Scopd manual

Table of content

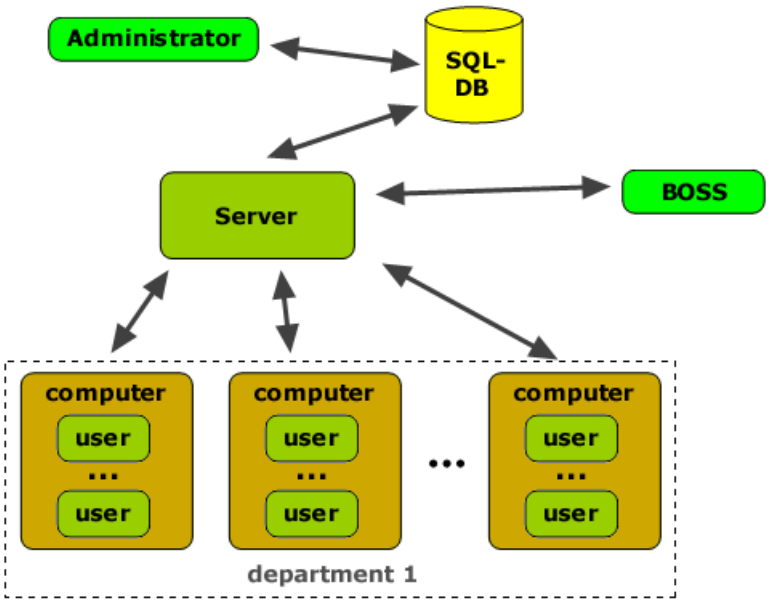
1. Introduction

Software suite **Scopd** is intended for surveillance of staff on their workstations as well as productivity evaluation derived from the factors presented in numerous reports generated by the program.
This software can be used in any company where staff works on computers.
It is intended for directors, HR staff and managers. It is also possible to use it for home surveillance.

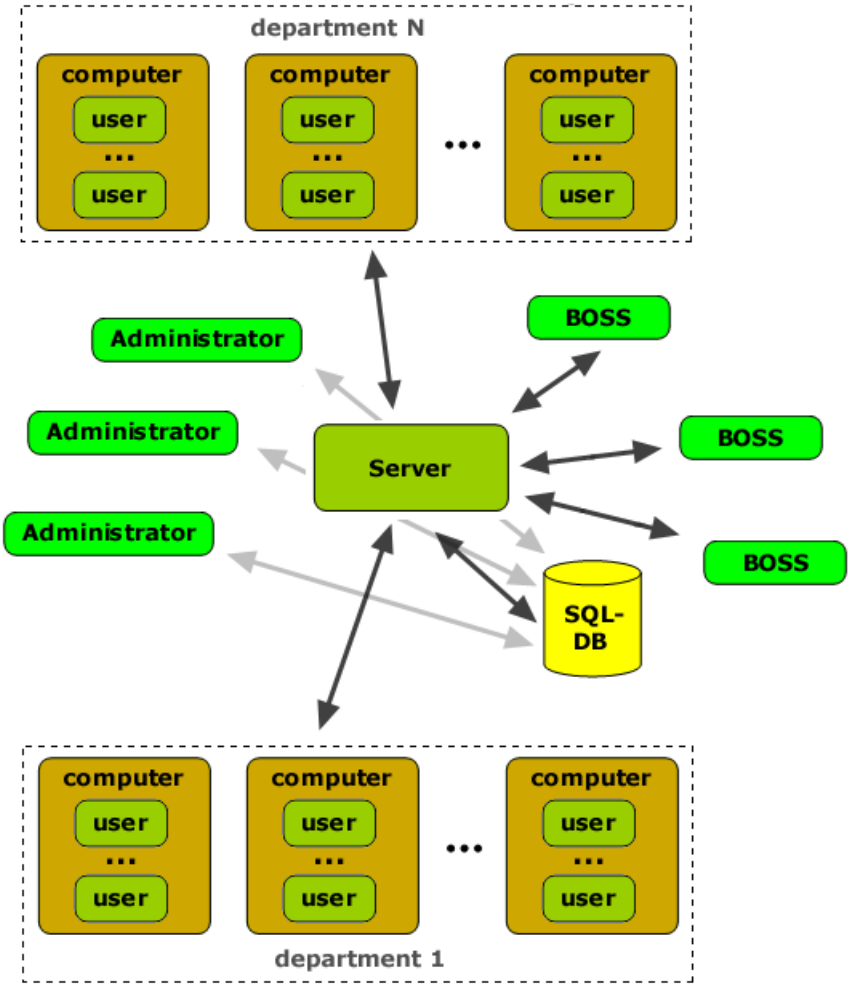
Attention! By default monitoring mode is set with notifications of employee, so when the client is manually installed on the local machine, the notification message will be shown (even before the actual settings are received from the server), despite the possibility of disabling this notification in the settings (see here)! When remote installation is used, priority is given to the current settings.

2. Software suite structure:

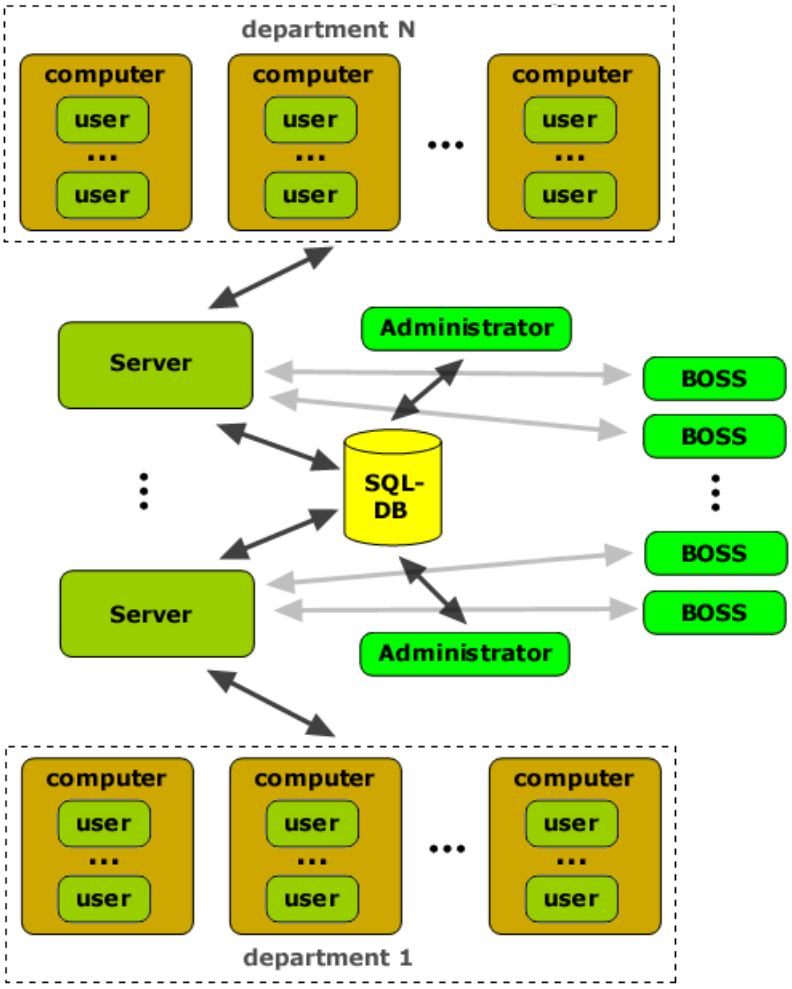
2.1. Basic case (one department and one server)



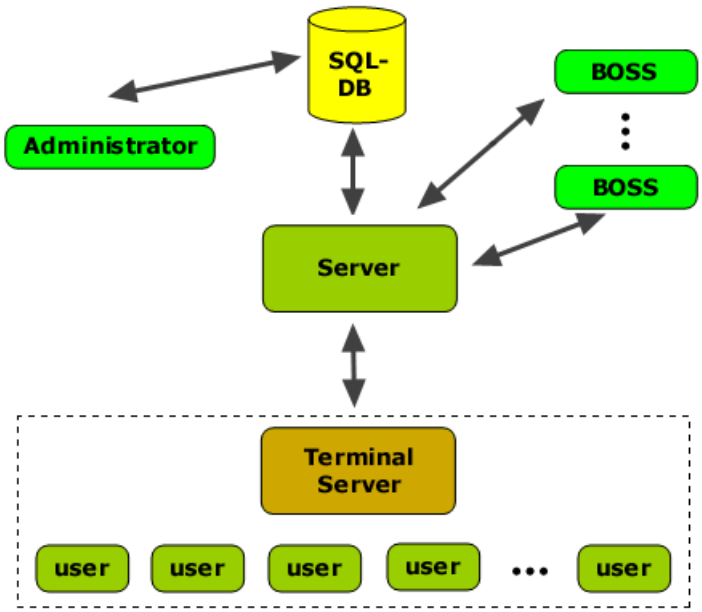
2.2. Several departments and one server



2.3. Complex case (several departments and several servers)



2.4. Working in terminal sessions



3. Software suite installation:

3.1. System requirements

Server (Windows):	2008R2/Win8.1/2012/Win10/11/2016/2019/2022 and latest OS versions (64-bit)
Server (Linux):	Ubuntu 22/24, Astra 1.7/1.8 ("Orel")
Client (Windows):	XP(SP3)/2003/Vista/Win7/2008/Win8/2012/Win10/11/2016/2019/2022 and latest OS versions (32/64-bit)
Client (Linux):	Astra, CentOS, Debian, Mint, Ubuntu, Rosa, RED OS (full list)
Client (MacOS):	Mojave, Catalina, Big Sur, Monterey, Ventura, Sonoma, Sequoia, Tahoe
SQL server:	MS SQL Server (minimum 2014), PostgreSQL (minimum 11)
Operation in terminals:	supported
Supported PACS systems:	Sigur (Sphinx)

see also **Server and client resources calculator**

3.2. Windows server:

3.2.1. Selecting an installation type

There are two installers of the complex: **"One click"** and **"Advanced" installation**.
It is important to understand that both installers install **the same software with the same functionality**, but only the installation itself goes differently.

"One click" installer allows you to quickly install all server components of the complex without any additional settings on one computer. Ideal for initial acquaintance with the complex, as well as for cases when it is planned to monitor a small number of employees (up to 50-70 people), or if there is no special need to install the server components of the complex on different computers.
To read more about **"one click"** installer visit the next page.

"Advanced" installation is recommended for experienced users and administrators, in particular, if the server components of the complex must be installed on different computers, or you need an SQL-server other than SQL Server Express.
Also, only **"advanced"** installation can be used to **update the complex** (regardless of which installer was used to install the complex!).
To read more about **"advanced"** installer visit this page.

Attention! Regardless of the type of installation, you may need to make preliminary settings described in "Common recommendations".

3.2.2. Installation in one click:

3.2.2.1. Installation in one click

How to choose an installation type (**"One click"** or **"Advanced"**) please read **here**.

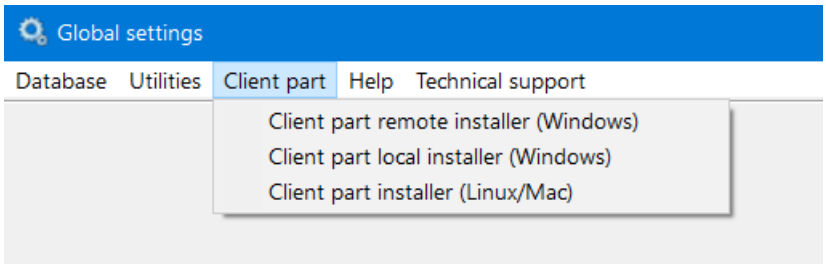
Features of "one click" installation:
- all server components are installed on a single computer (**Windows**);
- it will automatically install a new single instance of SQL Server Express or PostgreSQL (by choise);
- SQL Server Express: minimum supported OS is Windows 10/2016, also .NET Framework 4.7.2 should be installed before.
- SQL Server Express: the current Windows user will automatically become an administrator of created database;
- SQL Server Express: SQL Express has limitations: 10 GB per base (usually enough to monitor 50-70 employees with default settings), max use of 1 GB RAM and only one CPU;
- SQL Server Express: Internet access may be required during SQL Server Express installation.

After the installation, you will be taken to a page describing the next steps.
Also, all the necessary shortcuts will be created on the computer desktop:
- shortcut for **BOSS-Online, BOSS-Offline**;
- shortcut for **Global settings**;
- shortcut for **client part** installation using uncovered manual method.

Attention! For **remote installation of client parts** you need to use main menu item "Client part" -> "Client part remote setup" of the Global Settings application (see here for details).

3.2.2.2. Client part

After installing server components, there is often a need for quick access to local or remote installation of the client part of the complex.
The most convenient way is to use the main menu in the **Global Settings** program (available in the Start menu and on the desktop):



3.2.3. Advanced installation:

3.2.3.1. Advanced installation

How to choose an installation type (**"One click"** or **"Advanced"**) please read **here**.

If an advanced installation is selected **and server part should be installed on Windows**, it must be performed sequentially:
Step 0. Downloading the ne\u0000essary files
Step 1. Installing the SQL server
Step 2. Installing the administrator software
Step 3. Installing the suite server
Step 4. Installing the client part
Access to web-interface
Key activation (if available)

3.2.3.2. Step 0. Downloading the necessary files

Choose SQL server (necessary for operation):

Microsoft SQL Server 2014 Express (without FullTextSearch, minimum Windows Server 2008 R2, Windows 7)
Microsoft SQL Server 2019 Express (with FullTextSearch, minimum Windows Server 2016, Windows 10)
Microsoft SQL Server 2022 Express (with FullTextSearch, minimum Windows Server 2016, Windows 10)
PostgreSQL Server

Other (optional):

Linux/MacOS-clients
Neural network server
Utility for integration with PACS system Sigur (Sphinx)
Application for setup on the print-servers (if shared print server is available)
Application for printing captured files (.SPL)
Application for decryption of dump-files created by "black box" or quarantine (dumpdecrypt)
Utility for "marking" documents (adding marks/labels)
Utility for synchronizing data from files

3.2.3.3. Step 1. Installing the SQL server:

3.2.3.3.1. SQL server selection

SQL is needed to store all client settings, users' reports, permission rights etc.
MS SQL Server and PostgreSQL are supported in the present software version.
Installation files can be downloaded in the previous step.

Choose SQL-server in usage as an option:

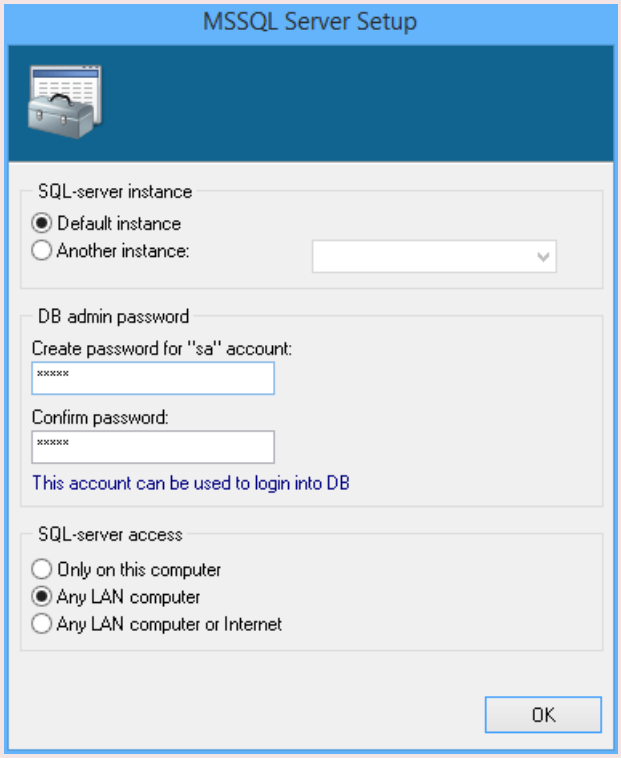
MS SQL Server
PostgreSQL

3.2.3.3.2. MS SQL Server

If SQL server was not installed before

Next will be described installation of the free edition of MS SQL Server: **Express Edition** through convenient installer, which should be downloaded here.
Please note, database size in the Express-edition **is limited to 10 GB**, which is usually enough to monitor 50-70 employees with default settings. If this volume is not enough, then you can install another edition of the SQL server.

Usually,installation is necessary to perform either on a separate server computer or on administrator's computer (if separate server room is not available).
The setup will run only under **administrator's account!**



The first required parameter in the process of installation is SQL server **instance**.
In many cases SQL data base is installed in a single instance on a single computer that is why it is necessary to leave installation option as "default instance". However, if you wish to setup several SQL server instances on a single computer you need to choose installation unique identifier.
In this case each instance is like an independent SQL server with its own database Scopd with its own settings, reports, users, rights, etc.
In this case it is also necessary to make software suite's server instantiation, so each server instance will connect to its own SQL server instance. Clients' workstations also must be connected optionally to this or the other software suite server instance. Administrator has to create database and set up each SQL server instance. As a result each manager can monitor his or her department via BOSS-Online, look through reports from SQL database only of his or her department as well as change settings if applicable (if administrator will delegate him or her permission rights).
In above mentioned case not only computer name must be specified but also instance name while connecting to a certain SQL server instance:
machine\instance, for example: **SERVER\inst1**

Later in the process of installation new password must be created for administrator's account with a special login **"sa"**.
Then using this login it will be possible to enter database to change all settings.
By default **current Windows user will be added as database administrator**.

Also it is suggested to choose SQL server accessibility depending on network configuration and your needs.

Information about **SSL-encryption** is here.

If MS SQL Server has been already installed

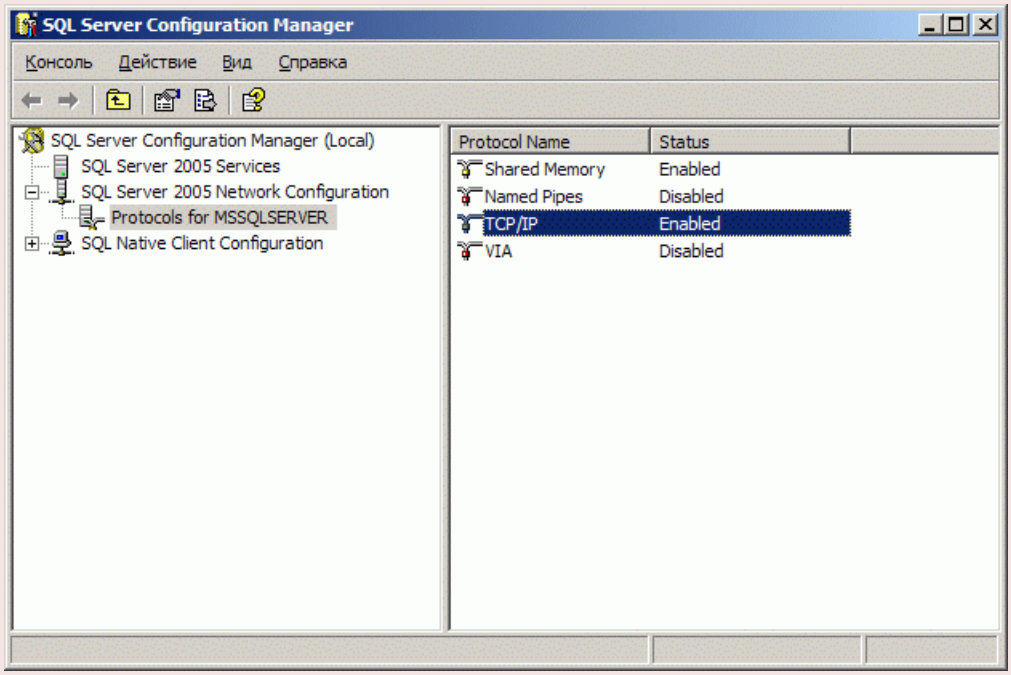
If MS SQL Server has already been installed, it is necessary only to check its configuration.

Attention!!! If before SQL server has been installed with the instance different to the instance by default or is

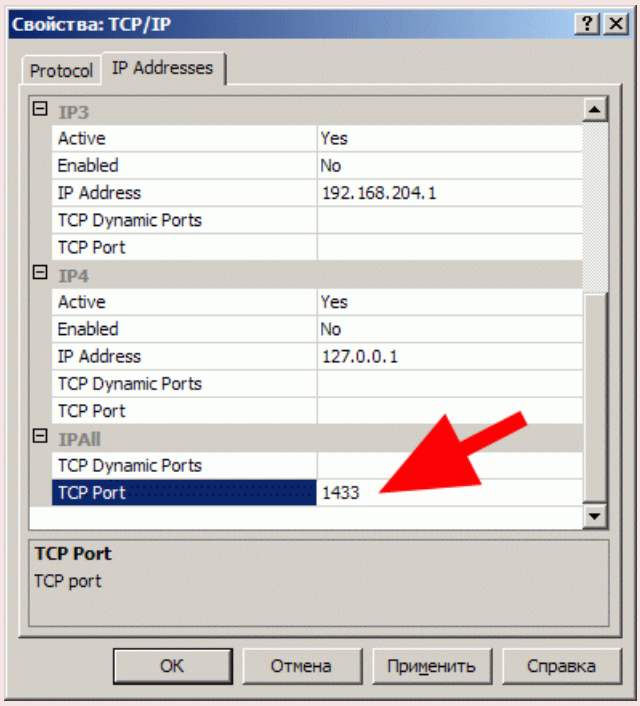
installed in several instances it is important to specify not only computer name and its IP address but also instance name and its port while connecting to the server.
For example: SERVER\Instance1 or 192.168.1.10,1433
It is possible to see instance name via "SQL Server Configuration Manager". Installation by default will be named as "MSSQLSERVER".
For remote access to instance different to instance by default it is necessary to turn on service "SQL Server Browser" on the server. It is also convenient to do it via "SQL Server Configuration Manager".

