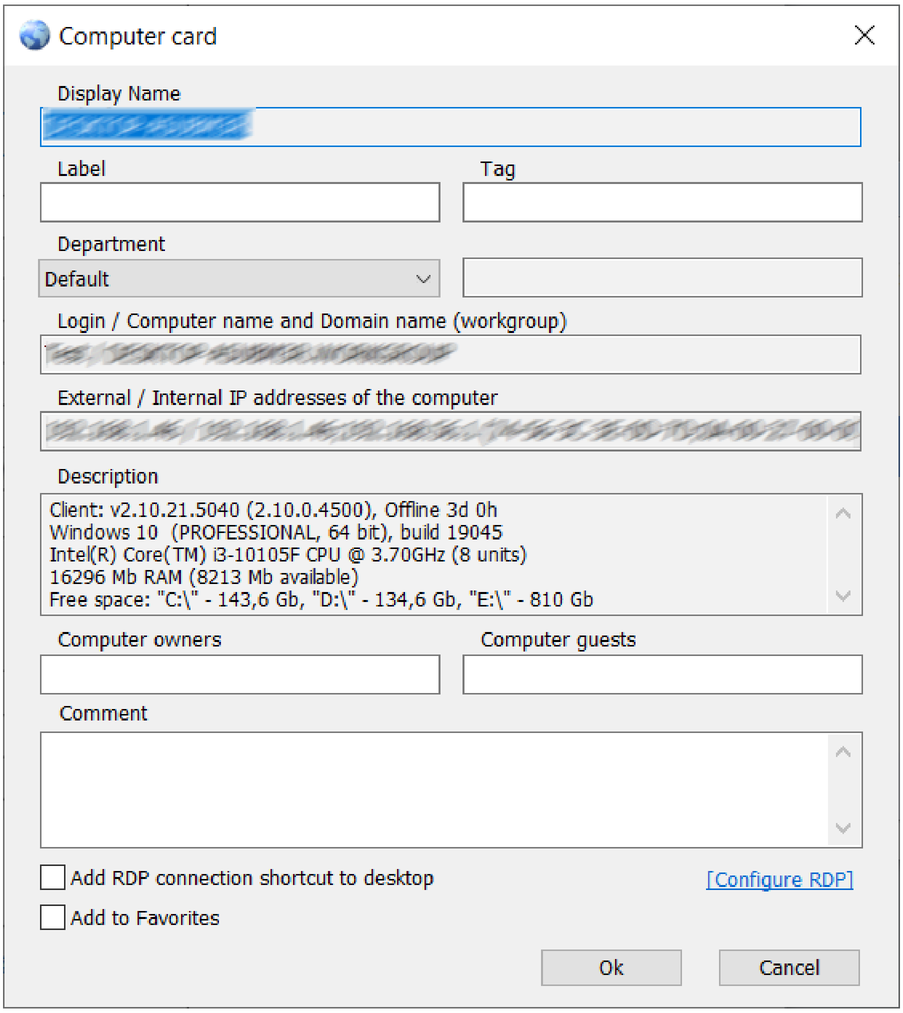
Login: Password:

To send the “Allow remote modification of program settings" settings to the selected computers, select “Enable remote settings” from the menu, specify the username/password of the system account of the remote computer with administrator rights (both the local account and the Active Directory account will work), and click “Send”.

Attention! Care should be taken when sending settings, for example, if you specify incorrect authorization data, then all selected computers will be disconnected from the server and their further remote configuration will be impossible.

6.4.3. Editing computer cards

If the administrator has the necessary rights, he can edit computer cards not only using a browser, using the server's control panel, but also directly in the client module. To open a computer card, select the required entry, right-click on the context menu and select "Computer card". After editing the computer card, click "Ok" to save the change. For more information about editing computer cards, see "Editing computer cards", in the "Administration of the TrustServer Server" section of this manual.



Display Name: [redacted]

Department: Default

Login / Computer name and Domain name (workgroup): [redacted]