Server authentication mode **"Windows authentication"** is unsupported for software suite! In this case it is recommended to change it to **"mixed"** mode.
This can be done in the system registry:
HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.<InstanceId>\MSSQLServer\LoginMode set to **2** and restart SQL server!

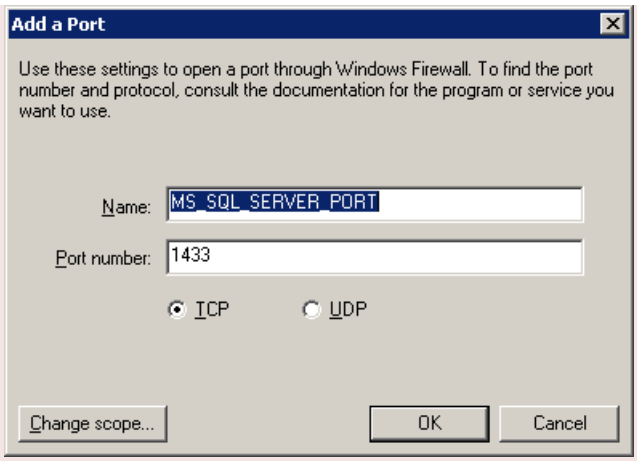
Then you need to check if there is an access to server through the network in case of remote SQL server position.
You need to start **SQL Server Configuration Manager** (through the menu "START")
and check TCP/IP protocol has to be activated:



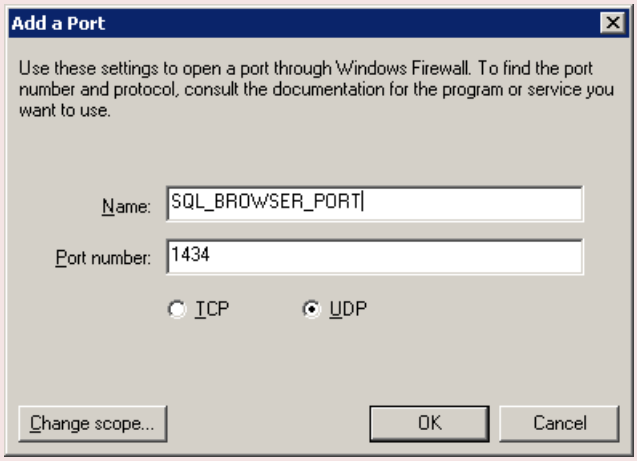
Also it is necessary to set TCP **1433** port (or other) in the protocol settings:



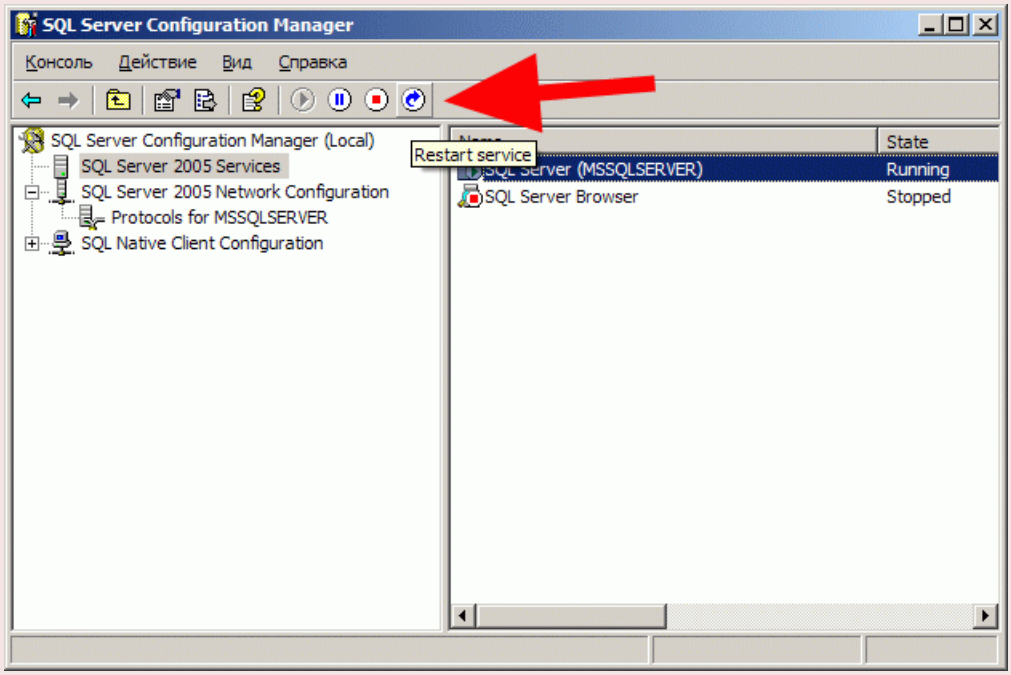
Also make sure this TCP port **1433** is added for exclusions in your firewall:



Also make sure UDP port **1434** is added to exclusions in your firewall (if instance is different to instance by default): (in such case it is necessary to activate service **"SQL Server Browser"**)



Afterwards the service **SQL Server** must be restarted:



For further work you need to know database administrator's login and password (it can be **"sa"** account or other) or Windows account.

SQL server re-installation

SQL server uninstallation must be done through "Control panel->Program installation and uninstallation".

In such case database file of Scopd **will remain** on the disk after server uninstallation.
It is nessesary to delete it for next server installation!
Files are located in the following path: "\Microsoft SQL Server\MSSQL.<InstanceId>\MSSQL\Data\stkh.*" (depends on MSSQL version)
Afterwards SQL server can be reinstalled.

3.2.3.3.3. MySQL

Starting from version 10.x of the complex, support for MySQL has been discontinued!

3.2.3.3.4. PostgreSQL

If PostgreSQL server was not installed before

It can be installed on **Windows** as well as on **Unix**.

The setup, as usual, is necessary to perform either on a separate server workstation or on administator's workstation (if separate server room is not available).

Attention! PostgreSQL versions below 11 are not supported!

During installation, you need to create a password for the superuser **"postgres"**, with its account you can further perform complex setup.

Setup on Windows:
The installation is intuitive and does not require comments, after which you may need to open the port **5432** in Firewall.
Configuration files **postgresql.conf** and **pg_hba.conf** are located in folder **data** of the main installation folder.

Setup on Linux (Ubuntu example):

```
sudo apt update
sudo apt upgrade
sudo apt install postgresql
sudo -i -u postgres
psql
\password postgres
Enter new postgres password: *****
Repeat postgres password: *****
\q
exit
```

Configuration files **postgresql.conf** and **pg_hba.conf** are located in:
/etc/postgresql/**<version>**/main/postgresql.conf
/etc/postgresql/**<version>**/main/pg_hba.conf
It is convenient to use to edit next command: **sudo nano**

If you need remote (**not localhost**) access to the SQL server, opening port in the Firewall will not be enough.
In the file **postgresql.conf** you need to make sure that the parameter **listen_addresses** is set to '*'
In the file **pg_hba.conf** you need to add the IP address(es) or ranges from which access will be allowed.
For example, change 192.168.0.1/24 to 0.0.0.0/0 (for all IPv4) and ::/0 (for all IPv6)
After the changes it is need to **restart** the SQL-server service!
On Linux:

```
sudo systemctl restart postgresql
```

Information about **SSL-encryption** is here.

If you need to be able to **login with Active Directory accounts**, then you need to make a number of settings (here).

If PostgreSQL is already installed

If PostgreSQL is already installed, then you only need to check the possibility of remote access to it (if required). See previous section "If PostgreSQL server was not installed before".

If you need to be able to **login with Active Directory accounts**, then you need to make a number of settings (here).

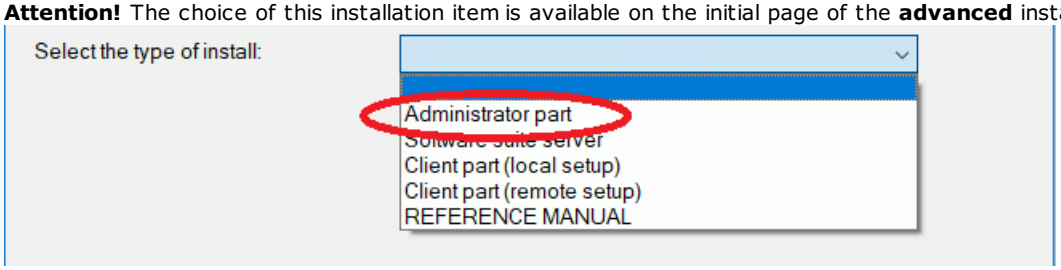
PostgreSQL-server re-installation

Removing the SQL server should be done in a standard way through the "Control Panel" -> "Add or Remove Programs" (information for Windows).
In this case, after deleting the server, the Scopd database files will remain.

It is recommended to delete database files before reinstalling the SQL-server again.

3.2.3.4. Step 2. Installing the administrator software

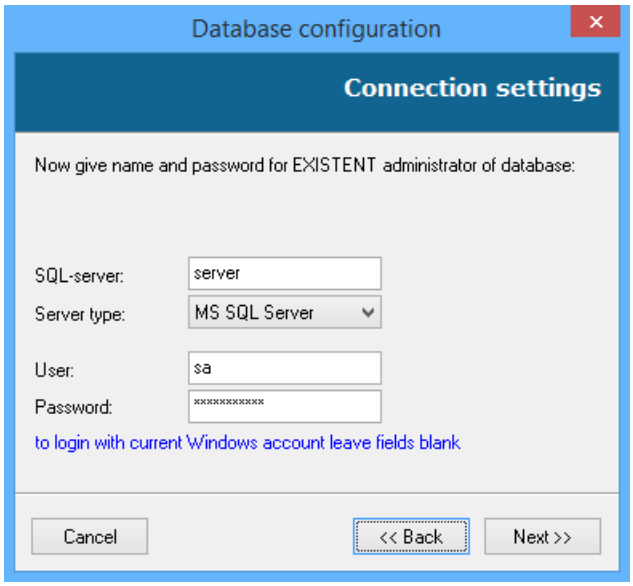
Attention! The choice of this installation item is available on the initial page of the **advanced** installation of the complex:



Usually administrator's program is set up on a separate computer although it can be installed on the computer with SQL server if required.
The main program objective is changing all settings for clients' workstations, server settings as well as setting up permission rights for additional administrators/managers.
It is possible to install this program on several computers simultaneously if there are several administrators working on different computers in your organization.

The setup will run only in administrator's account!

When setup is finished the database configuration utility will be launched automatically.
It is possible to launch this program again at any moment if required (for example after SQL server re-installation).
This program will create the Scopd database on the SQL server and will perform all required activities to get started.
It's enough to run this program only once.
It is necessary to know the database administrator's login and password to enter the program. For example, user **"sa"** for **MSSQL**, **"postgres"** for **PostgreSQL**.
It is possible to enter **MSSQL** with **Windows accounts**:
- do not specify the user or password to enter with **current account**;
- designate user in **DOMAIN\username** format (domain without dot in NETBIOS form) to enter with **a certain account**.



Information about **SSL-encryption** is here.

If **an error** occurred and you've **uninstalled** SQL server before it is necessary **to delete old Scopd database files** that remained after SQL server reinstallation (this information is valid only for MSSQL Server).
Usually they are located in the following path: "\Microsoft SQL Server\MSSQL\Data\stkh.*". Afterwards it is required to restart the database configuration utility **once more**.

After successful processing the database is ready for operations and now you need to execute the **"Global settings"** application. It is important **to add at least one manager** at once in the program and define needed rights. See here

Then it is necessary to move to the page with clients' computers and server settings. See here
Moreover it is possible to enter Global settings program with new created manager's login (if you have delegated corresponding rights for changing settings).

Alternatively it is possible to create a **dossier** for each employee (in the tab "Dossier of employees").

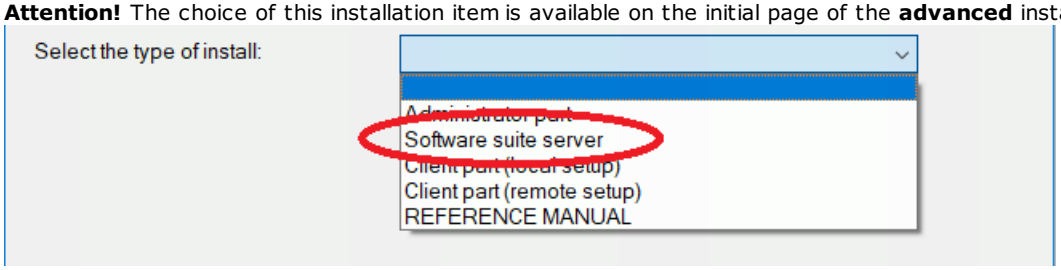
Optionally it is possible to create a **company hierarchy** for more convenient view (See here).

Automatic **synchronization with Active Directory** is also available in homonym tab here.

It is possible to finish operation in Global settings after creating a manager and settings setup.

3.2.3.5. Step 3. Installing the suite server

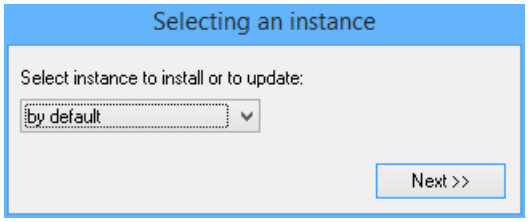
Attention! The choice of this installation item is available on the initial page of the **advanced** installation of the complex:



Scopd server is a Windows system service which connects all client computers and "BOSS-Online" programs.
Usually the server is installed on a single computer. Although if required it can be installed on administrator's computer.
The server must be enabled during the whole clients' computers operations (although intervals in client-server connections loss are possible). Otherwise data is stored on the clients' computers till connection will be restored.
In general it is possible to operate with several servers within one company. Thus in many cases one server is enough.

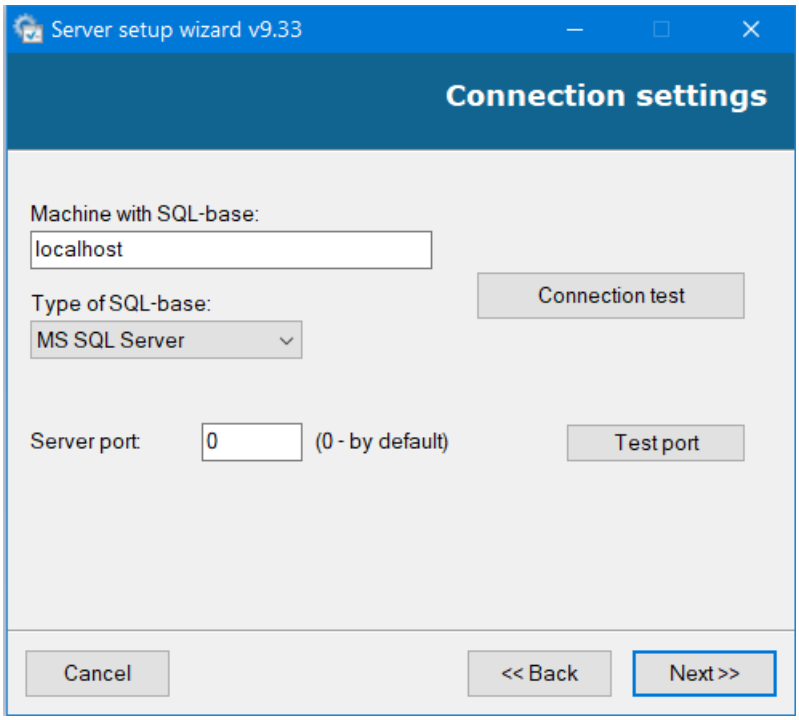
The setup will run only in **administrator's account**!

At once you will be suggested to choose the server instance:

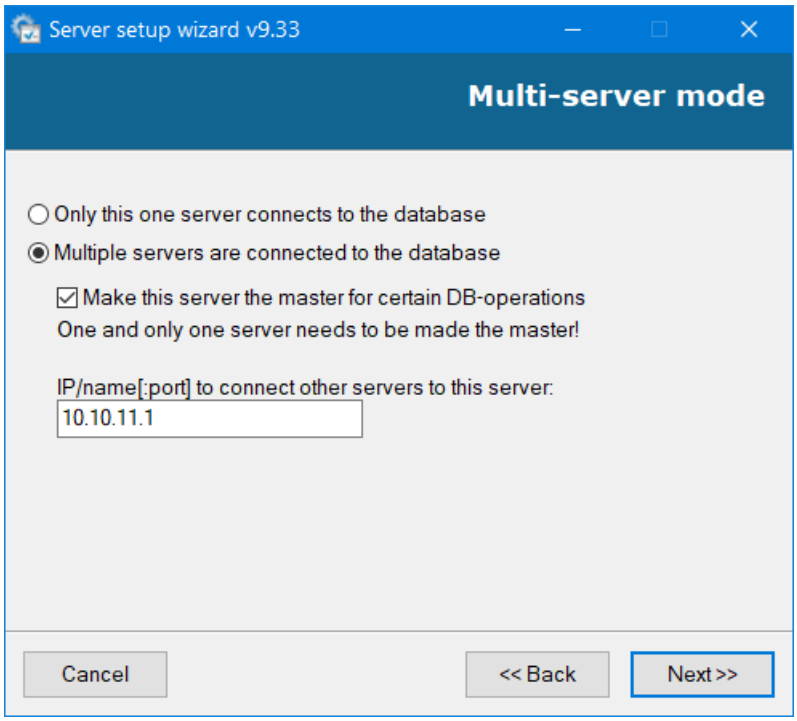


In many cases the software suite server is installed in a single instance on a single computer that is why it is necessary to leave installation option as "by default". However, if you wish to setup several suite server instances on a single computer you need to choose installation unique instance.
In this case each instance is like an independent server can connect to a certain SQL server instance.
Client computers also must be connected to a certain software suite server instance. In above mentioned case it is necessary to specify not only computer's name or its IP but also server instance port as well while connecting to required instance: **machine:port**, for example: **SERVER:12345**
How to choose the port for Scopd server will be described later.

Then server settings program will be launched.
At the first page it is necessary to identify connection settings with SQL base as well as specify the port for clients connections.
It is possible to leave 0 in **TCP server port for clients connections** (by default) if you don't use multi-instance server. If you have several server instances on a single computer then **the port must be unique** for each instance. Do not leave it "by default"!
The server setup program can be run at any moment to change setting (in such case if the port has changed it is necessary to restart server suite service):



If in your architecture several servers of the complex must connect to a single database, on the last page of settings you need to enable the "multi-server" mode and additionally configure two parameters:
1) **"Make this server the master"**. Only one server in this configuration should be the master. It is recommended to assign the one that is located "closer" to the database.
2) **"IP/name to connect other servers"**. When generating reports in BOSS-Offline, it will be possible to transfer shadow copy files between servers, so here you need to specify the IP (name) and optional port (if different from the default port) of this server to access it from other servers of the complex connected to a single database.



Apache web server will be also installed in the folder **%ProgramFiles(x86)%\httpd**
The web server is needed for monitoring and reviewing reports in browsers.
Apache web server is Windows system service that listen connections on **HTTP ports 80/443**
All settings are stored in the file %ProgramFiles(x86)%\httpd\conf\httpd.conf which you can change by yourself.
Here you can see how to setup access via secure **https:**
After web server installation is complete on Windows Firewall the ports 80/443 will be opened completely. If you have non standard Firewall either **ports 80/443** or **%ProgramFiles(x86)%\httpd\bin\httpd.exe** must be added to its exceptions.
If by some reasons you won't be able to use ports 80/443 then it can be changed in %ProgramFiles(x86)%\httpd\conf\httpd.conf (to change see parameter "Listen"), after **Apache service must be restarted**.

If any web server (**Apache**, **Microsoft IIS** or other) **has been already installed** on your server computer the program will detect that **ports 80/443 is busy** and will install embedded Apache on **ports 81/444**.
- If using ports 81/444 is acceptable in this case you don't need to do anything more (just don't forget to add port when moving to web site: http://localhost**:81**/scopd).

- If it is necessary to use only port 80/443 and additional web servers are not required then they must be deleted (for example IIS) and changed embedded Apache to 80/443 (see above how to do it).
- If it is required to use only existing web-server then certain servers settings must be adjusted on its own:

If Microsoft IIS web server has been already installed

In such case it is necessary just to create virtual directory on a web server with the link to suite web content.
It is important **to allow CGI program execution** inside the directory.

Attention! It is necessary to check whether **CGI/ISAPI support has been installed**. If it's not available it is necessary to install it (see **"Windows components installation"** for clients OS and **"Server role"** for server OS). If installation is not done CGI startup won't be possible!

Attention! IIS will run the CGI scripts in context of special user **IUSR** that is why if a folder with **shadow copy, screenshots, webcamera shots, auto recording** aren't located **on server disk C:** it is necessary **to give read permissions for user IUSR to these folders**!

It is possible to run **inetmgr.exe** and enter server section **"ISAPI and CGI restrictions"** to set permissions:
"Allow to execute unspecified CGI modules"

In the section **"Configuring Handler Mappings"** map **.exe** with **CGI module** and **allow execution**

Then add virtual directory **"scopd"** and specify the path to folder with software suite web content:
C:\ProgramData\PBL\Stkh\Server\Web

If Apache web server has been already installed

In such case it is necessary just to add alias **"scopd"** with the path on software suite web content.
For **WinXP/2003** this content is located here: **"C:\Documents and Settings\All Users\Application Data\PBL\Stkh\Server\Web"**
For **Vista/7/2008** - here: **"C:\ProgramData\PBL\Stkh\Server\Web"**
It is important **to allow .exe CGI program startup** inside directory!