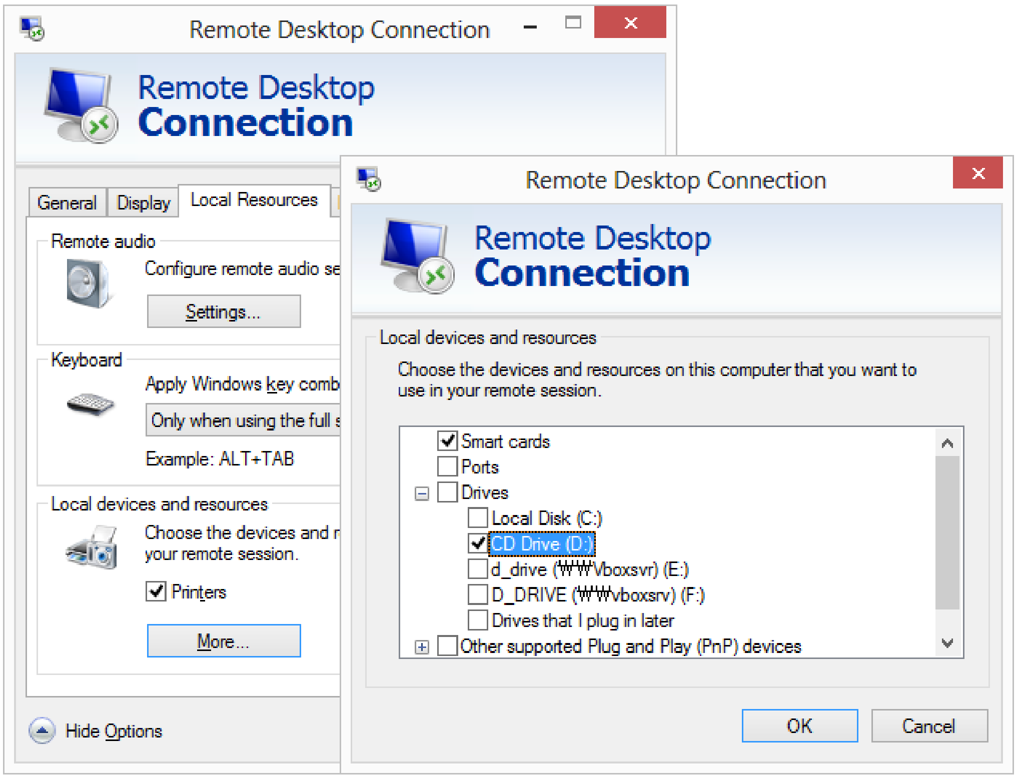
External / Internal IP addresses of the computer: [redacted]

Description:
Client: v2.10.21.5040 (2.10.0.4500), Offline 3d 0h
Windows 10 (PROFESSIONAL, 64 bit), build 19045
Intel(R) Core(TM) i3-10105F CPU @ 3.70GHz (8 units)
16296 Mb RAM (8213 Mb available)
Free space: "C:\" - 143,6 Gb, "D:\" - 134,6 Gb, "E:\" - 810 Gb

☐ Add RDP connection shortcut to desktop
☐ Add to Favorites

6.4.4. Configuring RDP Connection Settings

By default, when connecting to a remote computer in the RDP session mode, the system uses the connection settings predefined by the system, however, you can change them: open the card of the required computer (select the required entry, right-click on the context menu and select "Computer Card", or just double-click the required entry with the left mouse button) and click on the "Configure RDP" link - the standard connection settings window will open. Thus, you can, for example, configure for a remote computer constant access to the local computer's drives (the "Local resources" tab, the "Local devices and resources" panel, "Details", "Disks" panel).


Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Remote audio
Configure remote audio se
Settings...
Keyboard
Apply Windows key comb
Only when using the full s
Example: ALT+TAB
Local devices and resources
Choose the devices and r
your remote session.
More...
Hide Options
Remote Desktop Connection
Remote Desktop Connection
OK
Cancel

☑ Printers

Local devices and resources

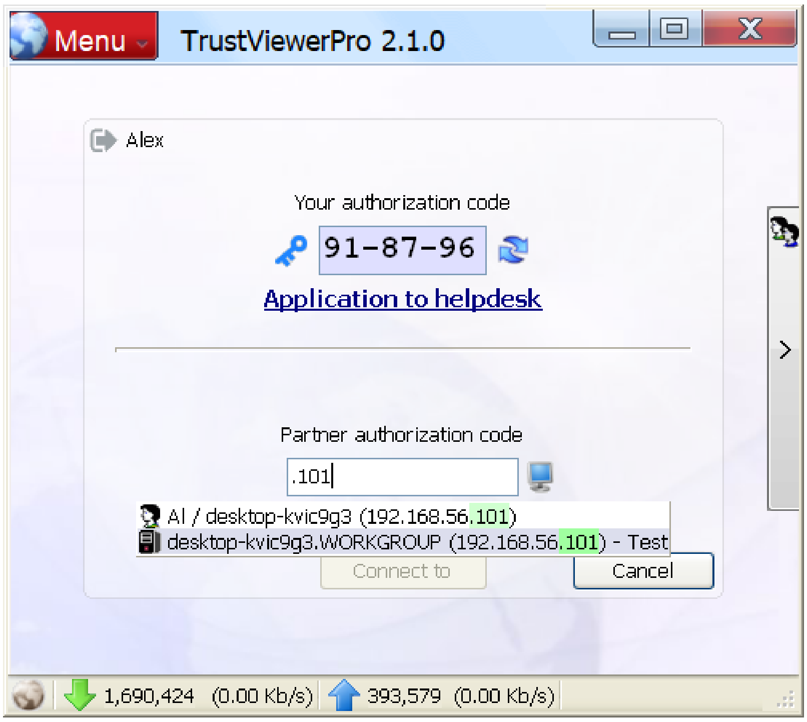
Choose the devices and resources on this computer that you want to use in your remote session.

- ☑ Smart cards
- ☐ Ports
- ☐ Drives
  - ☐ Local Disk (C:)
  - ☑ CD Drive (D:)
  - ☐ d_drive (\\Vboxsvr) (E:)
  - ☐ D_DRIVE (\\vboxsrv) (F:)
  - ☐ Drives that I plug in later
- ☐ Other supported Plug and Play (PnP) devices

On the form of a computer card, you can also customize the display on the desktop of a shortcut for quick connection to a computer in the RDP session mode (the checkbox “Add RDP connection label to the desktop”).

6.4.5. The mode of fast connection to a computer on the network

For convenience, the registered computer can also be accessed directly from the main form of the program in operator mode: just start typing the IP address, computer name or username in the session ID input field - and the list of matches will be immediately updated and displayed.



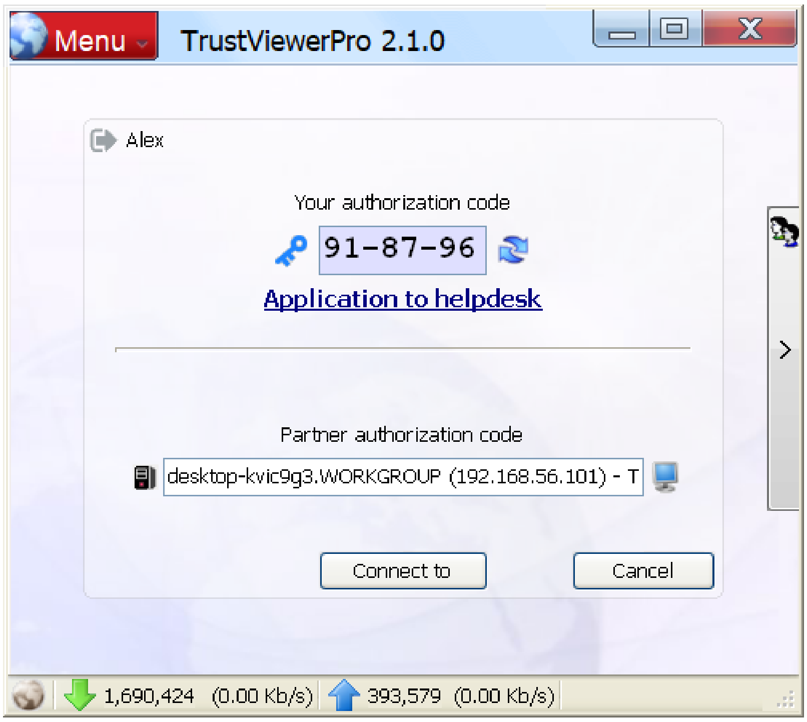
Your authorization code: 91-87-96

Partner authorization code: .101

Al / desktop-kvic9g3 (192.168.56.101)
desktop-kvic9g3.WORKGROUP (192.168.56.101) - Test

To connect to the computer - select the desired entry (recording with a user icon means that a user’s remote desktop connection will be made on request, recording with a computer icon -

that you will be connected to a computer in uncontrolled access mode), then select the required connection mode (click the button to the right of the ID input field and select the required mode from the drop-down list) and click “Connect” (you may need to enter a password to access the computer).