Here is example with settings (path for WinXP/2003) that need **to be added** to file **httpd.conf** Apache web server:

```
##############################
Alias /scopd/ "C:/Documents and Settings/All Users/Application Data/PBL/Stkh/Server/Web/"
Alias /scopd "C:/Documents and Settings/All Users/Application Data/PBL/Stkh/Server/Web/"
<Directory "C:/Documents and Settings/All Users/Application Data/PBL/Stkh/Server/Web">
    AllowOverride None
    Options FollowSymLinks ExecCGI
    Order allow,deny
    Allow from all
</Directory>
AddHandler cgi-script .exe
##############################
```

If other web server has been already installed

In such case it is necessary just to add an alias (or virtual directory) **"scopd"** to suite web content directory.
For **WinXP/2003** this content is located here: **"C:\Documents and Settings\All Users\Application Data\PBL\Stkh\Server\Web"**
For **Vista/7/2008** is here: **"C:\ProgramData\PBL\Stkh\Server\Web"**
It is important **to allow .exe CGI program startup** inside the directory!

You don't need to do anything if there isn't **any web server installed** or **you don't know** what is web server!

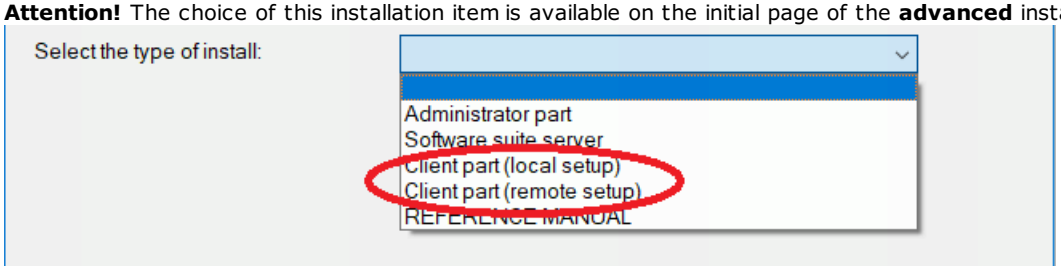
After installation the server is ready to work and running.

Note: the server uses TCP port `13289` by default, the web server uses standard **HTTP ports 80/443** by default.

3.2.3.6. Step 4. Installing the client part:

3.2.3.6.1. General description

Attention! The choice of this installation item is available on the initial page of the **advanced** installation of the complex:



Client part performs monitoring of users and transfers data to server (if connection to the server is currently available). The server records all monitoring data in the SQL database.
Client part must be installed on each clients' workstation only **once**.
In case of **terminal server** usage it's enough to install only once on the terminal server.

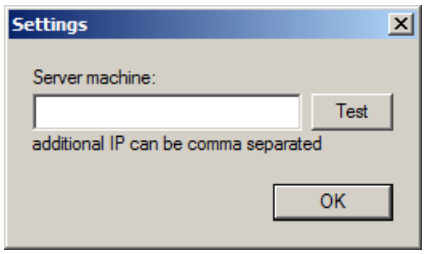
It is suggested to install client's app **on the local computer** or to install it **on the remote computers** at the setup stage. Let's have a closer look at both options.

Attention! By default monitoring mode is set with notifications, so when the client is manually installed on the local machine, the notification message will be shown (even before the actual settings are received from the server), despite the possibility of disabling this notification in the settings (see here)! When remote installation is used, priority is given to the current settings.

3.2.3.6.2. Installation on local computer (Windows)

The setup will run only in **administrator's account** !
If there are several users on one workstation the installation must be performed only **once** in administrator's account!

After setup configuration app will run automatically:



"Server machine" - it is necessary to set suite server IP address or DNS-name. In case of connection to nonstandard port (or connecting to a certain server instance) specify the port with colon also (for example, **SERVER:12345**).
Also you can specify an additional server address separated by comma. Usually this is the external IP of the same server for case employees can take out laptops from the office. Client will automatically reconnect to the external address if there is no connection to the internal corporate server.

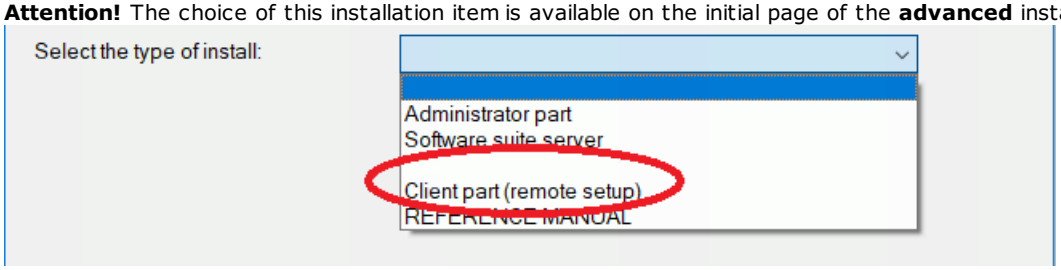
At this stage client's app installation is completed. There will no visible changes in the system.

Client's app can be **deleted** only via BOSS-Online app.
It is possible **to change settings** either from client's workstation (by running installation app again) or from BOSS-Online app.

3.2.3.6.3. Installation on the remote computers (Windows):

3.2.3.6.3.1. General description

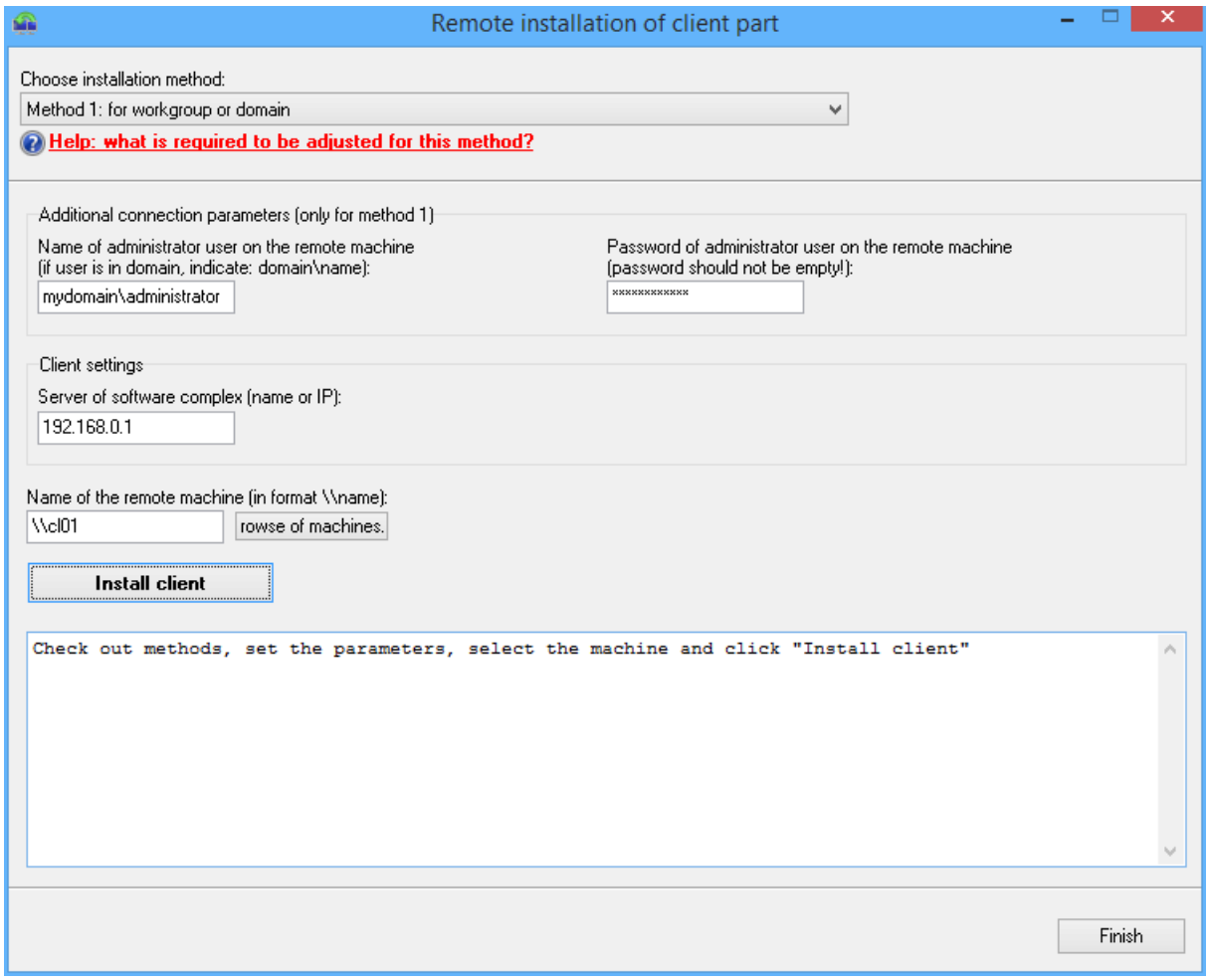
Attention! The choice of this installation item is available on the initial page of the **advanced** installation of the complex:



It is possible to install client app on remote computers from the workgroup or domain. There are four different installation options you can choose.
Perhaps some preliminary activities must be performed for remote installation (especially important for workgroup). Detailed information about each option is provided later.

See also **"Automatic deployment in Active Directory"**

Remote installation app:



Client's app can be **deleted** only via BOSS-Online app.
It is possible **to change settings** by executing installation app again or from BOSS-Online app.

3.2.3.6.3.2. Option 1. Installation in the workgroup or domain

1. It is important to know administrator's **name** and **password** of the remote computer. Besides administrator can be local as well as the domain one.
It is necessary to enter the name in the format **domain\name** for domain's administrator.
Sometimes it is required to enter the name in the following format **computer\name**

2. Make sure that shared folder **admin$** is actually shared on the remote computer. In most cases there is no need to do anything except to make shared access on the remote computer:
net share admin$

3. For workgroup: it is important to check the parameter in the remote computer registry:
HKLM\SYSTEM\CurrentControlSet\Control\Lsa
ForceGuest DWORD type
This parameter has to be equal **0**
For domain: this parameter is set in security policies ("Network access"). By default is set in such way that it doesn't need to be changed.

4. For workgroup: it is required to disable UAC there (Users Account Control) or to add this parameter to the registry:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
LocalAccountTokenFilterPolicy:DWORD=**1**
For domain: it doesn't need to be changed.

5. For **Windows Home Edition** this option may not work!

6. For domain: make sure that domain administrator (used to perform the installation) and the user whose credentials are entered for installation (in the particular case it may be the same user), are not removed from the list of local administrators of the remote computer (see "Computer management"->"Local users and groups"->"Administrators" on the remote computer)

7. "Remote registry" service must be enabled on the remote computer.

See also **"Automatic deployment in Active Directory environment"**

3.2.3.6.3.3. Option 2. Installation only for domain

1. It is necessary to perform installation with domain administrator's rights.

2. Make sure that shared folder **admin$** is actually shared on the remote computer. In most cases there is no need to do anything but shared access has to be performed on the remote computer:
net share admin$

3. "Remote registry" service must be enabled on the remote computer.

4. It is important to make sure the domain administrator is not deleted from local administrators list on the remote computer (see "Computer management"->"Local users and groups"->"Administrators" on the remote computer)

Attention! Sometimes some antivirus software on clients' computers can block this installation option.

See also **"Automatic deployment in Active Directory environment "**

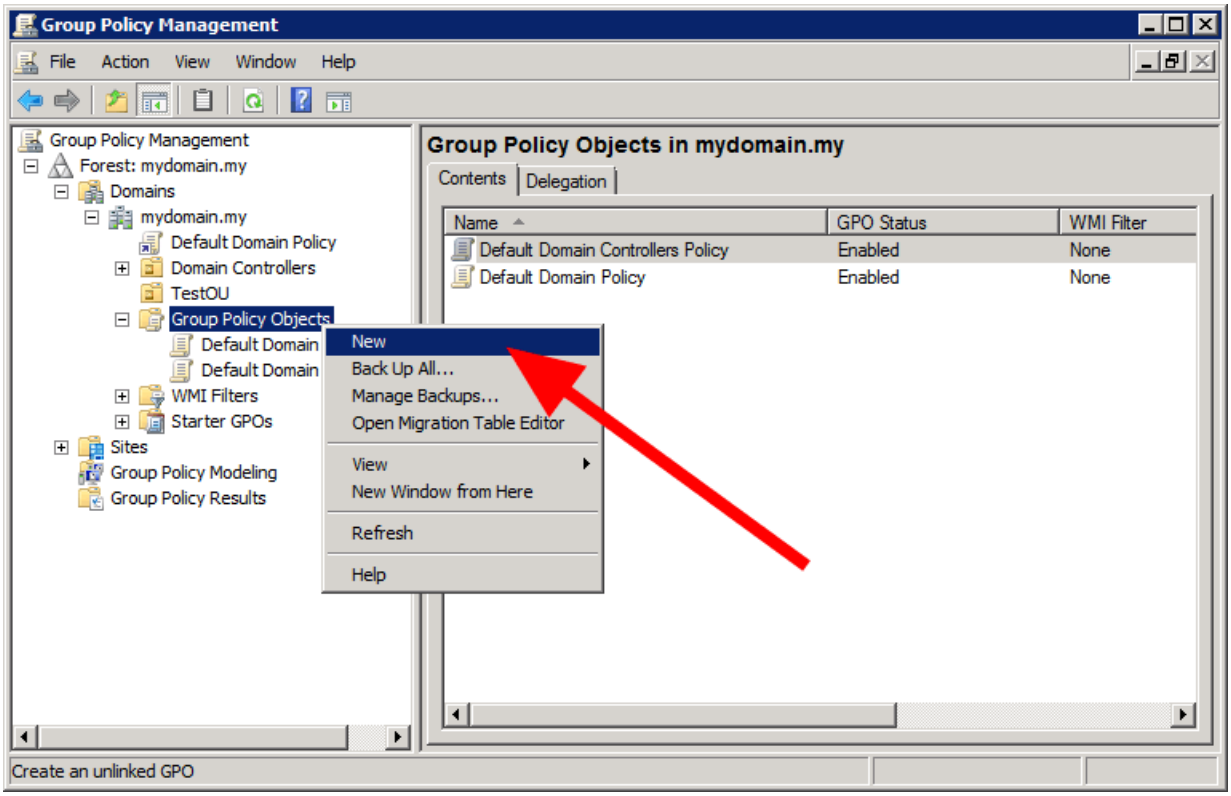
3.2.3.6.3.4. Option 3. Installation via Active Directory

With the help of Microsoft Active Directory service it is possible to perform automatic remote installation of the client's app on a group of computers. To perform this installation procedure it is required to obtain domain's administrator's rights as client's app will be installed on computers from this domain. It is also required to have network resource available for reading (Shared Folder).

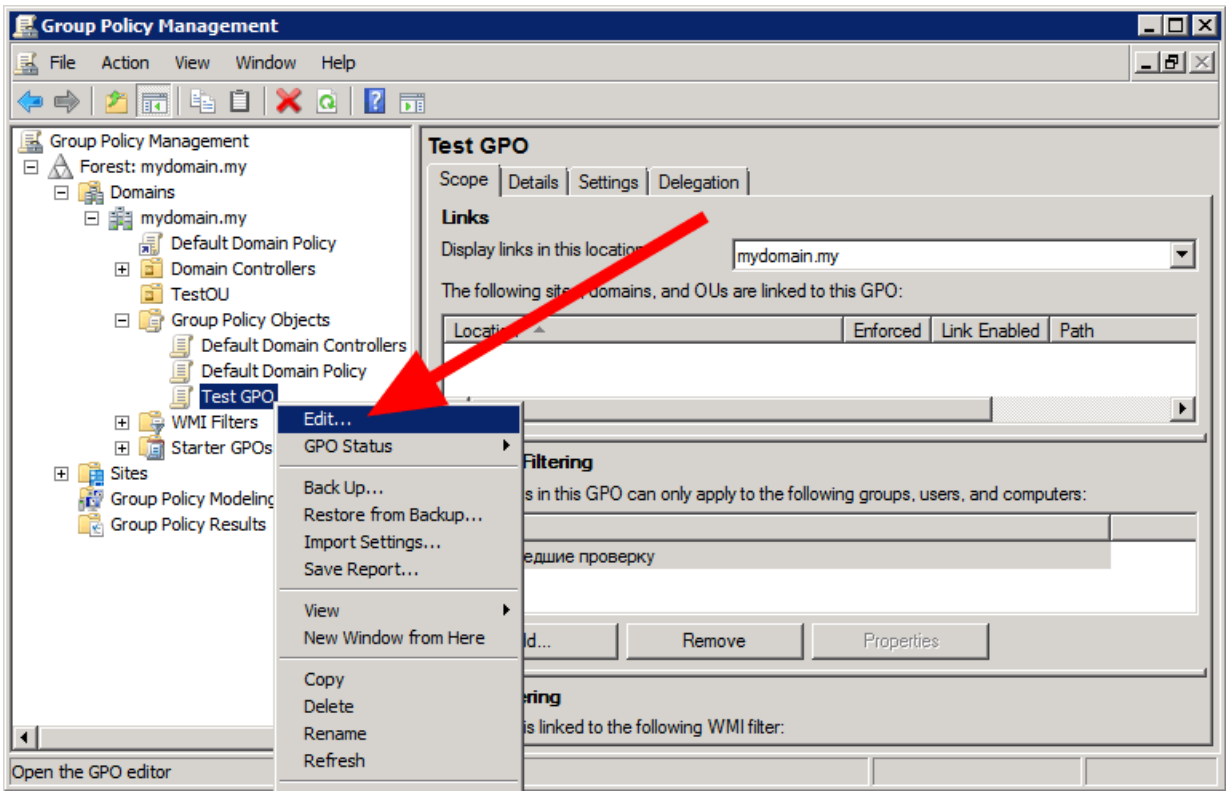
Run the installer by selecting the "Installation on the remote computers" mode. In the Remote Installation Wizard select method 3.

Here as an example will be shown creation of GPO ("Test GPO"), setup of msi-packages and adm-template, as well as linkage of this created GPO to the present OU ("TestOU") with computers for which you initially need to deploy clients.

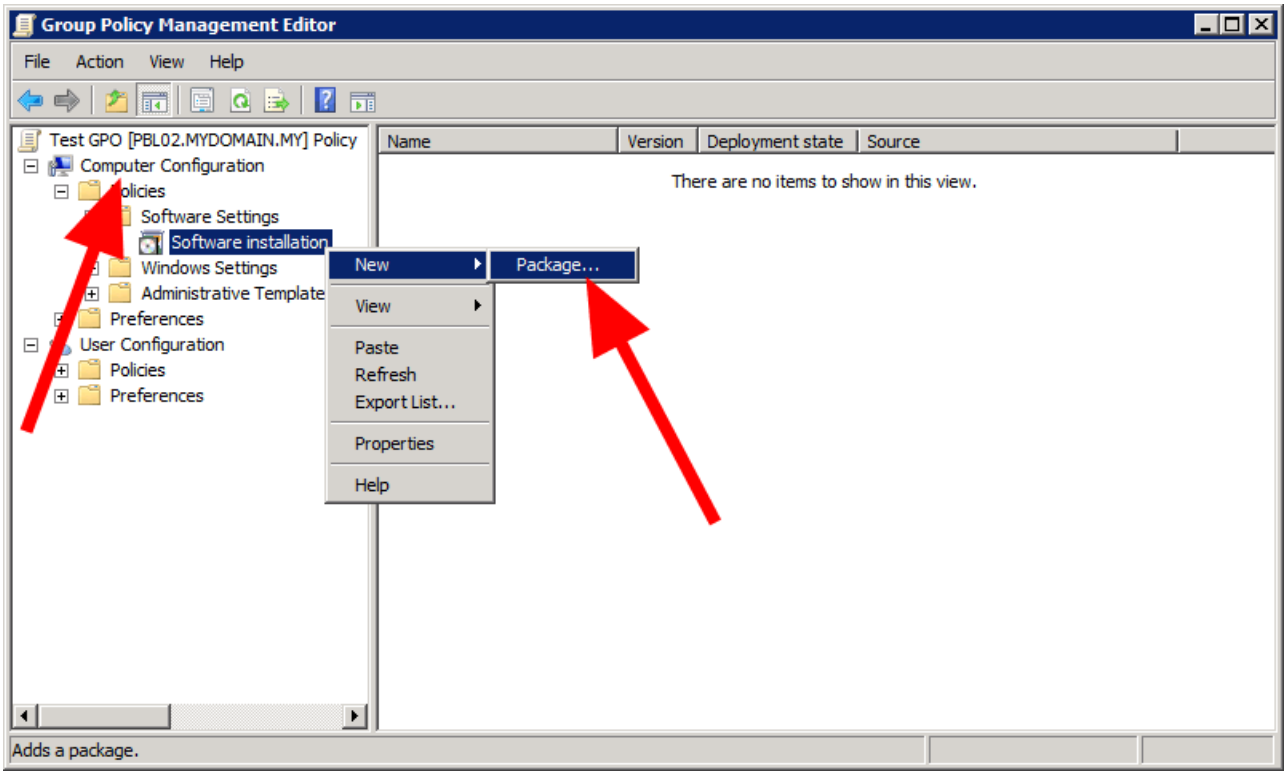
First create new GPO ("Test GPO"):