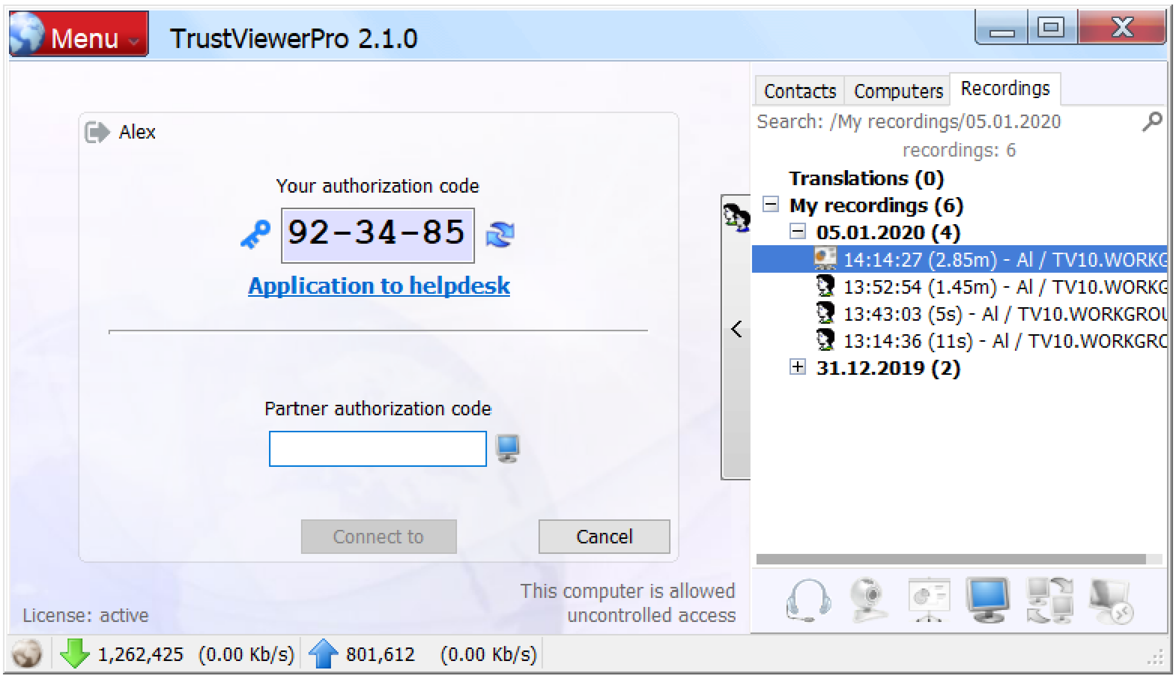
Your authorization code: 91-87-96

Partner authorization code: desktop-kvic9g3.WORKGROUP (192.168.56.101) - T

1,690,424 (0.00 Kb/s) 393,579 (0.00 Kb/s)

6.5. Working with recordings and translations of communication sessions

Saved recordings can be opened either from the main menu (“Open recording") or from windows Explorer (provided that the option to associate the program with recording files *was selected during installation.tvr), or download from the server on the operator panel tab “Recordings" (the server must be enabled centralized storage of records, and the operator must be assigned the necessary rights).



Your authorization code: 92-34-85

Partner authorization code:

Search: /My recordings/05.01.2020

recordings: 6

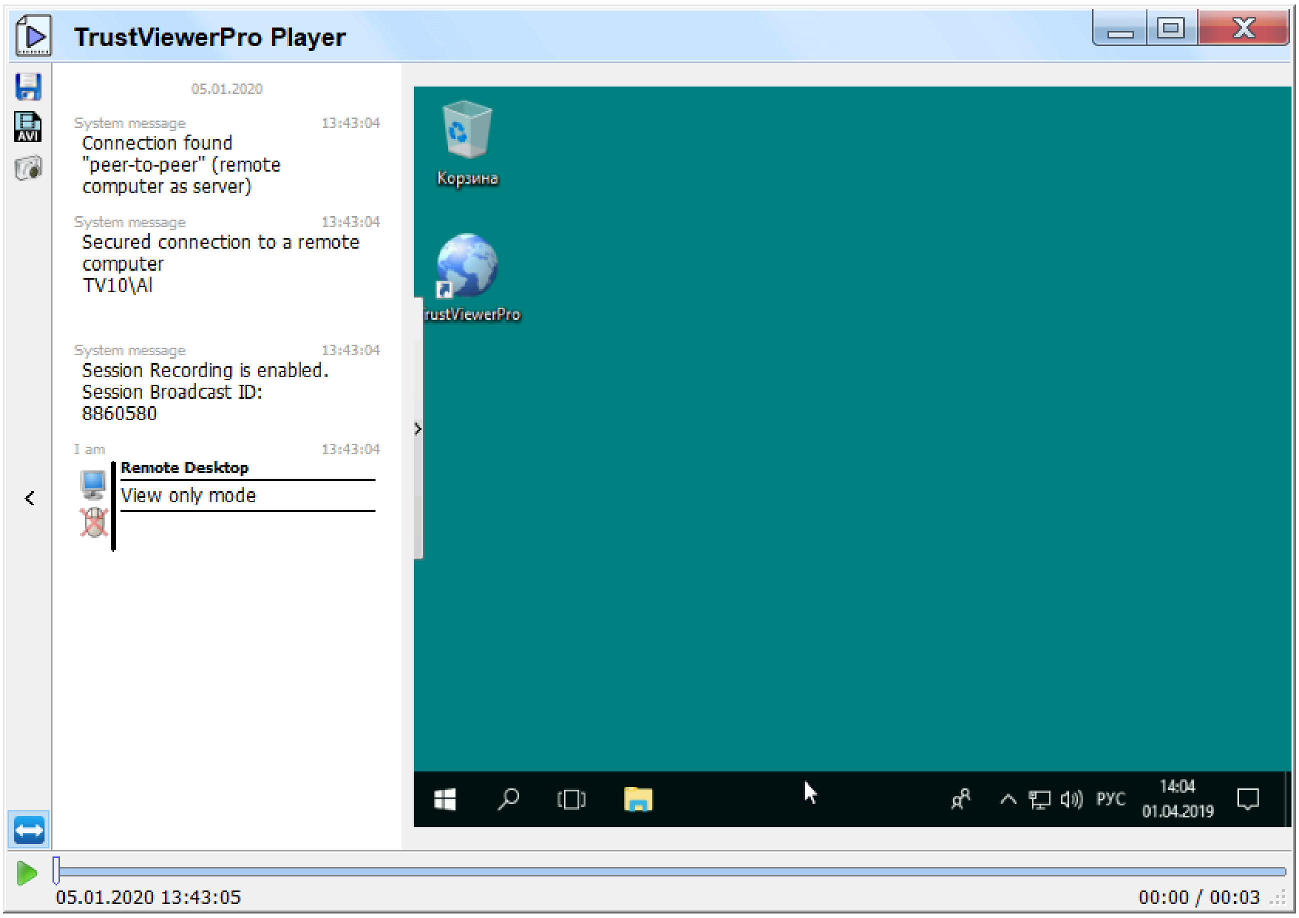
Translations (0)
My recordings (6)
05.01.2020 (4)
14:14:27 (2.85m) - Al / TV10.WORKG
13:52:54 (1.45m) - Al / TV10.WORKG
13:43:03 (5s) - Al / TV10.WORKGROU
13:14:36 (11s) - Al / TV10.WORKGRC
31.12.2019 (2)