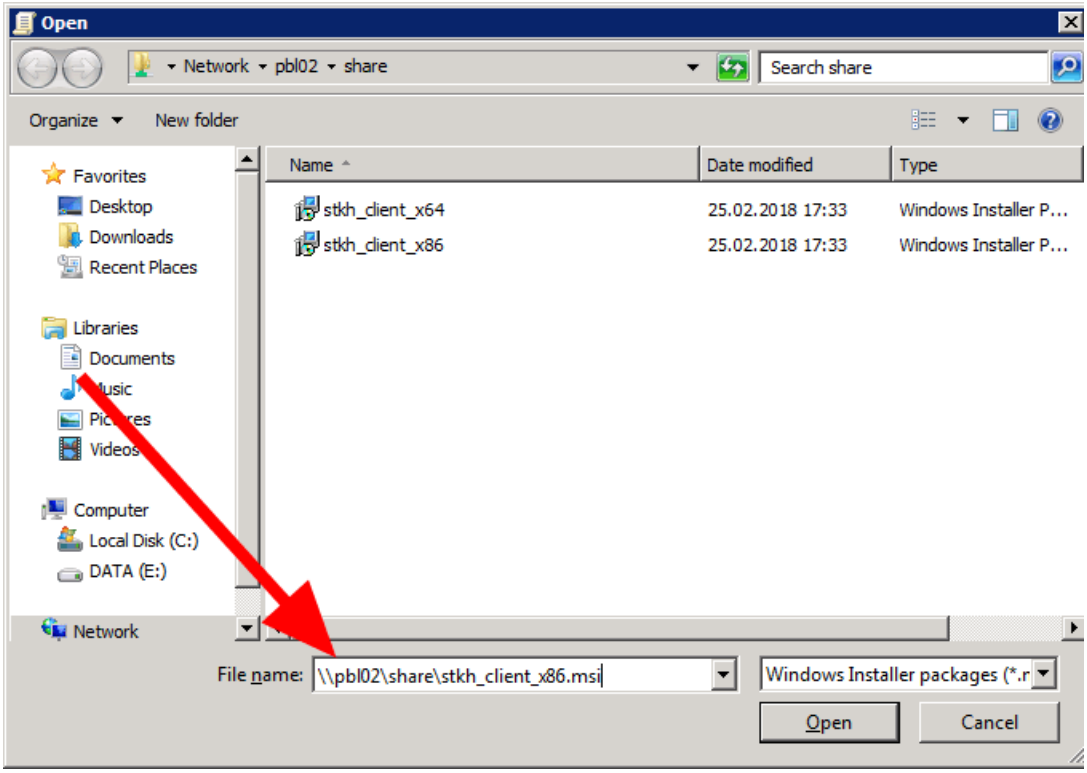
Edit created object:



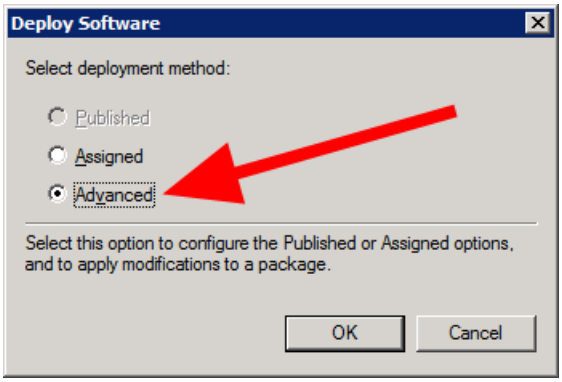
In **Computer Configuration** add msi-package:



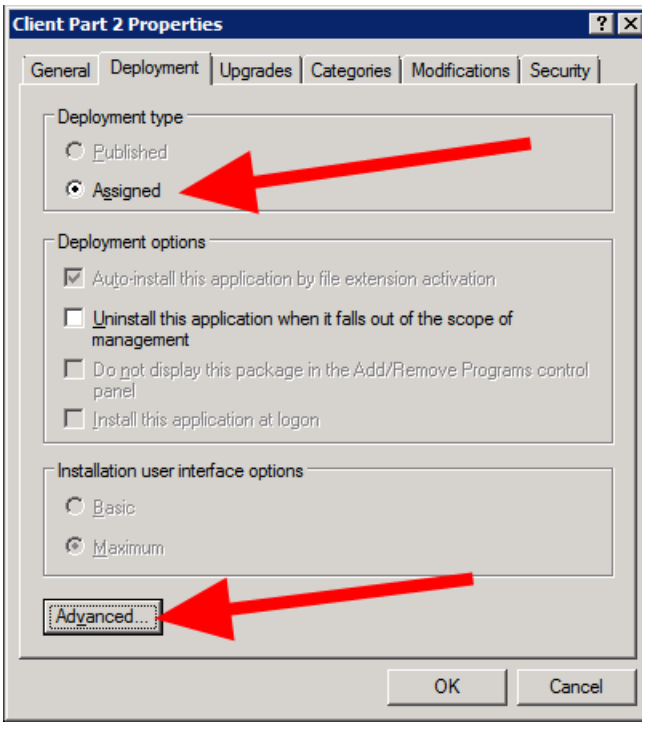
Choose path for msi (x86) always within **network share**.
You must first copy the msi packages into this network folder, and the client machines must have access to this path:



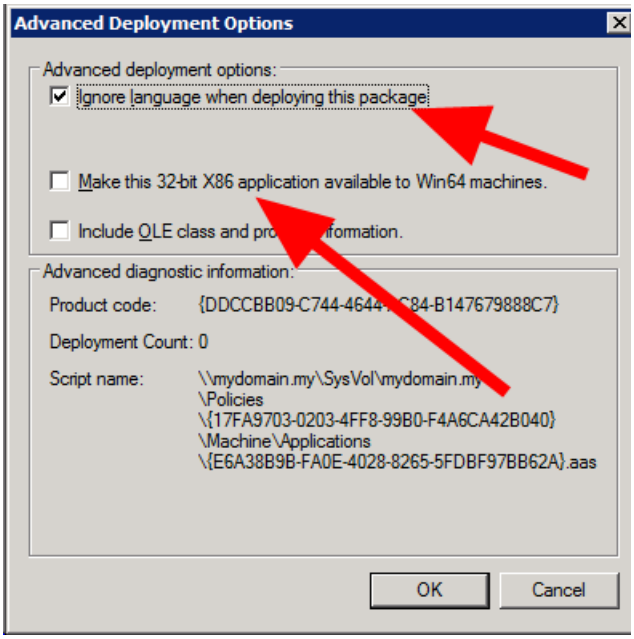
Select type of deployment:



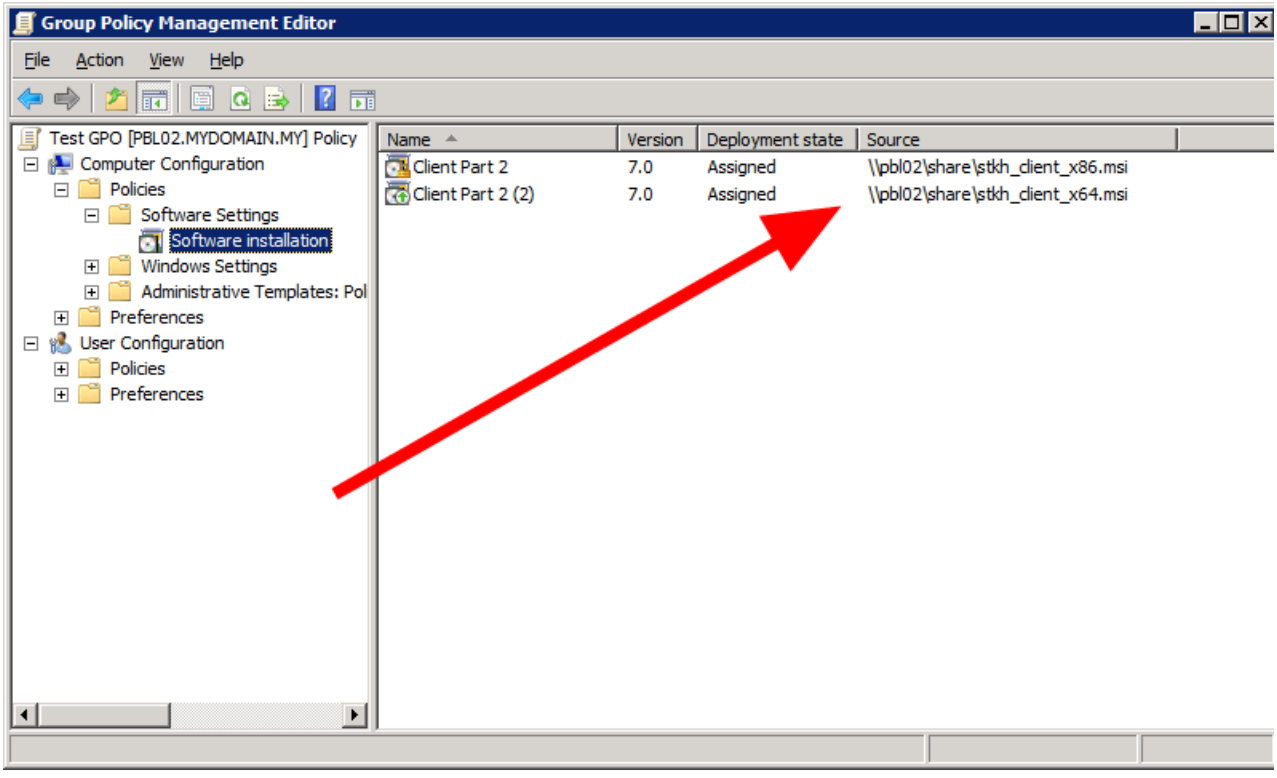
Go to the advanced settings:



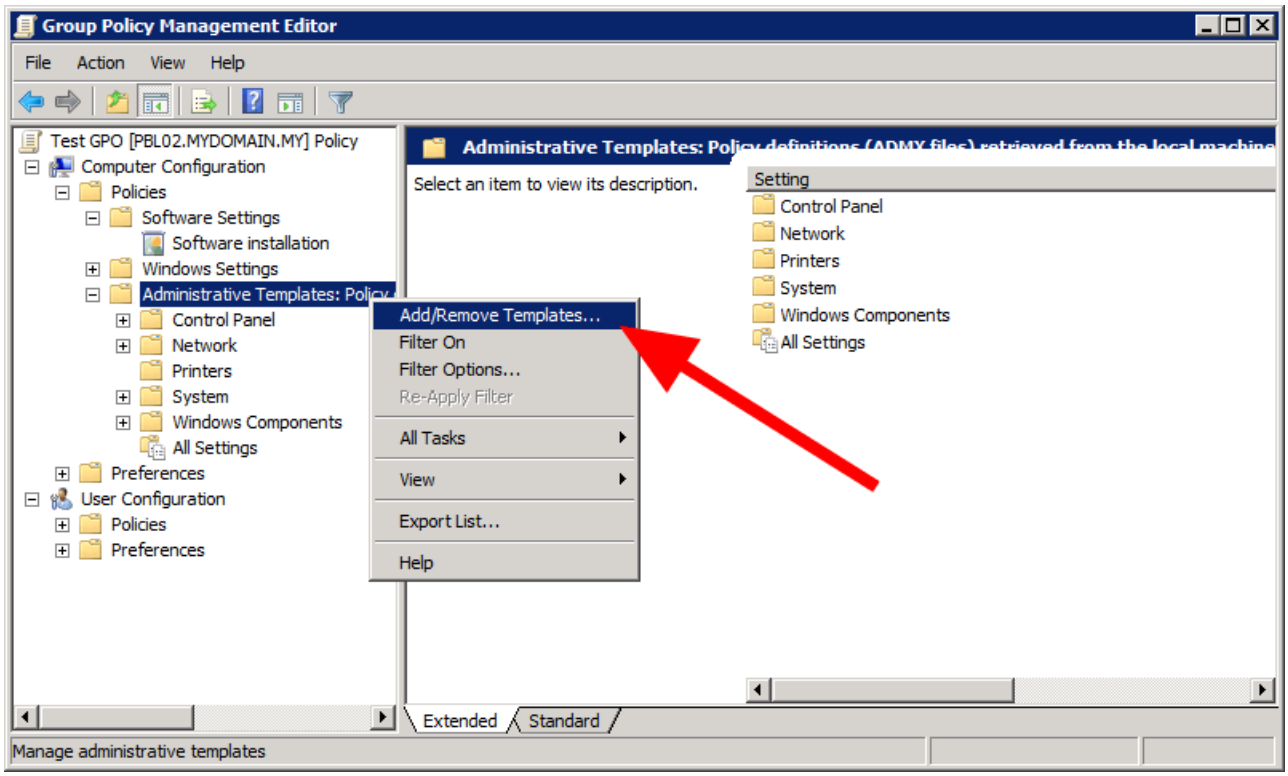
Change flags:



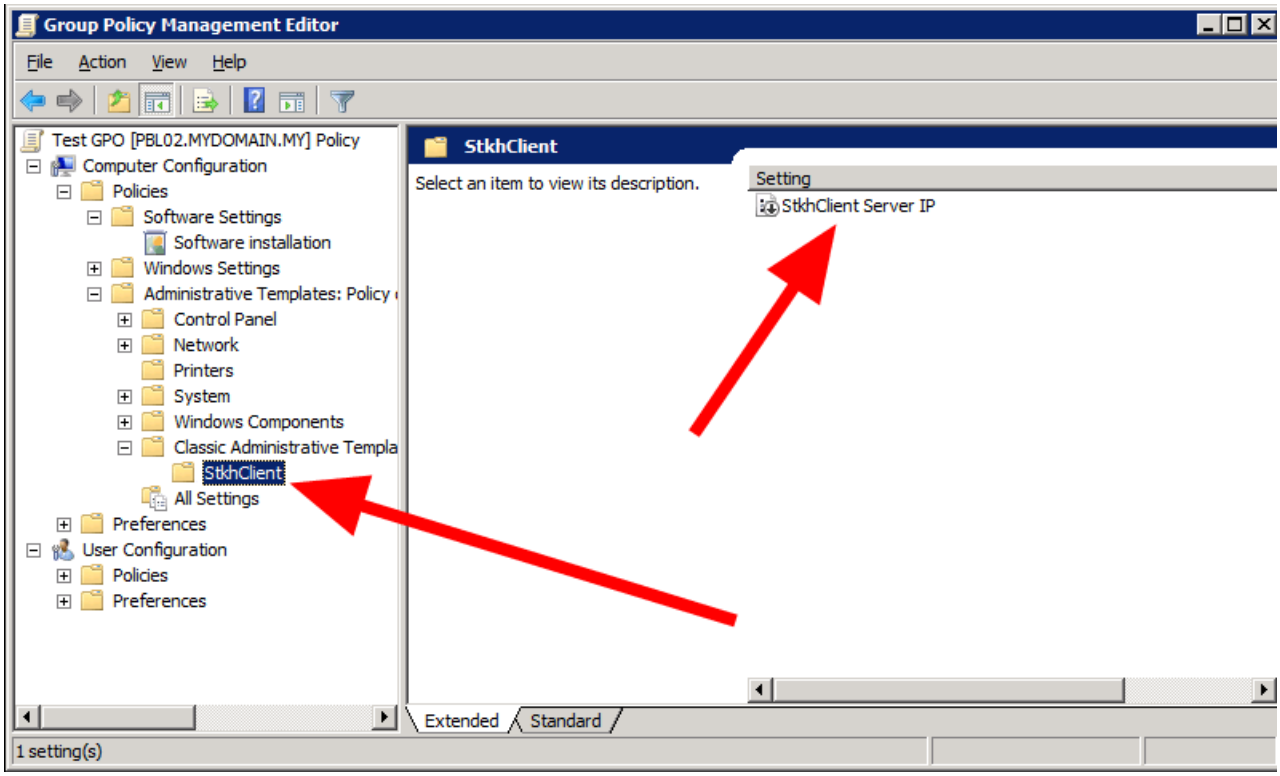
All the same again for the x64-package:



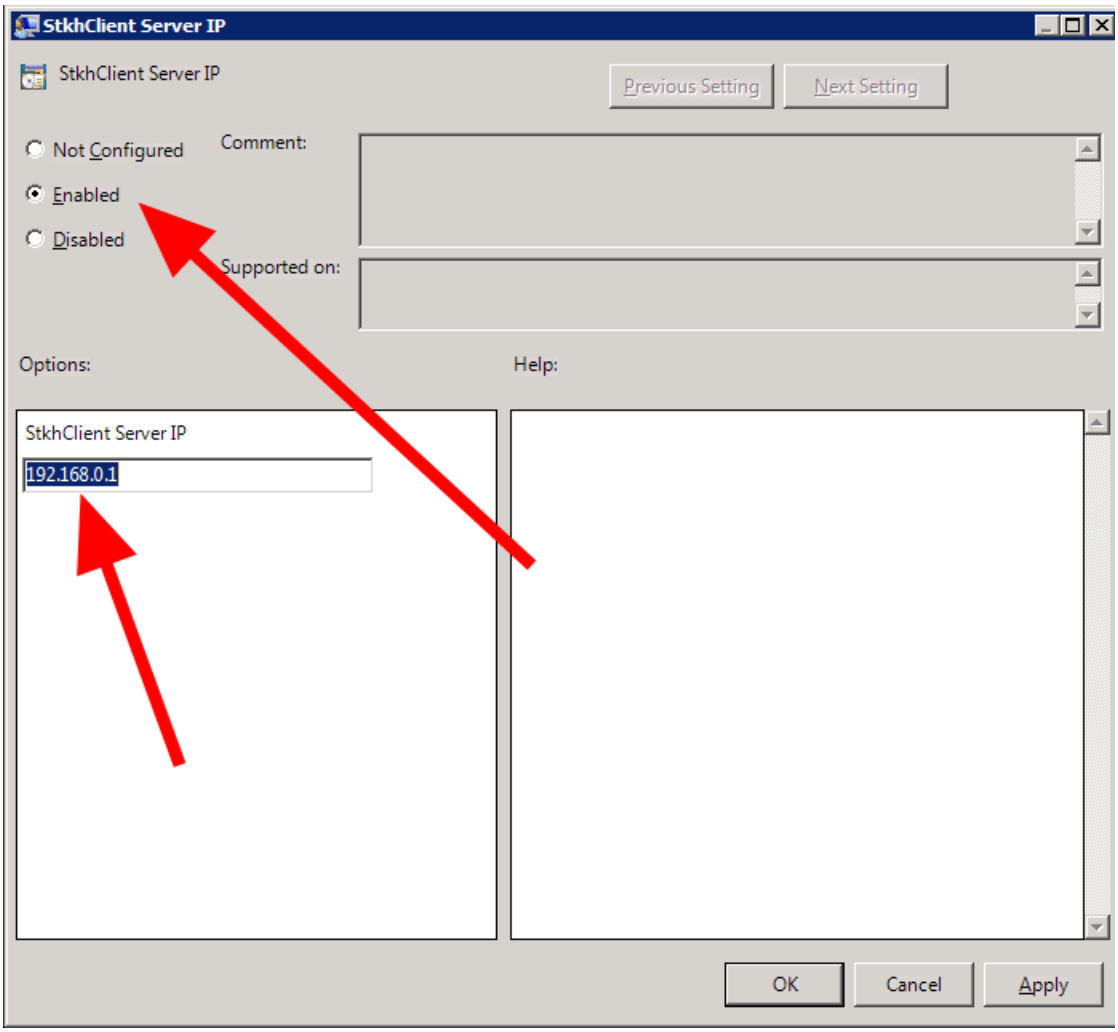
Add template from attached adm-file:



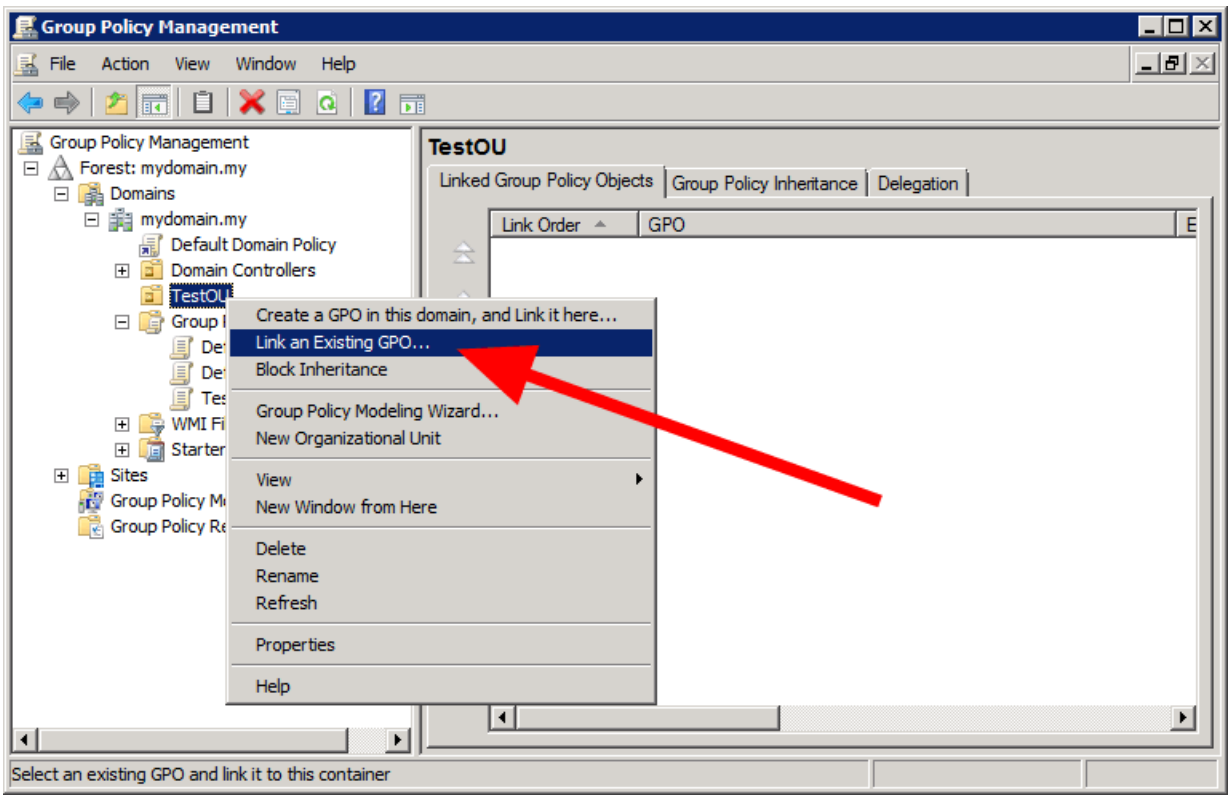
Edit newly added template:

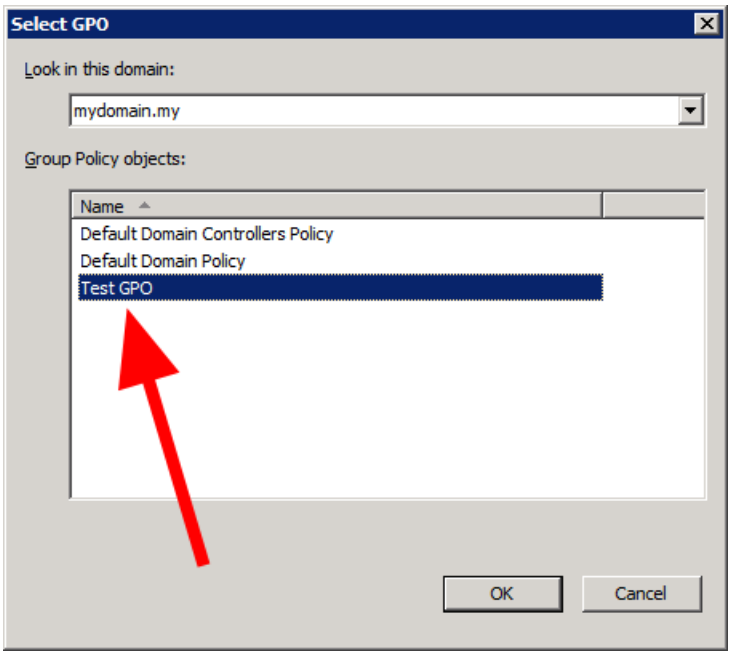


Setup IP/server name for the client connections:

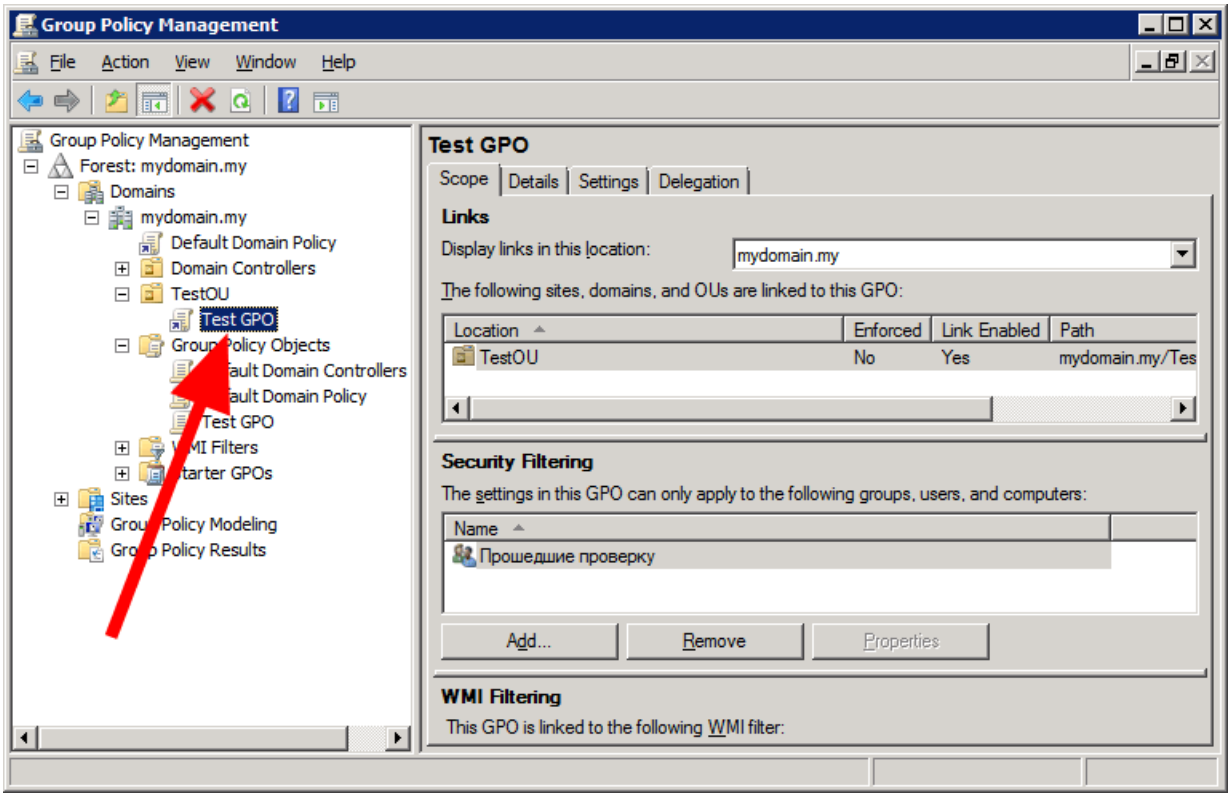


Link created GPO to the OU with computers:





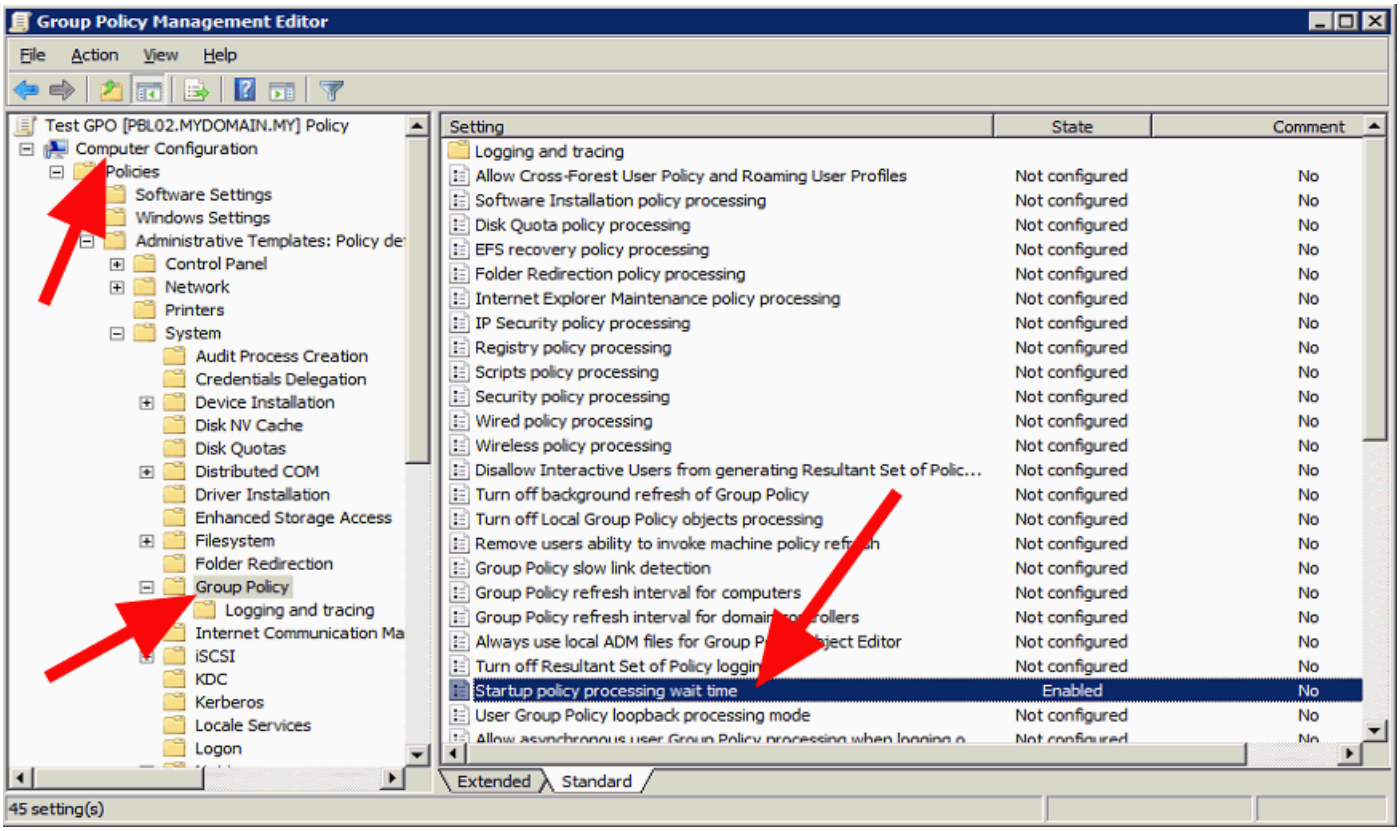
Setup is finished:



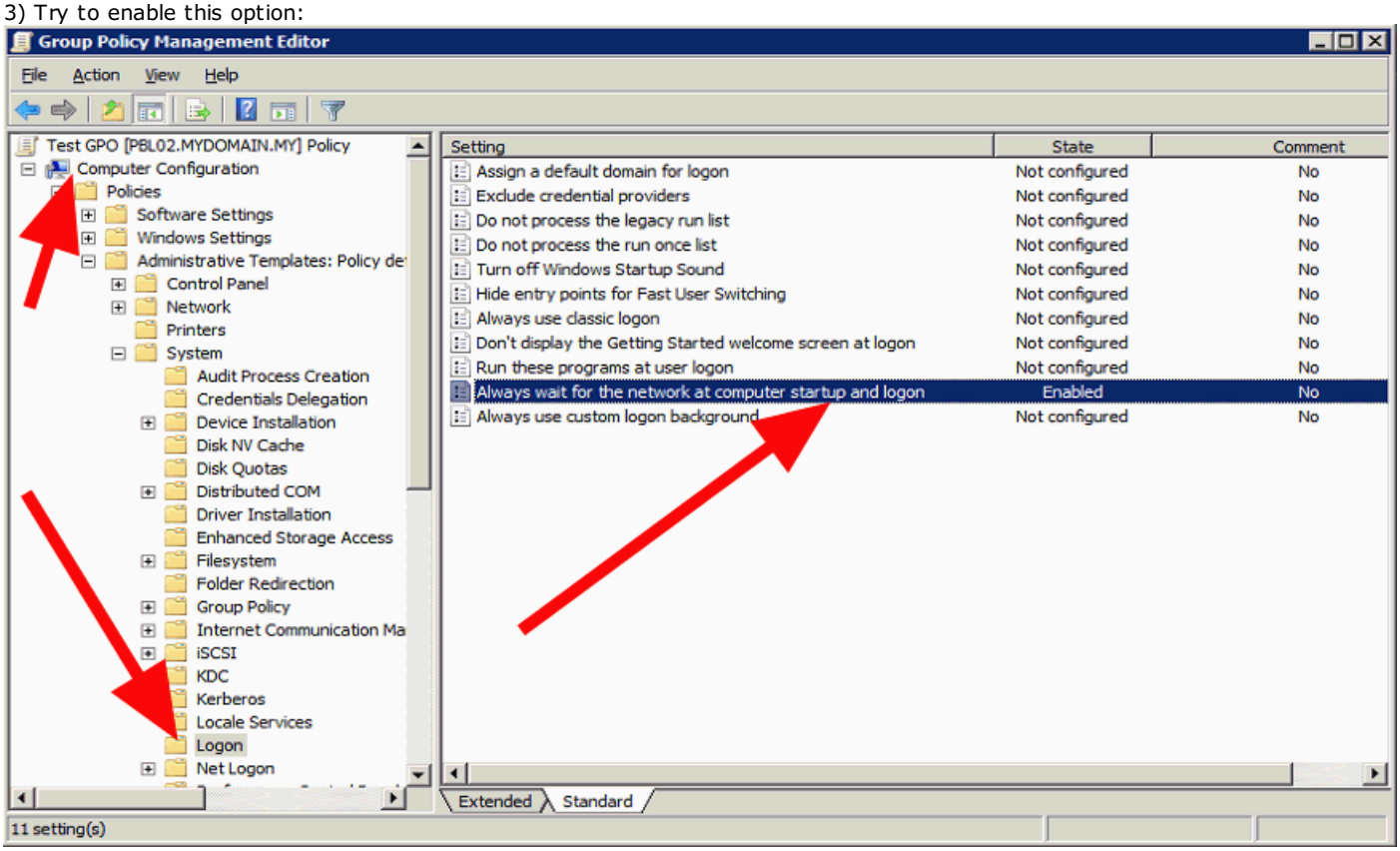
Then after next restart of the clients workstations the client's app will be installed.

Note: this .msi-package do not contain information about updates and uninstall so these actions are performed only with **software suite** and not with Active Directory!

If after restart **nothing has happened**:
1) Try to restart client's computer one more time.
2) Try to increase loading time up to 30 seconds:



3) Try to enable this option:



4) Perform on the client's computer: **gpupdate /force**

See also **"Automatic deployment in Active Directory"**

3.2.3.6.3.5. Option 4. Installation via command prompt

Run the installer by selecting the "Installation on the remote computers" mode. In the Remote Installation Wizard select method 4.

Attached file of client's installation **inst_client.exe** can be run **locally** as well as **remotely**.
Common installation with all dialog windows (interactive mode) will be run from the local machine without command prompt specified.
If **-server <machine>** is specified from command prompt then "silent" client's app installation will be performed and client will be connected to server <machine>
For example:
inst_client.exe -server "192.168.1.1"

Usually such remote "silent" installation can be used with **Microsoft System Center** or other software which allows to run programs remotely.

Attention! If client's app has been already installed then only the parameter **<machine>** will be changed for connection to server. However, if you specify the optional **-forceupdate** parameter along with the **-server** parameter, the client will be updated after the PC is rebooted.

See above **return codes** of command execution:
0 - success;
1 - success, but client's app will be activated after restart (sometimes it is only possible on WinXP);
-1 - not supported old OS (Win2000/98);
-2 - administrator's rights required;
-3 - user has stopped installation (only interactive mode);
-4 - client's app of version 1.xx is installed. First it is necessary to delete it;
-5 - it is necessary to perform restarting and then continue with installation;
-6 - an error of writing to file;
-7 - in non interactive mode the startup was made without command prompt.

If you add the **-nostart** parameter to the command line, the client service will be installed but not started. The launch will occur only after restarting PC or in manual mode.

Also it is possible to **uninstall client** using command line.
Uninstall and keep reports: **inst_client.exe -uninstall_keep -key <KEY>**
Uninstall with reports also: **inst_client.exe -uninstall_delete -key <KEY>**
Parameter **<KEY>** should be the same like set at this settings page.

Also additional return codes are possible with uninstall option:
-8 - client not installed or cannot connect to the client;
-9 - internal error;
-10 - key is not set in the settings;
-11 - entered key does not match the one set in the settings.

3.2.3.6.4. Installation on local computer (Linux)

Installation package should be downloaded here.

It is highly recommended to use standard Linux **terminal** for entire installation process!

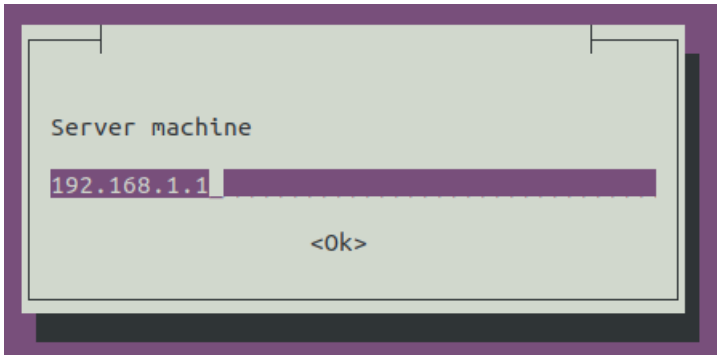
Installation of .deb-package (Ubuntu, Debian, Linux Mint, Astra Linux):

1. Update packages lists:
sudo apt-get update

2. Setup our package:
sudo dpkg --install stkh-client_X.XX_amd64.deb

3. In case problem with dependencies additional must be downloaded:
sudo apt-get install -f

During the setup process standard window with "Server machine" field will appear:



The options for filling this field and the rules for client update/uninstall are completely similar to the Windows-client.

Installation of .rpm-package (CentOS, RED OS, Rosa Linux, AltLinux, AlterOS):

1. Setup our package:
sudo yum localinstall stkh-client-X.XX-0.x86_64.rpm
For Rosa Linux:
urpmi stkh-client-X.XX-0.x86_64.rpm

2. Set the server connection option:
stkh-client --server=192.168.1.2

3.2.3.6.5. Installation on the remote computers (Linux)

Remote installation is available via the **web interface** of the Global Settings (menu item "Client part" - "Client part installer (Linux/Mac)")

Linux: The remote computer(s) must have an OpenSSH server installed and configured beforehand, and you must also know the administrator's password on the remote PCs or have an SSH-key.

The **"Download Client"** tab offers to download the client part for the required OS.
Note: for **MacOS** only manual (local) installation is possible.

The **"Linux: installation via script"** tab offers to download the **deploy_client.sh** script for remote installation via the command line.
First, you need to add the file attribute to allow execution **(chmod +x deploy_client.sh)** and then run the script with the **--help** parameter to get help on how to use it.
This script can be used independently in any automation processes.

At the **"Linux: web-installation"** tab, you can install client remotely on a group of computers via an intuitive interface.
Attention! Remote installation at this tab will only work if the complex server is installed on **Linux** OS!

Let's take a closer look at the interface elements:

Upload client installation package
You need to attach the downloaded client package file for installation/update on remote client machines.
If you do not attach it, then the script will only update the address of the server of the complex without installing/updating the client itself.

IP-addresses/ranges/DNS-names of client machines
You have to specify a list of remote machines to install.
Attention! Each entry must start on a new line!
The entry can be:
- DNS-name: pc-001.domain.local
- IPv4-address: 192.168.0.10
- IPv6-address: [2001:0db8:85a3:0000:0000:8a2e:0370:7334]
- IPv4 range: 192.168.0.10-192.168.0.20
- IPv4 subnet: 192.168.1.0/24

ssh-port
TCP-port of SSH-server on remote machines.

Complex server (for clients connection)
Specify which server clients will connect to (DNS name/IP). Optionally, you can specify the port via a colon, and the secondary server via a comma.
String format: **primary[:port][,secondary[:port]]**
Attention! If the client is already installed, this parameter will also change server on the client to connect to!

Connection test
A simple TCP connection is made to the server for testing. It should also be noted that the connection is made from the machine where the web server is installed!

Administrator login on client machines
Specify the login of the superuser ("root") or administrator (with sudo rights) on whose behalf the package will be installed on the client.

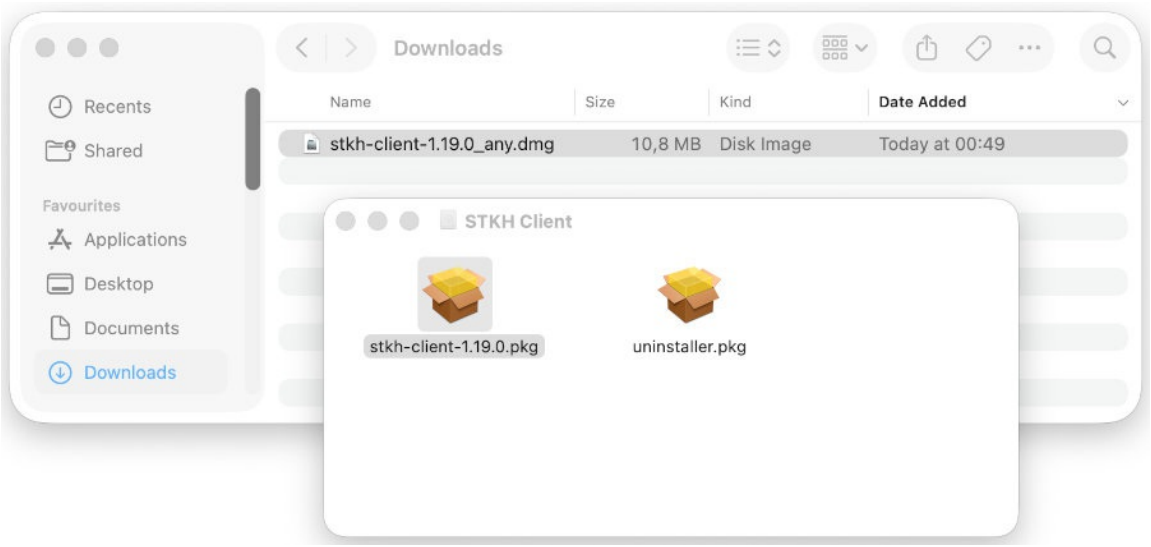
Administrator password or ssh-key
Specify one of them, depending on the ssh server settings on the clients.
Attention! ssh-key is supported only if administrator login is specified as "root"!

Max connection timeout (in seconds)
Wait for connection to remote machine no more than (seconds).

3.2.3.6.6. Installation on local computer (Mac)

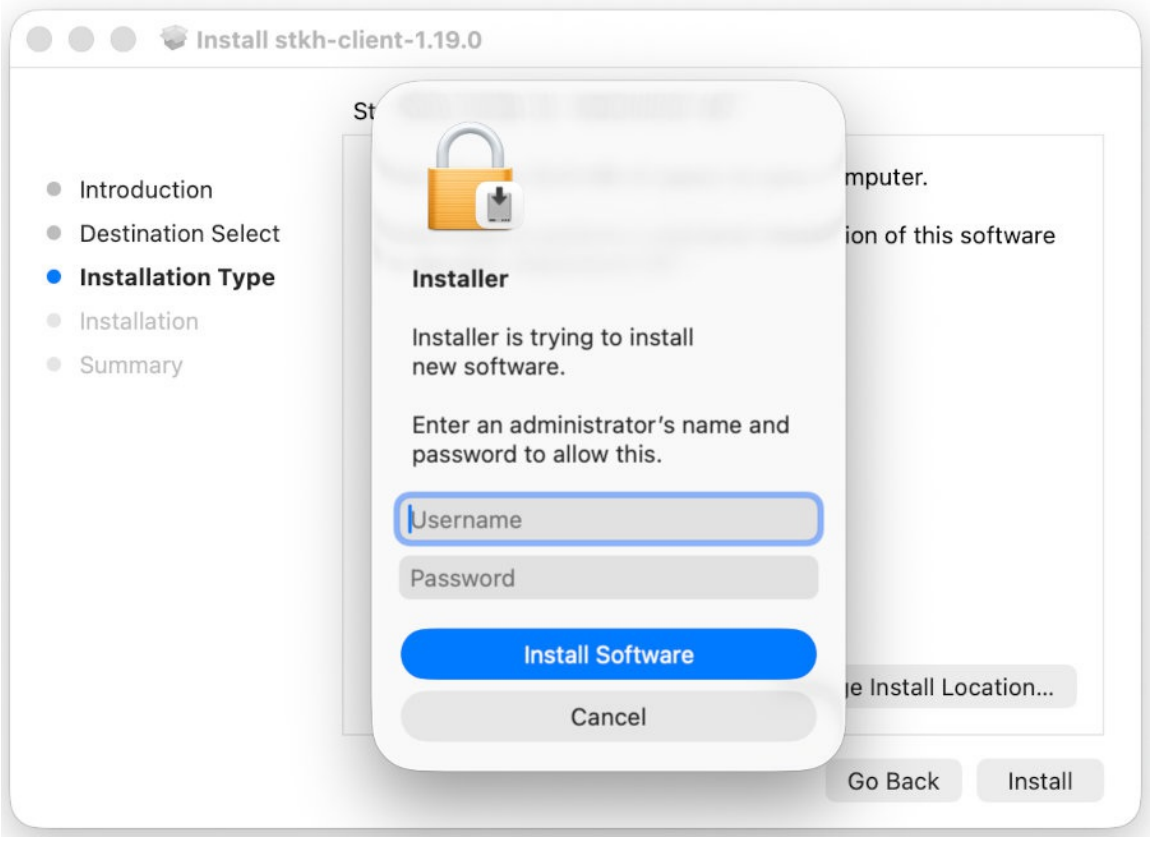
The installation package should be downloaded here.

After downloading, open the folder with the downloaded file in Finder:

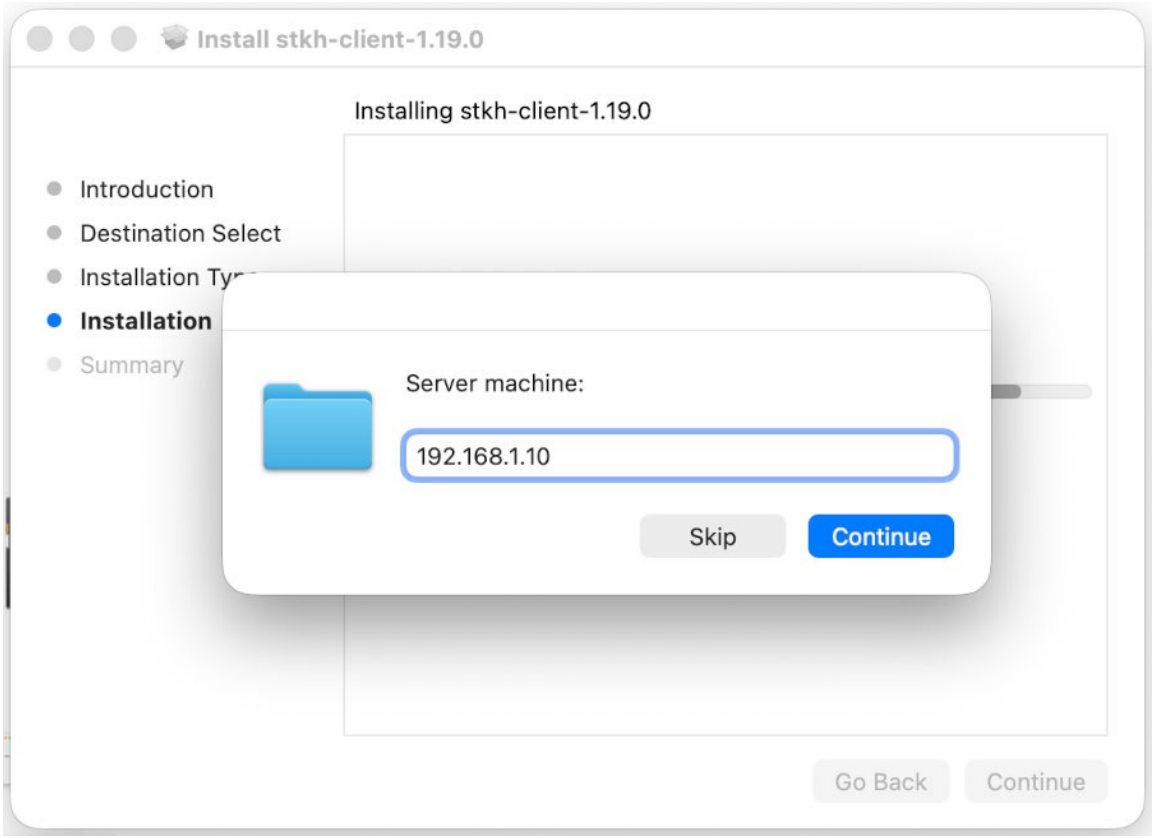


Attention! If the system issues a warning that the application is potentially dangerous and cannot be opened, you need to right-click on the .pkg file, then with the context menu open, hold down the "option" key and then click on the "Open" menu item.

To install, you need to know the **administrator name and password**!

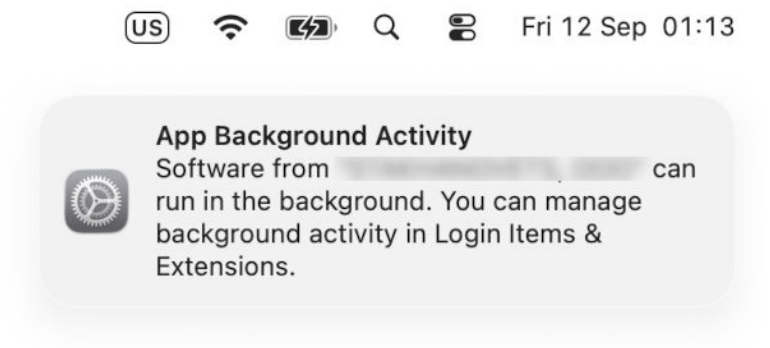


During installation, a dialog box will appear for entering the server machine address:

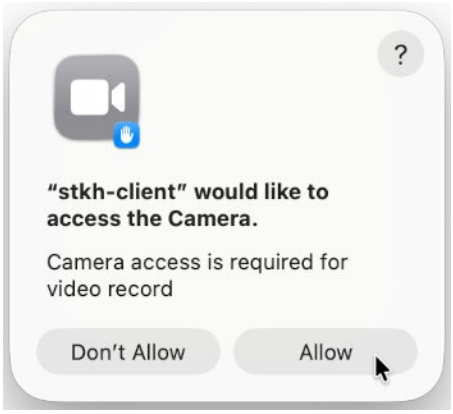


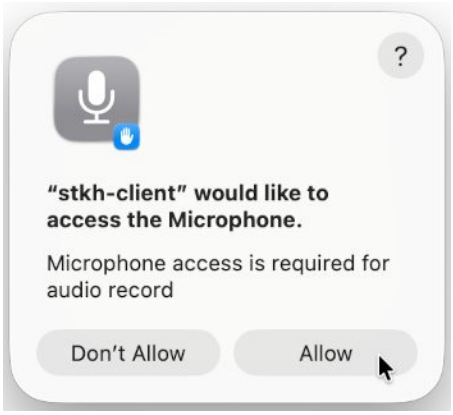
The options for filling this field and the rules for updating/deleting a client are completely identical to Windows-client.

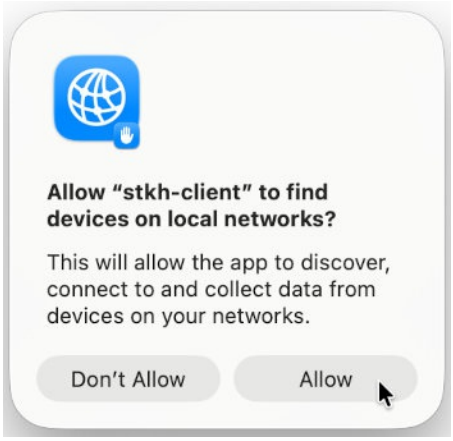
A message may appear in the notification area about adding the application to autorun:

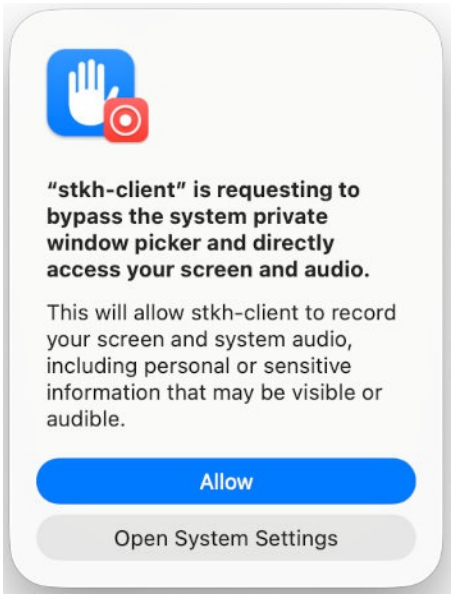


During the installation process and then during the first minute of normal program operation, the following requests for additional permissions may appear on the screen. You need to click "Allow" in each such window.
Such requests appear once per user.

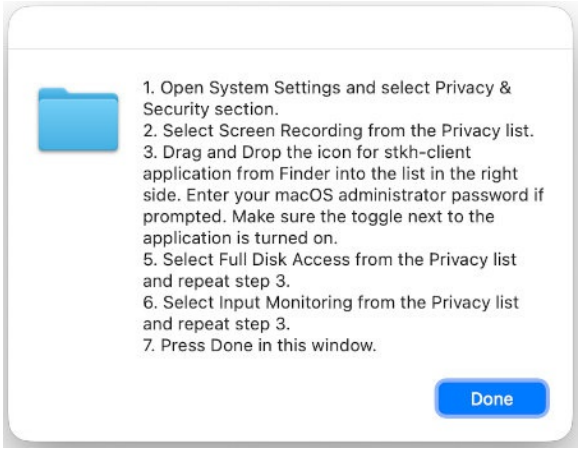




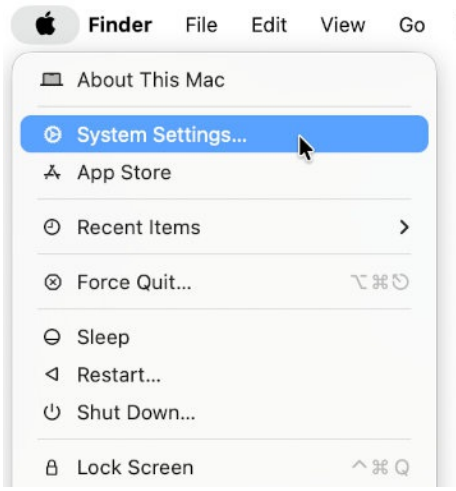




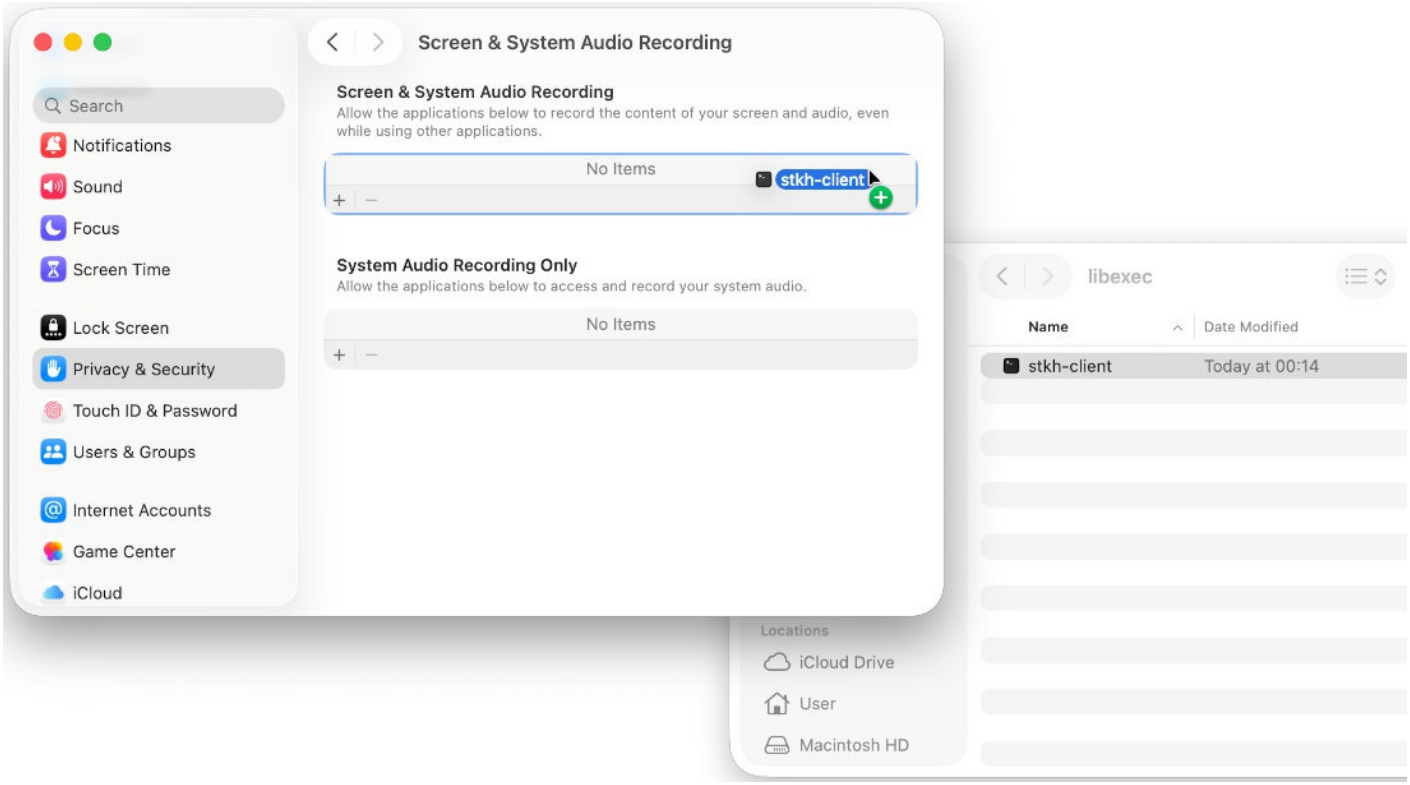
Next, a pop-up window displays brief instructions on what to do next.
Do not click "Done" button! (you can simply move the window to the side)



Click on the system menu in the upper-left corner of the screen, select "System Settings":

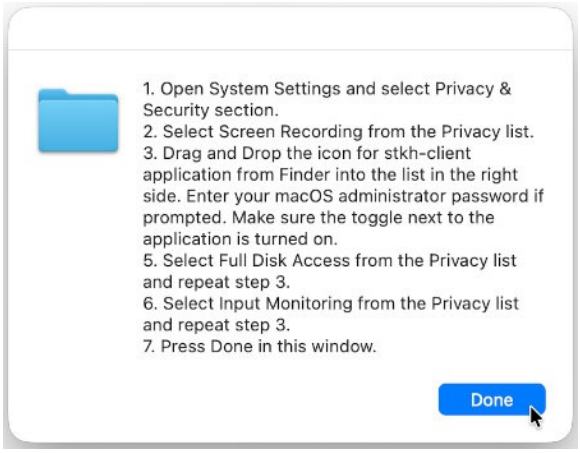


Next, in the window that appears, select a category "Privacy & Security → Screen & System Audio Recording" and drag file "/usr/local/libexec/stkh-client" to the applications list:

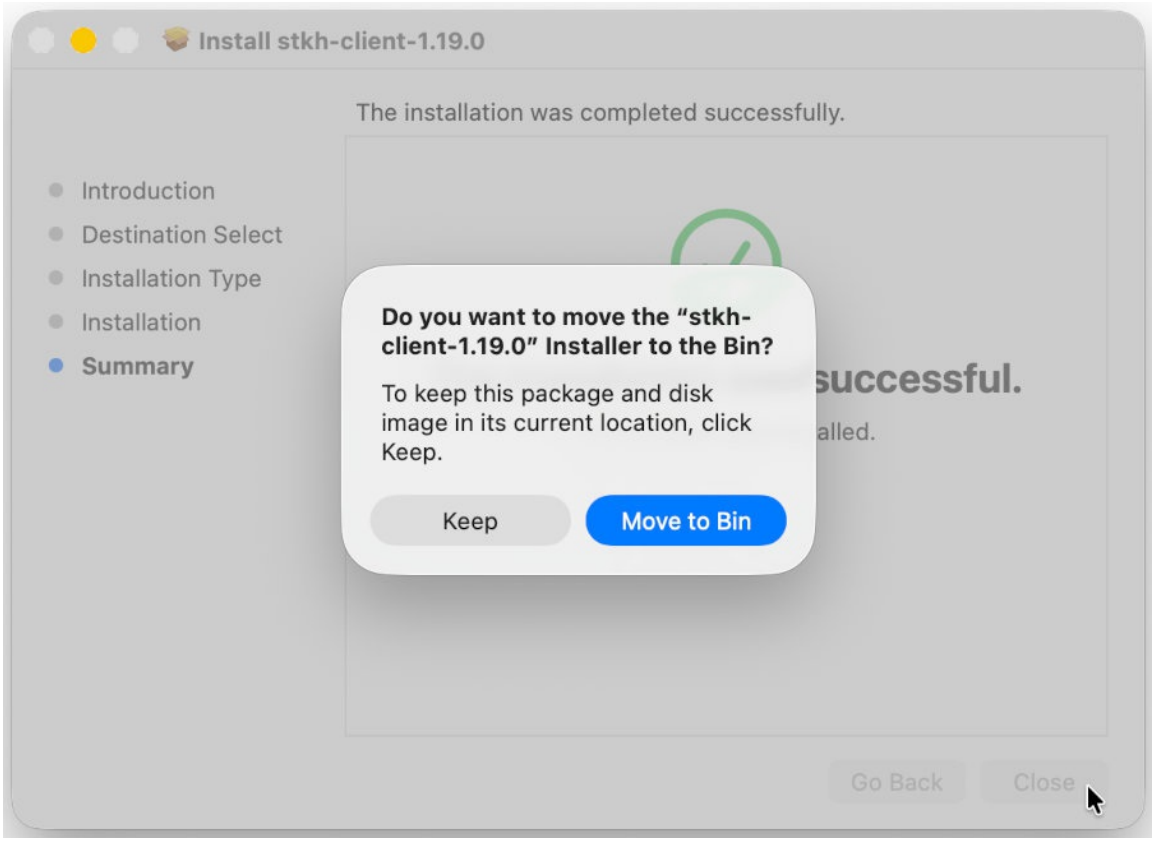


Similarly, do the same for the categories:
- **"Privacy & Security → Full Disk Access"**
- **"Privacy & Security → Input Monitoring"**

Then close the system settings window and click "Done" in the installer window:



Installation is complete! Click "Close". If the package is no longer needed, click "Move to Bin":



3.2.4. Common recommendations

It is recommended to perform installation **using the manual precisely**.

3.3. Linux server:

3.3.1. Installing the suite server

Documentation is not available in the current version!

3.3.2. Installing the administrator software

Documentation is not available in the current version!

3.3.3. Installing the client part

Documentation is not available in the current version!

3.4. Access to web-interface

Web interface of the complex consists of two parts: **"BOSS-Online"** and **"BOSS-Offline"**. The first part is intended to monitor online users and workstations in a real time as well as to perform a set of administrator's tasks.
The second part is for the viewing reports from SQL database.

"BOSS-Online" and **"BOSS-Offline"** are presented as web interfaces, e.g. it is not required to install additional software for monitoring and reports reviewing. It is enough to run any browser from any computer in the network and visit certain web site (see above).

Use any web browser on any workstation and put the following in the address bar:
http(s)://<DNS_name_or_IP_server>/scopd
Example:
https://localhost/scopd (**if the Scopd server is on the same workstation**)
http://server/scopd
http://mycompany.org/scopd
https://95.135.21.16/scopd

If server instance is different from instance by default then use the path **/scopd.X** where **X** is an instance number.
Example:
http://remoteserver/scopd.2 (connection to server instance number 2)

If non standard web server port is used (do not mess it with Scopd server port!), it is necessary to specify after colon.
Example:
http://myserver:81/scopd (connection to **port 81**, but not standard 80)

Attention! It is necessary to put IP address, not server name on some mobile devices (smartphones).

How to configure **remote monitoring via Internet** see here
How to configure the access via **https:** see here

Let's have a closer look at **"BOSS-Online"**.
After **"BOSS-Online"** startup it will be suggested to enter the database for manager.
In 1-2 seconds you will get a list with active workstations from the server (in case of succesful connection with server and active workstations in the network).
Active workstation means a workstation with installed client app on it.
It is important to differentiate "user" and "computer":
Computers in the list are computers with installed clients parts;
Users in the list are logged in Windows users.
As a result it is possible to have several users on a single computer (for example, in case of **terminal server** or **FastUserSwitch** mode)
So, commands for users and computers will differ. For example, you can update clients software **on the computer** but request **user's** screenshot only!
Computers and users, that are offline now or there is no connection with them (but was connected before) will be shown **in red color in the corresponded tab**.