License: active

This computer is allowed uncontrolled access

1,262,425 (0.00 Kb/s) 801,612 (0.00 Kb/s)

Attention! Here, in the "Translations" folder, you can also view and open the currently available translation sessions. In addition, if you know a special seven-digit translation ID, you can also use it to open an active translation (the ID should be entered in the “partner authorization code" field on the main program form and click "Connect to").



05.01.2020

System message 13:43:04
Connection found "peer-to-peer" (remote computer as server)

System message 13:43:04
Secured connection to a remote computer TV10\Al

System message 13:43:04
Session Recording is enabled. Session Broadcast ID: 8860580

I am 13:43:04
Remote Desktop
View only mode

05.01.2020 13:43:05 00:00 / 00:03

The following are the button assignments on the session recording control panel.

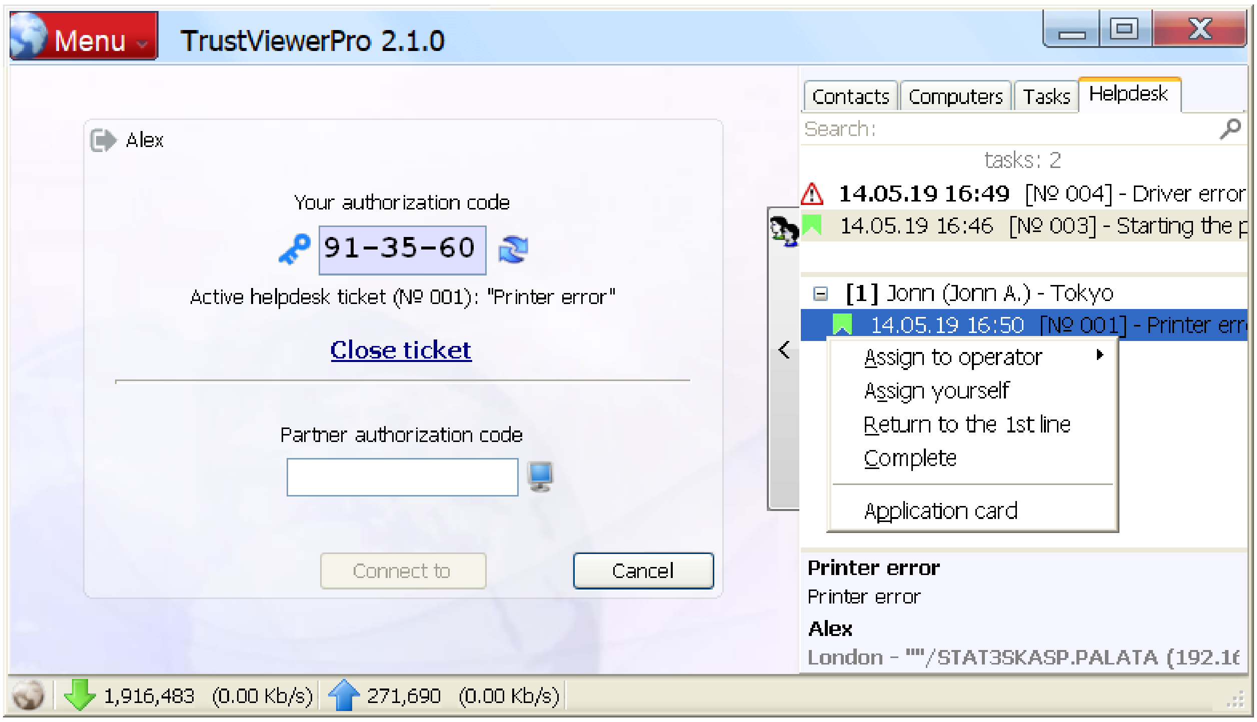
Field	Description
💾	Saves the current entry to the specified file
AVI	Converts the current session recording into a video recording using one of the codecs installed in the system (by default, the XVID codec is used)
📷	Saves the current frame in *.bmp format
⇔	Switches the display mode of the remote desktop image: true size or fit size.
▶	Starts recording playback
⏸	Pauses recording playback

6.6. Working with the «TrustViewerPro» client module in operator helpdesk mode

Authorized user with the helpdesk operator rights - can connect to remote computers on request, using tickets from user requests to the support service (subject to the rights of the 2nd line helpdesk operator, and also provided that the specified requests were explicitly assigned to this operator), and also assign these requests to other operators (requires the rights of the 1st line operator helpdesk). Thus, it is possible to organize convenient and secure access to computers on demand, without using temporary identifiers and without having to give operators network administrator rights.