Now let's have a closer look at **"BOSS-Offline"**.
"BOSS-Offline" is intended for reports viewing from the database. The program don't require workstations to be online currently. Moreover it is possible to see reports data **remotely** (for example from home) if technically it is allowed by network infrastructure and is properly set by the network administrator.

Please note, that data is written into the database **with delays** (about 10 min). So it will not appear immediately after the software installation.

3.5. Key activation

When installing the complex for the first time, as well as after receiving a new license key (for example, in the case of its expansion), it is necessary to activate the key.

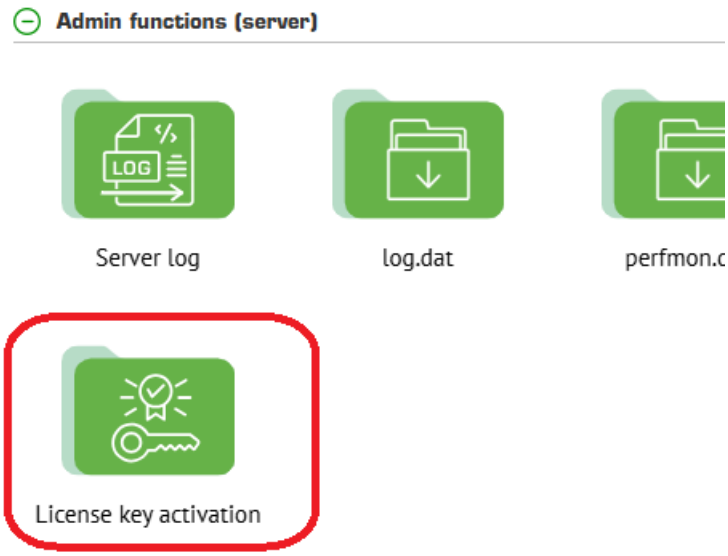
Attention! The BOSS-Online user must be granted rights to activate keys at this page (name of right: **"Allow licenses key tasks in BOSS-Online"**).

If server of the complex has access to the Internet (TCP port 443), then it is easier to use your **online-key** for activation.

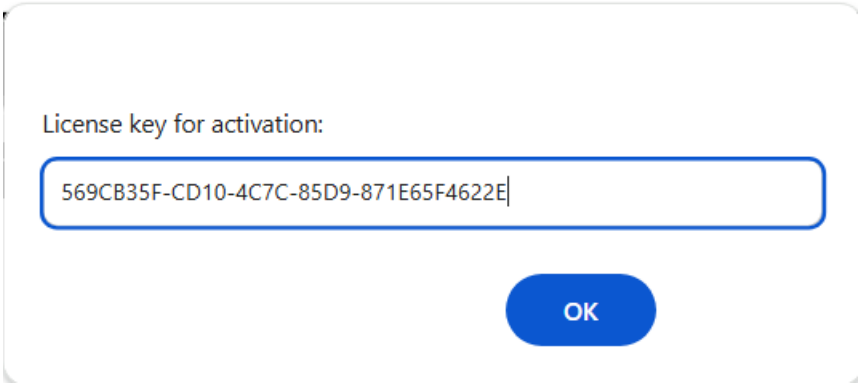
If there is no Internet access, then to activate you have to first obtain an **offline-key**. To do this, submit to the **technical support team** special identifier **HWID** (accessible via the BOSS-Online menu "Admin functions (server)" - "License information") and your **online-key**, after that you will be replied with an **offline-key**.

Procedure:

Login to BOSS-Online and click on "License key activation" button:

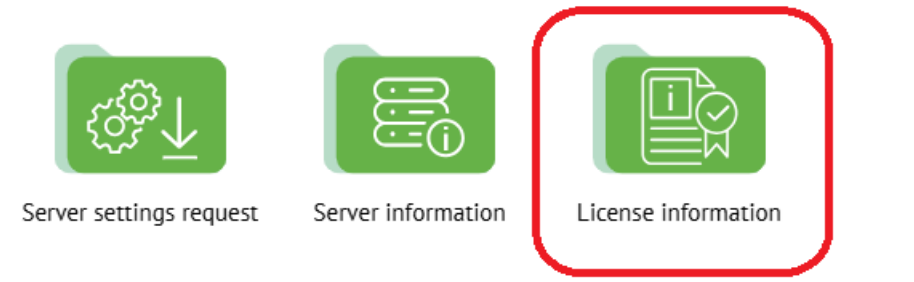


Next you need to paste **online- or offline-** key:



Result:

Wait 30-60 seconds for the server to accept the license and check the current information about the installed key:


Server settings request
Server information
License information

4. Software suite uninstall:

4.1. Suite uninstall

Unistall must be performed **in reversed order** of installation.

1. Perform uninstall of all clients' apps via **"BOSS-Online"** (see also).
2. Delete administrator's app on administrator's computer (on Linux execute **sudo apt remove stkh-admin**).
3. Delete the Scopd server suite in the same way (on Linux execute **sudo apt remove stkh-server**).

It is worth mentioning that all settings **are kept** even after uninstall.
That is also concerns Scopd **database**.
It is possible to delete SQL server as well, but the database file itself will remain. Later it can be connected to the database again. It is possible to delete it manually.

5. Software suite update:

5.1. Suite update (server on Windows)

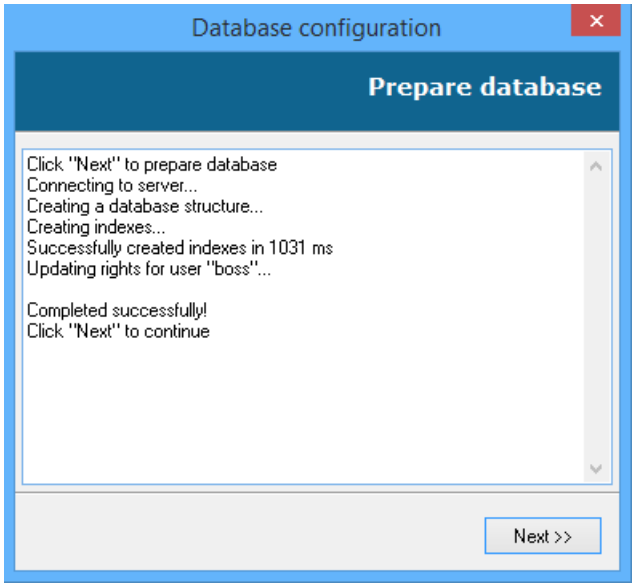
Administrator's app and **server** update must be done **manually** (e.g. to install new version over existing one) although it is necessary to use the update via **"BOSS-Online"** for **clients' workstations** or clients' automatic update option.

Sequence of steps:

1. Download the latest installation package from the website (**do not use "one click" installation!**)

2. It is recommended to stop software suite server. This can be done thru the Start Menu->Programs->Scopd Server->"Stop server" (command execution should be made within administrator's account only!).

3. Install **administrator's** app installation over existing version.
It is forbidden to stop database configuration utility execution at startup which is run automatically in the installation process.
To configure the database, you should use an account with **database administrator rights**.
For MS SQL this can be:
- user "sa";
- a Windows account with database administrator rights;
- leave the username/password fields blank to use the current Windows account (if you installed SQL Server using it).
For PostgreSQL:
- user "postgres";
- any other database user with database administrator/superuser rights.
The "boss" user cannot be used!



4. Execute installation package again and select **server installation**, then install it over existing version.
Attention! If a new version of the complex includes a newer version of the built-in Apache Web Server, then to update it (this is optional), you have to first perform **uninstall** of the complex server, but also need to first save your SSL-certificate files and possibly httpd.conf (if changes were made in it manually).

5. Update all **clients workstations via "BOSS-Online"** with the command **"Update client software"**.
If an option clients' **automatic update** is enabled (**it is enabled** by default) then this function will run automatically in 1 or 2 hours. Activation of client's new version will happen only after client's workstation **restart**!
It is possible to check current version of the client's app via BOSS-Online **"General information"**.

5.2. Suite update (server on Linux)

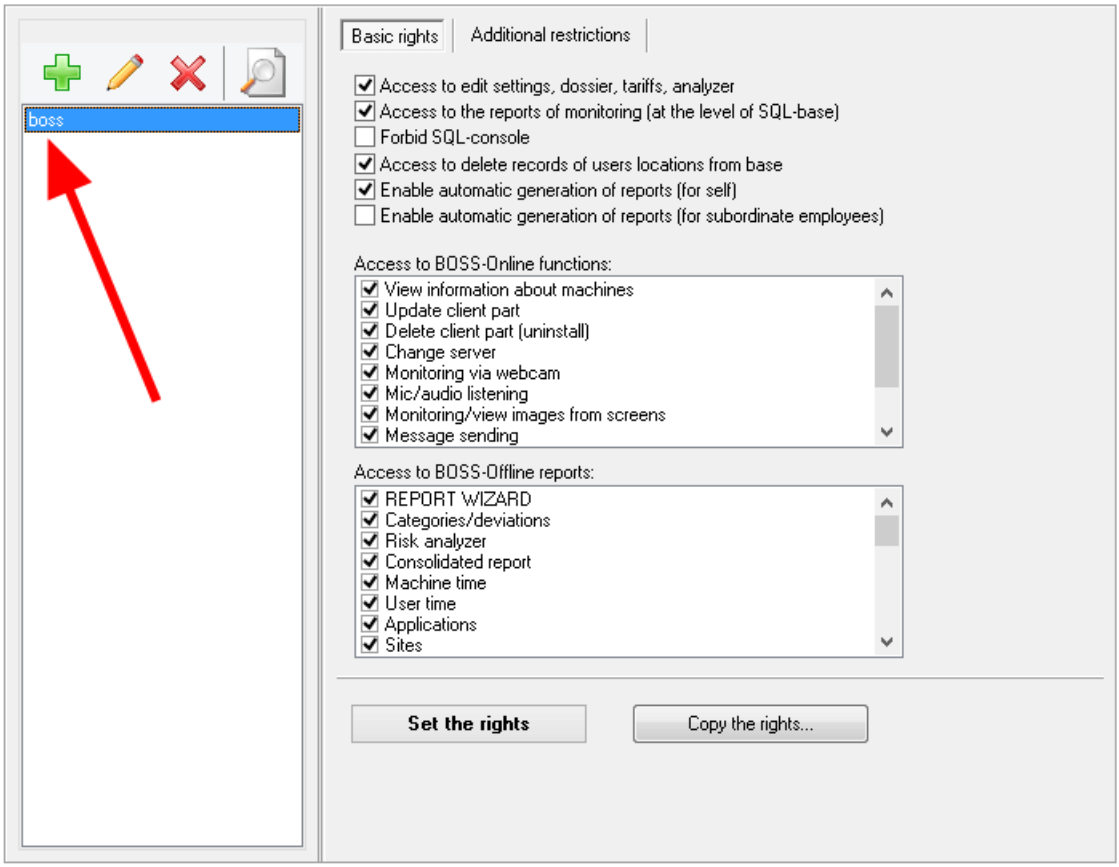
Documentation is not available in the current version!

6. Global settings:

6.1. Database users

On this page it is possible to add managers (**at least one is obligatory!**) as well as additional administrators (if required). They differ from each other only in permission rights. Permission rights may be added or changed only from **database administrator's account!**
Adding means creation of a new user **in the SQL database** and delegating rights to it.
Important warning: if a certain user has already been in SQL base and it is necessary to allow it to work with the Scopd database, then **it is necessary** to add it here on this page as **it is not enough** for this user to be available in the SQL database for fully functional work!
For **MSSQL/PostgreSQL** it is also possible to add **AD accounts** - specify the user in the format **DOMAIN\username** (abbreviated domain without a dot - NETBIOS). **Case matters for PostgreSQL! (see also LDAP for PostgreSQL)**
Managers created here and additional administrators also may enter into global setting app. They won't be able to add/delete users and set their rights. Only the database administrators is capable to do it!

Example how to create the manager "boss":



The most important options in the manager's rights:

Access to delete records of users locations from the database
To allow or forbid the access to the page "List of users".

Enable automatic reports generation (for self)
It allows automatic reports generation about employees with a function to send reports to yourself (or saving them to the folder).
More details you can find in the information about server configuration "Reports generator".

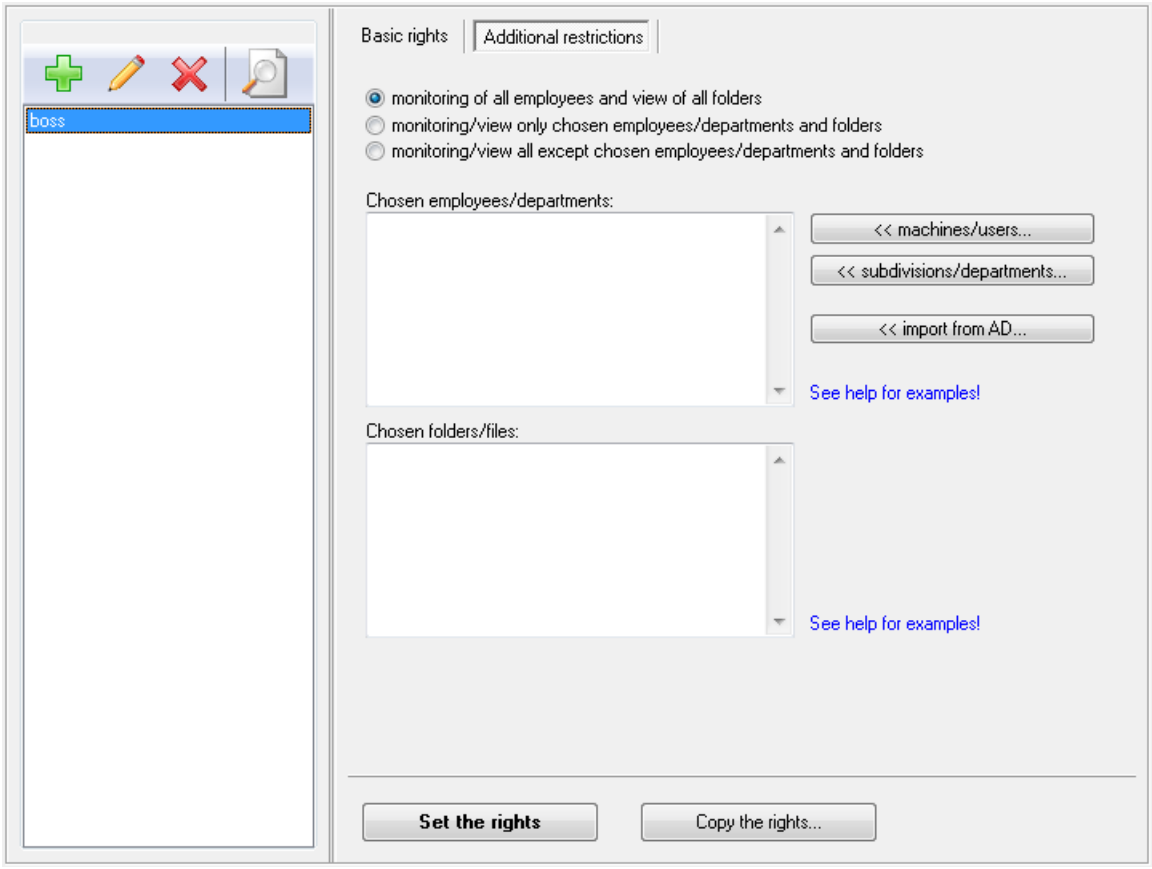
Enable automatic reports generation (for subordinates)
It allows report auto generation about each subordinate with report sending to the subordinates themselves.
More details you can find in the information about server configuration "Reports generator".

Allow commands to server from the Telegram messenger
Allows to send remote commands to the server via the Telegram messenger. For details see here

Allow confirmation/deletion faces of employees at the BOSS-Offline report
Used in face recognition report of BOSS-Offline.

Disable 2FA
See details here

Separately see "Additional restrictions" in the section right assignment for database users:



By default database new user can monitor in the online/offline mode all employees/departments and view all folders via BOSS-Offline. Although it will be useful to specify certain employees or departments for monitoring for each database user (manager). In such case it is possible to choose these departments (and employees if required) as well as folders.

It is possible to use the button "machines/users" (this list will be empty till first monitoring data from employees won't be transmitted to DB) **to choose employees**, add them manually or import from the Active Directory (see also here).
Use the button "subdivisions/departments" **to choose departments** (company structure is created in correspondent global settings part).
Note: rights for department are distributed also recursively to all its subsidiary departments.
Note: root department (company name) is not specified in the department hierarchical path.
Note: if department is added there is no point to add all users/computers inside it separately.
Each data entry must start with **new line**!
Data entry format for computer: **COMPUTER.DOMAIN** (for organizations with domain) or **COMPUTER.WORKGROUP** (for organizations with workgroups).
Important! The domain must be specified in the **full format**!
Important! If there is no domain and DNS suffix connection is used then it must be specified. In the common case computers must be designated like they are shown in the lists of computers in BOSS-Offline.
Data entry for users: **DOMAIN\USER** (for domain user) or **COMPUTER\USER** (for local users).
Important! The domain must be specified **in the short format (without dot)**!

It is enough to specify path fragment to the file (each fragment with a new line) in order **to choose permitted folders/files**.
It is forbidden to use masks "*" and "?"! It is necessary to omit certain path part instead of masks.
Fragments examples:
_PC1\PC1_Smith\
\Department1_
If full path to the file comprises at least one fragment from this list while reviewing files via BOSS-Offline this file will be reflected in the report.

It is necessary to press button **"Set the rights"** after rights configuration.

You can also use the **"Copy the rights"** option if needed to quickly copy the rights of one user and apply them to the currently selected user. After clicking on the button, a drop-down menu will appear with a list of all users, then one should be selected to copy the rights from.

6.2. Software suite settings:

6.2.1. General settings description

All software suite settings are divided into **server** and **clients'**.
Server settings are used by the server itself.
Clients' settings are used by the clients' computers and users. They receive these settings from the server with the start up and during computer work time. If the connection with the server is temporarily unavailable then previous settings will be used that are stored in the local cache of the clients' computers.
Settings changes will come into force in 1-3 minutes.
It is possible to find out which settings are used in the present moment via **BOSS-Online "General information"** function.

Client's settings are also divided into: **"for computers"**, **"for users"** and **"groups"**.
For computers - settings used by computers but not users! In such case it is possible for several users to work on one computer (simultaneously as in terminal server or alternately).
For users - settings used by certain computer's users but not computers itself.
To understand this difference one can look into the settings itself and see how they differ.
It is required to use **groups** if you **don't want** clients' settings **will be the same** for all computers/users. In such case it is required to create settings profiles and then link groups with these profiles. To create profile it is needed to click on **drop down menu** near the buttons "For computers", "For users".
Attention! If in your case settings for all computers and users **the same** there is **no need** to create profiles and groups!
Profiles - here you can assign friendly display name for each profile.

6.2.2. Server settings:

6.2.2.1. Common settings

The most important options in this tab:

Store reports no more then N-days
Indicate users' reports retrospective saving to the database and to folders (incl. shadowcopy folder). Do not indicate too big value in order not to occupy to much space on SQL server and the disk.
If you specify 0, cleaning will not be performed!

Store journal no more then N-days
The same option for Journal.

Daily database optimization
Optimization refers to the process of deleting old records from the database in acc. with prev. retrospective option.
It is recommended to perform during off-hours the minimum load on the database.
For the multi-server mode (several servers connected to one database), only the server that is selected as the main one will perform optimization (see server settings).

Reindex base
The re-indexing operation is optional and can improve database query performance.
Otherwise, the features of this option are similar to the previous one.

Keep reports for user _LOGOFF_ (logged off session state)
If checked it will be possible to see the user with the name **_LOGOFF_** in BOSS-Online.

Optimization: ignore computer name for domain users (at DB-level)
It makes sense to turn on this option in large companies where domain users can work on different computers. In this case, the list of users in BOSS-Offline can be very large and this will adversely affect the performance when building reports. With this option computer name for each user in the list will be replaced by **_ANYPC_**, this will reduce their total count.
After enabling the option, the old entries (with real computer names) in BOSS-Offline will remain and will be gradually deleted in accordance to the retrospective of reports storage. Enabling this option entails changing the data in the DB table (TUserLocations), unlike the second optimization option (see below).

Optimization: ignore computer name (only in BOSS-Offline)
The option is similar to the previous one, but with the difference that the changes will be visible immediately and only in BOSS-Offline, and in the DB the records and the size of the user location table (TUserLocations) will not change! Thus, enabling two optimization options at the same time makes no sense.

Traffic limitation
Warning! Use small values with great caution!
Set 0 to cancel restrictions.

Storage on clients
If **any of the three** options is enabled and the corresponding problem occurs, then the clients will be notified by the server about the occurrence of such an event and will stop transmitting the intercepted monitoring data to the server. In this case, no data separation is performed. For example, if only the shadow copy folder is unavailable and the sensitivity is set to this event, but the monitoring data does not contain shadow copies, then they will still not be transferred to the server! Conversely, if only the database is unavailable, then even shadow copies will not be transferred.
The data on the clients is stored in this case as standard in the local storage.
This status is polled by clients approximately once per minute.
If the options are not used, then all data will be transmitted to the server even if there are problems, and in this case:
- if the shadow copy folders are unavailable, the transferred shadow copies will be destroyed by the server;
- if the database is unavailable, the packets will be delayed in the server's RAM (and after it is full, data is no longer accepted from clients at the TCP protocol level).
Attention! When disabling use of the ShadowCopy folder, it is considered that this folder is unavailable, so in this case you need to disable "storage on clients" option to allow monitoring data be transmitted to the server!