6.6.1. Work in the operator mode of the 1st line helpdesk

The interface for working in the operator mode of the 1st line helpdesk is placed on the "Helpdesk” tab. Here in the upper panel displays a list of applications received from users, in the lower part – a summary of the current selected application (indicating the subject and text of the application, as well as the name and territorial belonging of the user), in the middle panel – a list of operators of the 2nd line helpdesk and a list of assigned applications (also here you can see the status of availability of the operator (online, if there is a green circle next to the operator's name, offline – otherwise), the number of incomplete applications from the operator and its territorial belonging). Thus, when choosing the contractor of the application, the operator of the 1st line has sufficient information about the workload, availability, and territorial belonging of all operators of the 2nd line. To assign selected orders – drag and drop them for the required operator (drag-and-drop is supported), or use the right button to open the context menu, select “Assign to operator” and select the required operator in the drop-down list (here you can quickly assign selected orders ("Assign to yourself” item), or close them ("Close” item)). In addition, the operator of the first line here can manage the applications assigned to the operators of the 2nd line (reassign to another operator, return to the 1st line or close), to do this open the list of applications of the required operator, mark the required applications, call the right-click context menu and select the appropriate menu item (“Assign to operator”, “Assign to yourself”, “Return to the 1st line” or “Complete”).



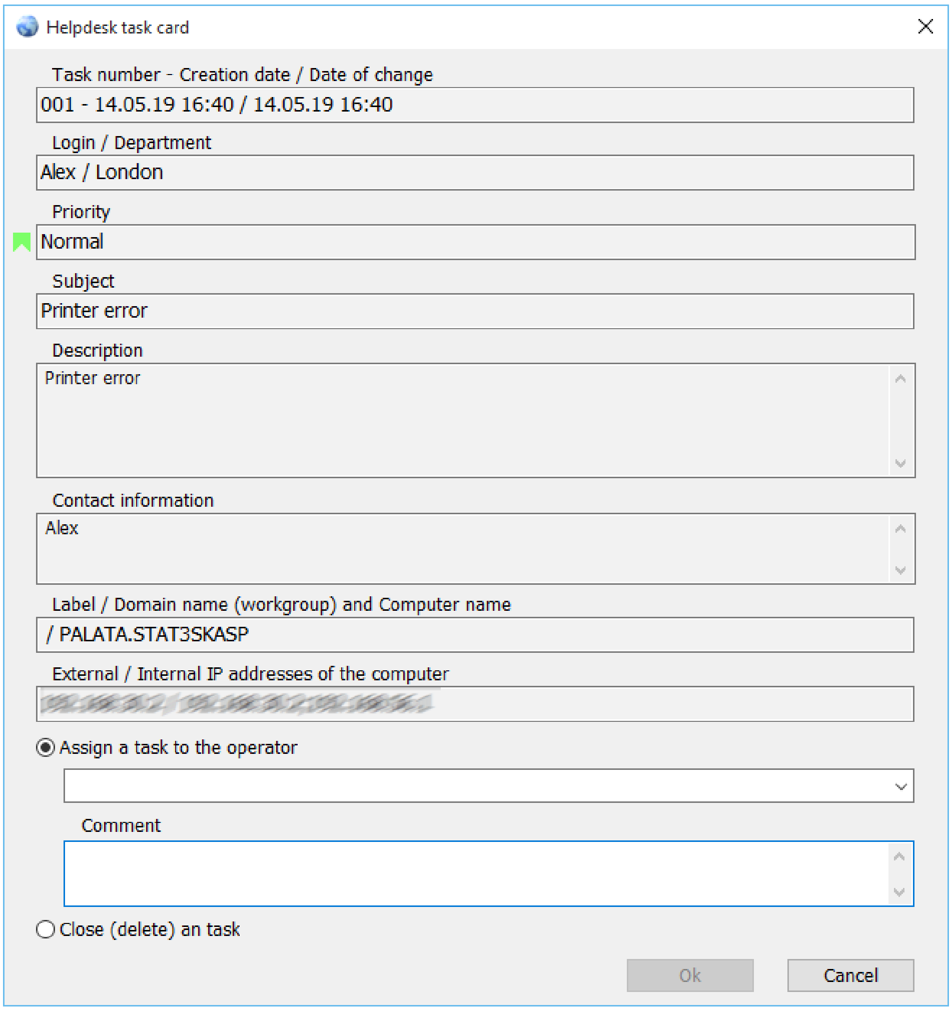
Your authorization code
91-35-60
Active helpdesk ticket (№ 001): "Printer error"

tasks: 2
14.05.19 16:49 [№ 004] - Driver error
14.05.19 16:46 [№ 003] - Starting the p

[1] Jonn (Jonn A.) - Tokyo
14.05.19 16:50 [№ 001] - Printer err

Printer error
Printer error
Alex
London - ""/STAT3SKASP.PALATA (192.16

For more information about the application can be viewed in its card (select the required application, right-click the context menu and select the “Application Card” item, or simply double-click the required application). Here you can also assign an application to an operator with an indication of a comment, or close it.



Helpdesk task card

Task number - Creation date / Date of change: 001 - 14.05.19 16:40 / 14.05.19 16:40

Login / Department: Alex / London

Priority: Normal

Subject: Printer error

Description: Printer error

Contact information: Alex

Label / Domain name (workgroup) and Computer name: / PALATA.STAT3SKASP

External / Internal IP addresses of the computer: [redacted]

● Assign a task to the operator

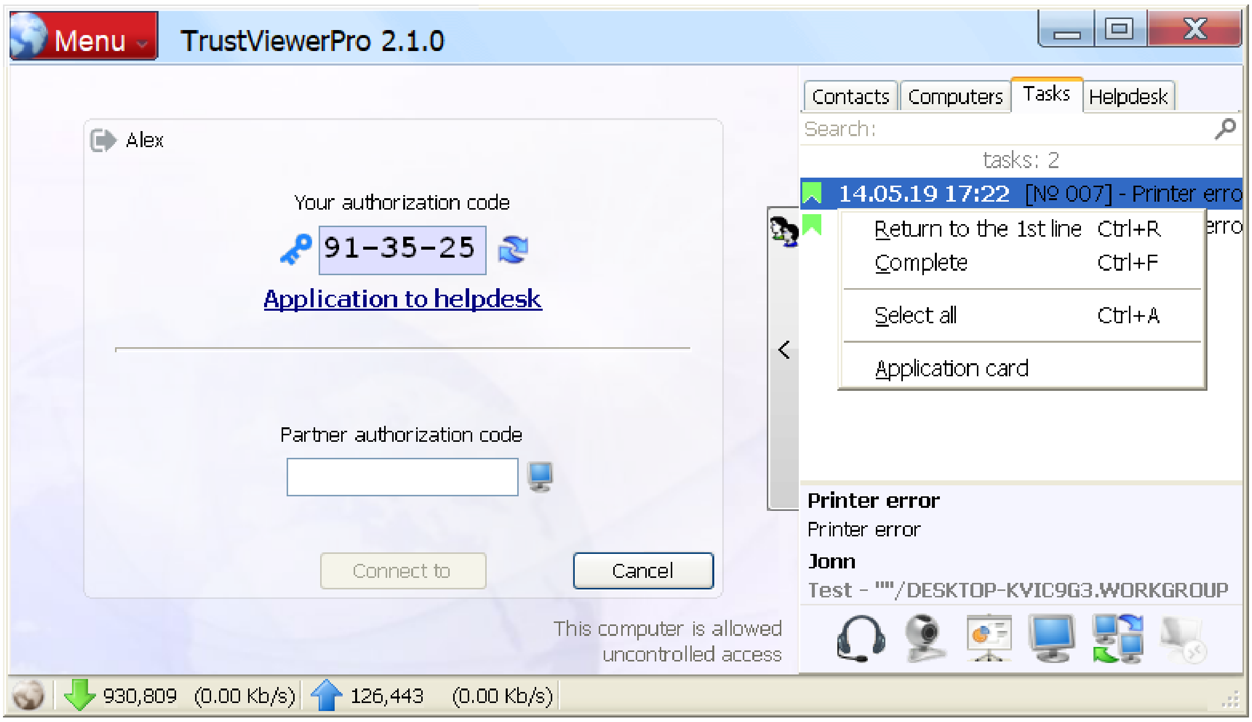
Comment

○ Close (delete) an task

Find the required application - you can use the search panel: for example, start typing the topic of the application, and the list of matches will be immediately displayed in the search result group.

6.6.2. Work in the operator mode of the 2nd line helpdesk

The interface for working in the operator mode of the 2nd line helpdesk is placed on the “Applications” tab. Here, in the top panel, a list of applications assigned to the operator is displayed, in the middle part there is a brief information about the current selected application (indicating the subject and text of the application, as well as the name and territorial belonging of the user), at the bottom – the interface to connect to a remote computer. In general, here the process of connecting to a remote computer is the same as in the case of connecting using contacts: you need to find and highlight the required application, wait for a positive response from the remote computer (buttons for the corresponding requests should be activated in the access panel), click the button with the required connection mode (“Voice communication”, “Video call”, “Desktop demo”, “Remote desktop” or “Chat, file sharing, etc.”) and wait for the confirmation of the request from the remote about the user. Also, here you can send a message to the user using the instant messaging panel (if the user of the remote computer responds, the chat form will open). After processing of applications, they must either be completed or returned to the 1st line: select the required applications, right-click the context menu and select the item “Return to the 1st line” or “End”, respectively.



Your authorization code

91-35-25

Application to helpdesk

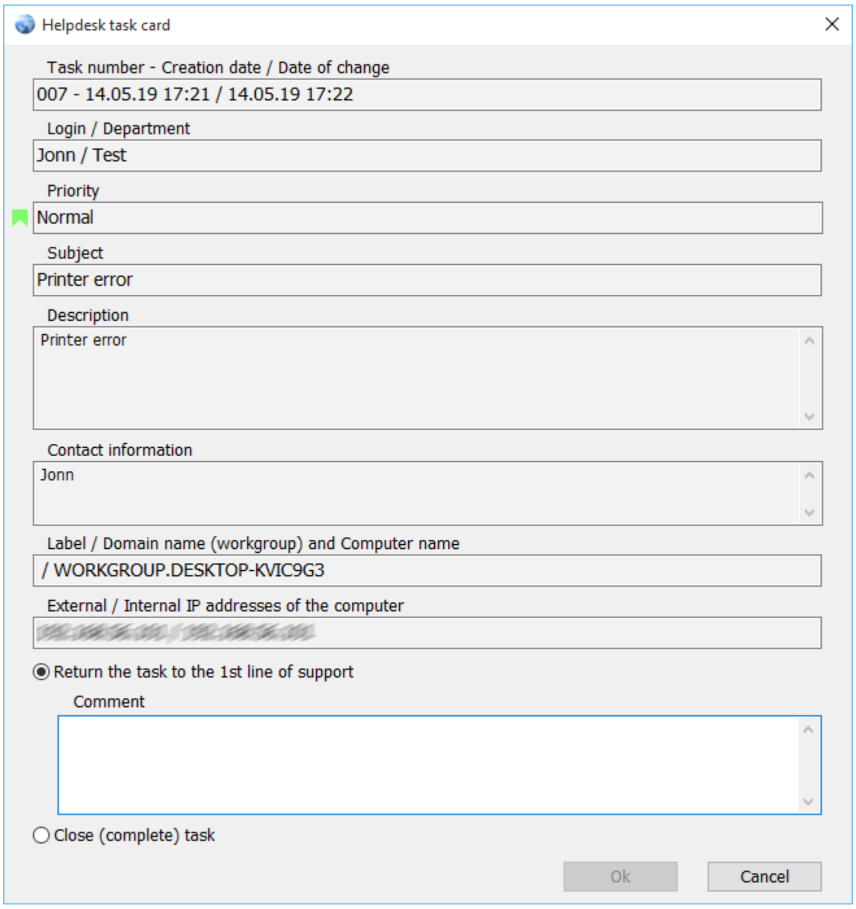
Partner authorization code

14.05.19 17:22 [№ 007] - Printer erro

Printer error
Printer error
Jonn
Test - ""/DESKTOP-KVIC9G3.WORKGROUP

This computer is allowed uncontrolled access

For more information about the application - you can look at its card (select the required application, right-click the context menu and select the “Application Card”, or simply double-click the required application). Here you can return the application for the 1st line with an indication of the comment, or complete it.



Task number - Creation date / Date of change	007 - 14.05.19 17:21 / 14.05.19 17:22
Login / Department	Jonn / Test
Priority	Normal
Subject	Printer error
Description	Printer error
Contact information	Jonn
Label / Domain name (workgroup) and Computer name	/ WORKGROUP.DESKTOP-KVIC9G3
External / Internal IP addresses of the computer	[redacted]

● Return the task to the 1st line of support

Comment

○ Close (complete) task

6.7. Integration with Active Directory

If the operator logged into the system with an AD account that has access to computers with administrator rights, then an additional node "ActiveDirectory" appears in the root of the computer control panel with a structure of child nodes in full accordance with the structure of computers in AD.

In general, computers enter the "ActiveDirectory" node under the following conditions:

- Computers are registered in AD;
- The operator has access to these computers in AD with administrator rights;
- These computers have TrustViewerPro installed with a group account;
- The operator is allowed access to these computers on the trustserver.

In general, when entering the "ActiveDirectory" node, computers are duplicated, as if they were in the "Favorites" or "My Computers" node, so the "ActiveDirectory" node can be used as an additional tool for more convenient (usual) access to computers registered in AD, without canceling the ability to access computers based on the structure of departments / trustserver access rights. However, it is possible to use the "ActiveDirectory" node more flexibly, using the additional scope of the "ActiveDirectory" access rules (along with “*”, “DepartmentName”, “LabelName” and “[MAC]”, for more details, see the section “Permissions to access departments/computers”, in the section “Administration of the «TrustServer» server" of this manual).

In a particular case, if in a large organization with a developed network of departments/branches all computers are registered in AD, and appropriate groups of computers are assigned to AD administrators, then setting up a trustserver can be greatly simplified: all computers can be authorized by one common group account for all, regardless of departments / branches in which they are located; all operator accounts can be created with the same access rights settings, regardless of the departments/branches in which they are located. Of course, in this case, if necessary, more flexible configuration can be carried out in the future: for example, assign hotel groups to some computers, or add separate rights other than AD to some operators (see "Example 9", "Example 10" and "Example 11" in the section "Permissions to access departments/computers", in the section “Administration of the «TrustServer» server" of this manual).

7. Contact Information

All copyrights to the software product “TrustViewerPro” belong to “Trust Ltd” OOO.

Comments and suggestions for the program can be sent to the email address mail@trustviewer.com, or on the website, using the feedback form http://www.pro.trustviewer.com/en#contacts.