Max. number of attempts to enter an incorrect password
If you specify a non-zero number, and the number of consecutive failed login attempts to the BOSS web console equals this number, the account will be blocked during N-minutes (next parameter)!
If the block duration is set to zero, only the administrator can unlock it by resetting the password on the "Database Users" page (for SQL accounts) or by deleting/creating an account (for accounts from the Active Directory).

6.2.2.2. Postponed monitoring

It makes sense to use **Postponed monitoring** to save client-server network traffic, as well as to reduce the load on the complex server and the database at great number of client connections to the server.
If this mode is active for **computer** or **user** the monitoring data are accumulated locally on the client machines and are not submitted to the server if the reports on the given computer/user were not built for more than N-hours (**"Keep history of reports building"** parameter). In fact, this is the maximum time that the BOSS-Offline operator can wait for all postponed data to arrive after the report is built. Do not specify too big value for the parameter, as increased load on network resources. Usually a value of more than 6-8 hours does not make sense.
It should be noted that postponed monitoring data is transmitted to the server only within the time period for which report was built!
It also does not matter which PC the user worked on - building a user report for any PC initiates the transfer of postponed monitoring data from all PCs where this user worked in the specified time intervals.
Disabling postponed mode does not automatically send postponed data to the server!
Thus the users "not interesting" for the monitoring at the present moment will not load the network and the database with their data (retrospective of the local storage on the machines and other options are set on the Computer Settings tab **"Local storage"**).
Should the report be built by the user being in the postponed mode of operation, then naturally there will be no data in the database and the report will be blank. Though 1-2 minutes later the transmission of the accumulated data will be started to the server until all the data are transmitted.
The current size of the machine local storage can be viewed with the BOSS-Online function **"General information"**. Also it is possible to delete the local storage or stop transfer of postponed datas from BOSS-Online.

Limitations for building reports in BOSS-Offline
There may be situations where operators through BOSS-Offline will massively generate reports on a large number of users for large periods of time, as result the load on the network and database will increase significantly when transferring pending data from clients to server, as there can be a lot of data!
To prevent this, you can set a limit for one report request and/or for total pending requests made within last N-hours (**"Keep history of reports building"** parameter) by one or several operators.
Value calculated as **count of users/computers multiplied by count of days for report depth**.
For example, when value 30 is specified, it will mean that you can build a report:
- for one user within 30 days interval;
- for three users within 10 days interval;
- for 30 users for 1 day interval;
and so on....
When **0** is set, there will be no restrictions.
If the limit exceeded, **an error** will be generated for the operator when building report.

6.2.2.3. Monitoring - Screenshots

The most important options in this tab:

To save shots in the folder
Specify the folder on the server where shots will be saved.
Attention! Do not specify root folder here (such as C:\, D:\ and etc.)
This option exists mainly for backward compatibility with software suite versions 3.xx.
Sometimes it can be useful to look through users' screen shots not via BOSS-Offline but directly from the server folder with a breakdown by users. In such case it is required to enable this option. At the same time it is necessary to enable shadow copy as it is important for screenshots review through reports.
It is also important for the option to allow this saving in the tab "Monitoring: Screenshots" in the clients settings.

If the hierarchy is set up for organization then corresponding hierarchy part will be added to the path in the folder.

File format
Specify how saved shots will be grouped: by computer's name, users, date and etc.
One must indicate the relative path inside the server folder in this line (see above option) using variable in the following way %variable%.
File name with extension .jpg should be added at the end of this path.
Acceptable variables:
%COMPLOC% - domain, DNS suffix or workgroup where computer is joined
%COMPNAME% - computer's name
%USERDOMAIN% - user's domain (in a short format)
%USERNAME% - user's name
%DATE% - shot's data in the format yyyy-mm-dd
%TIME% - shot's time in the format hh_mm_ss
%TIMEMS% - shot's time in the format hh_mm_ss_msec
So it is possible to group shots in many ways that will be convenient for review from server folder.

Take on disk not more than N megabytes
Specify maximum size for server folder with shots.
If "0" is indicated the folder won't be cleared.

See also clients settings tab "Monitoring: Screenshots"

6.2.2.4. Monitoring - Webcams

The most important options in this tab:

Saving shots in the folder
Specify the folder on the server where shots will be stored.
Attention! Do not specify root folder here (such as C:\, D:\ etc.)

Note: If hierarchy is set up for organization then the corresponding hierarchy part will be added to the path in the folder.

File format
Indicate how saved shots will be grouped: by computer's name, date etc.
In this line it is required to indicate the relative pathname inside the server folder (see above option) using variable which has view as %variable%.
The file name must be with extension .jpg at the end of this path.
Acceptable variables:
%COMPLOC% - domain, DNS suffix or workgroup
%COMPNAME% - computer's name
%DATE% - shot's data in the following format yyyy-mm-dd
%TIME% - shot's time in the format hh_mm_ss
So it is possible to group shots for convenient review from the server folder.

Take on disk not more than N megabytes
Specify maximum size for the server folder with shots.
If 0 is indicated then the folder won't be cleared.

See also clients settings tab "Monitoring: Webcams"

6.2.2.5. Monitoring - Autorecording

The most important options in this tab:

Save audios in the folder
Specify the folder on the server where audios will be stored.
Attention! Do not specify root directory here (such as C:\, D:\ etc.)

Note: If hierarchy is set up for organization then corresponding hierarchy part will be added to the path in the folder.

File format
Specify how saved audios will be grouped: by computer's name, date etc.
It is necessary to specify the relative path inside the server folder (see above option) using variable such as %variable%.
The file name must have extension .ogg at the end of this path.
Acceptable variables:
%COMPLOC% - domain, DNS syffix or workgroup where computer is joined
%COMPNAME% - computer's name
%USERDOMAIN% - user's domain (in a short format)
%USERNAME% - user's name
%DATE% - date of audio initiation in the following format yyyy-mm-dd
%TIME% - time of audio initiation in the following format hh_mm_ss

Take on disk not more than
Specify maximum size for the server folder with audios.
If 0 is indicated then the folder won't be cleared.

Save audio in the BOSS-Offline report
It is also necessary that **Shadow copy** is enabled in the server settings!

See also clients' setting "Monitoring: Autorecording"

6.2.2.6. Monitoring - Printing

By default intercepted printed files are saved as shadow files for viewing through a report in BOSS-Offline, however, it is possible to duplicate these files to a folder on the server.

Duplicate print files to folder
Specify the folder on the server where files will be stored.
Attention! Do not specify root directory here (such as C:\, D:\ etc.)

Note: If hierarchy is set up for organization then corresponding hierarchy part will be added to the path in the folder.

Folder format
Specify how saved files will be grouped: by computer's name, date etc.
It is necessary to specify the relative path inside the server folder (see above option) using variable such as %variable%.
Acceptable variables:
%COMPLOC% - domain, DNS syffix or workgroup where computer is joined
%COMPNAME% - computer's name
%USERDOMAIN% - user's domain (in a short format)
%USERNAME% - user's name
%DATE% - date in the following format yyyy-mm-dd
%TIME% - time in the following format hh_mm_ss

Take on disk not more than
Specify maximum size for the server folder with files.
If 0 is indicated then the folder won't be cleared.

Do not save
Specify the masks of files separated by commas that do not need to be saved to the folder.

See also clients' setting "Monitoring: Printing"

6.2.2.7. Monitoring - Shadow copy

The most important options in this tab:

The folder to save files
Specify a folder (accessible from the server) to save the shadow copy files. The use of **server PC environment variables** is allowed.
It is makes sense to use **Environment variables on the server PC** in multi-server mode (several servers connect to one database) and the case where the shadow copy folders for each server must be different. Those you can set a single setting here (for example, %SC_FOLDER%\shadowcopy), and set the %SC_FOLDER% variable to the desired value on each server PC. Thus, this setting will be the same in the database of the complex, and the folders can be different for all servers!
Note: for Windows root folders like C:\, D:\, ... not supported!
Attention! When disabling this option, you have to also disable the option **storing data on clients when the ShadowCopy folder is unavailable**, otherwise the monitoring data will accumulate on the clients and will not reach the server!

Secondary (backup) folder
You can specify a second folder where files will be saved if the main folder is not available. The rules for cleaning both folders are identical.

Important note when using network paths. If access to the file server requires the rights of a separate account, then you need to change the method of starting the complex server service (StkhServer) by specifying "Run as ..." in the service properties. However, for the correct operation of the complex in this case, it is also necessary:
1) the Apache Web Server service (ApacheHttpdSvc) also run under this account;
2) make sure the account has write access to the folder %ProgramData% (usually C:\ProgramData);
3) make sure the account has write permissions to the registry branch HKLM\SOFTWARE\WOW6432Node\StkhServer

Take on disk not more than
It is possible to limit maximum folder size (in ₽B). If 0 is indicated the folder won't be cleared.

Keep on disk at least
Additional option to clean up the shadow copy folder if free disk space is less than the specified number in MB.
This option is useful in a multi-server architecture, when each server has a different disk size. In this case, you can set the option "Take on disk not more than" to 0 and use this option.

See also clients' settings tab "Monitoring: Shadow copy"

6.2.2.8. Monitoring - File hashes

When using **file hashes** in case content of some files can be changed sometimes or new files can be added, it is good idea to not use manual files addition at this page, but better to specify here folders or files list, from where server will periodically (one time per hour) update hashes. In this scenario removal of file hashes from the database does not occur, even if the original file was deleted!
In each new line of the list specify folder or file (masks are allowed).
Example:

```
c:\documents\*.doc
c:\other\
\\server\file\data.pdf
```

Warning! All paths must be accessible from server!

6.2.2.9. Monitoring - Users online

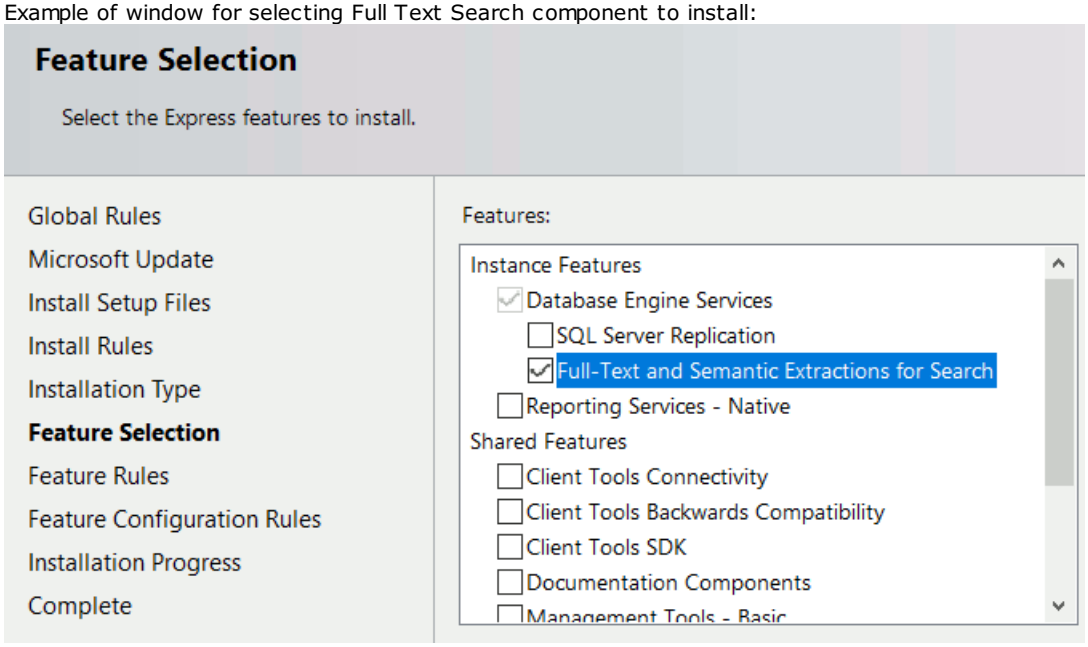
When this option is enabled, data for the "Users online" report will be transferred to the database (information about at what intervals users were connected to the server).
Attention! With a large number of users, enabling this option **increases the load** on the database!

6.2.2.10. Monitoring - Global search

On this page, you can enable data transfer to the database of the complex for the operation of the "Global search" report. In addition to enabling this report itself, you also need to include the types of data you need for your search.
You may also need to enable the option **"Transmit data for the "Global search" report when the active window changes"** on the settings page if you want to search by window title/site whenever the active window changes. The **"Additional screenshots when active window changes"** option on the Settings page may also be useful.

Attention! Enabling this report increases the load on the database, and also increases its size due to the formation large indexes and a large number of data!

Attention! **Fast indexed search** using **MS SQL Server** requires installation of the **Full Text Search** component. By default, it may not be installed, for example, in the Express version of SQL Server. You should download version with Advanced Services and install the component. After installing, you need to re-configure the database of the complex in the administrator part of the complex using the Database Configuration Wizard.
If the component is not installed, then only **slow non-indexed** search will be available!
Example of window for selecting Full Text Search component to install:



6.2.2.11. Monitoring - Chats-calls

ICAP TCP-port for eXpress DLPS incoming connections
Documentation for this option is not available in the current version!

ICAP TCP-port for TrueConf incoming connections
Documentation for this option is not available in the current version!

ICAP TCP-port for Dion incoming connections
Documentation for this option is not available in the current version!

6.2.2.12. Face recognition

Comparison sensitivity for events generation
The lower value: more likely that similar faces of different persons will be considered as the face of one person.
The higher value: more likely that faces of one person will be considered as faces of different persons.

Perform automatic system training
You can confirm that employee’s face matches the webcam image at the BOSS-Offline "Face Recognition" report, thus training the system. However, with a large number of employees, this task makes sense to automate by enabling this option.
Automatic training is based on the fact that an outsider spends time at the employee's computer much less than an employee.
Training will occur at the time specified for the option "Daily database optimization".

See also "Monitoring: Face recognition"

6.2.2.13. Text recognition (OCR)

On this page it is possible to choose the method and set up optical character recognition (OCR) features used in DLP-analysis and should be turned on at this page.

Built-in
Specify required languages, separated by commas: **aze** (Azer), **eng** (English), **kaz** (Kazakh), **rus** (Russian), **tur** (Turkish), **ukr** (Ukrainian), **uzb** (Uzbek).
Attention! Adding each new language to the list significantly **slows down** the recognition speed!
Maximum number of threads actually determines the speed of parallel processing of multiple requests to the server. If you specify 0, the number will be selected automatically. Specifying a value greater than the physical number of threads of the server CPU does not make sense. It is important to note that each thread at peak can take up to 100 MB of RAM!

Enable faces detection
You can enable this option as an addition to OCR to detect the presence of facial photos in documents or screenshots.
The option must be used simultaneously with adding the corresponding face template (FACE) on the page "DLP - Rules"
Enabling this option will slightly slow down the OCR process!

Attention! After changing the values on this settings page, it is recommended to **restart the server service** for the new settings to take effect!

6.2.2.14. Text classification

When you enable DLP document classification options on this page, documents will be transmitted to the server and classified according to the categories specified here.
The classification result can be viewed in the **"Files Classification"** report.
In the current version, classification is performed through LLM AI (settings are here).

Each category consists of a unique name (English letters only!) and a description.
It is advisable to use the word "probability" in the description.
If you need the "other" category, it is better to place it last in the list.

Condition for event formation
If a condition is specified, then when it is met, the corresponding DLP-event is recorded in the **"Events: user"** report. See events settings here.
The condition itself is a logical expression of comparisons of greater/less for category values (in percents), with the possible use of AND/OR operators, as well as parentheses.
For example, condition **(confidentiality >= 70) AND ((agreement >= 60) OR (statement >= 60))** means **"if the document's confidentiality more than 70% and at the same time one of two conditions (or both): the probability of an agreement is more than 60% or the probability of an statement is more than 60%"**.

6.2.2.15. Neural network server

In the current implementation, a neural network server is used to:
1) **Detection of photographing the computer screen by smartphone**: connection to the neural network server goes through the server of the complex.
2) **Speech to text translation**: connection to the neural network server goes directly from client machines.

Common description
The server should be downloaded from **downloads page**
It can be installed on **local**, or **remote** machine.
Supported OS: Ubuntu 22
Installation example:

```
sudo apt install ./stnnserver_2.02_amd64.deb
```

Data exchange with the neural network server is carried out using secure https-protocol.
The port for communication through a colon must be specified, because by default the neural network server is configured to port **27524**, and if no port is specified after a colon, then **443** will be used.
To change port in **Linux** edit next file **/etc/stnnserver/config** and then restart service: **sudo service stnnserver restart**

Detection of photographing the computer screen by smartphone
Client settings for this task are configured **here**.
Also, for detection, you need to have on the server machine (where the neural network server will be installed) **video-card GPU with CUDA support**. Also **NVidia drivers** must be installed for this card.
Current implementation uses CUDA 12.0, this version covers both old and newer video cards. Here https://en.wikipedia.org/wiki/CUDA#GPUs_supported you can find supported models. First column "Compute capability (version)" is from range 5.0 to 9.0.
More CUDA cores and more powerful GPU will result faster recognition cycles.
Estimate usage of VRAM - minimum 2GB, and RAM - near 2.5GB, CPU loading is minimal.

Speech to text translation
Client settings for this task are configured **here**.
GPU with CUDA is not required!
Attention! The connection test checks only the availability of the server, and not the voice recognition functionality itself!

Possible errors while testing the connection (common)
Timeout or error connecting to the complex server - it is impossible to connect to the server of the complex (the server of the complex is specified incorrectly, invalid port, Firewall blocking or the server is not running);
Server response timeout - failed to receive a response from the complex server within the maximum allotted time;
Config has not been read yet - the server of the complex did not read the settings from the database;
HTTP Error XXX - most likely the "server:port" of the neural network is incorrectly specified or the neural network server is not running;
Network error 12007/11001 - the DNS name of the neural network server is incorrect;
Network error 12029/10061 - error connecting to the neural network server (the neural network server is incorrectly specified, invalid port, the Firewall blocking or the neural network server is not running);
Network error 12002 - timeout for processing a request by the neural network server (large load);
Network error 12044 - client certificate error when connecting to the neural network server.

Possible errors while testing the connection (only the detection of photographing computer screen with smartphone - Objects detection)
Runtime exception: The detector is not initialized - no graphics card with CUDA support or acc. drivers not installed.

Note: example of installation NVidia drivers v550 on Linux Ubuntu:

```
sudo apt install linux-headers-generic linux-source
sudo apt install nvidia-headless-550-server
sudo apt install nvidia-utils-550-server
sudo reboot

nvidia-smi
```

6.2.2.16. LLM-server

Some BOSS-Offline reports use generative AI based on the LLM neural network, so to use them, you need to configure the settings at this page.

You can configure either a **local** server or a **cloud** server, or **both at the same time**.
If **both at the same time** are configured, the local server will take priority, except when neutral data (that does not contain confidential or personal information) is being transmitted.

For a local server Ollama framework is supported, and ChatGPT / YandexGPT for a cloud server.

Server URL
specify http or https URL of the server with Ollama installed
As usually, this is http 11434
Example:
http://192.168.0.111:11434

API-key
ChatGPT: you should create API-key and copy it here.
YandexGPT: you should create billing account here, and then obtain OAuth-token and copy it here.

Model
Ollama: specify the loaded model to use, currently, models from **qwen3** or **deepseek-r1** are recommended.
For example:
deepseek-r1:14b
deepseek-r1:32b
qwen3:14b
qwen3:32b
You need to specify the exact model that downloaded and installed in Ollama. Complete models list available on the Ollama website.
ChatGPT:
gpt-4o
o4-mini
gpt-4.1
gpt-4.1-mini
gpt-5
gpt-5-mini
and others
YandexGPT:
gpt://<folder_ID>/yandexgpt
gpt://<folder_ID>/yandexgpt/latest
gpt://<folder_ID>/yandexgpt-lite

Ollama:
- using a **GPU with CUDA support** is not required for operation, but is highly recommended, because the performance will be an order of magnitude higher even in comparison with multi-core CPU servers!
- **the model must fit completely** into the video memory or RAM;
- the larger the model, the better the quality, but the slower the speed;
- it is allowed to use several GPUs (if the video memory of one GPU is not enough to accommodate the entire model);
- when using GPU, CPU and RAM resources can be minimal (for example, 2 CPUs and 4 GB RAM are quite enough).

Example of installing Ollama on Linux Ubuntu (it is assumed that the GPU drivers are already installed):

```
curl -fsSL https://ollama.com/install.sh | sh
```

For non-localhost access and increasing the allowed model loading time, it is recommended to make additional settings:

```
sudo nano /etc/systemd/system/ollama.service
```

The following lines should be added to the **[Service]** section:

```
Environment="OLLAMA_HOST=0.0.0.0"
Environment="OLLAMA_LOAD_TIMEOUT=60m"
```

Then save the file and execute:

```
sudo systemctl daemon-reload
sudo systemctl restart ollama
```

Then you need to download and install the model. For example, **qwen3:32b**

```
ollama run qwen3:32b
```

6.2.2.17. Azure-integration

In current implementation Azure-integration is used for:
- **contacts synchronization for MS Teams**.

App
To integrate with Azure, you need to create an application and endow it with the appropriate rights:
1) Go to the portal.azure.com with administrator login.
2) Go to page "App registrations" https://go.microsoft.com/fwlink/?linkid=2083908
3) Click on the link "New registration", enter any App name and click "Register".
4) Copy the application parameters to this page of the complex settings: Application ID, Directory ID.
Example ID values: d376fb82-c3d7-487e-900f-26562cef13eb, 4404791d-2074-4418-9ece-fdad6fd354c1
5) On the left in the menu click on the item "Certificates & secrets".
6) Next click on "New client secret", enter its name and add, and then copy the secret value into the "Secret" field on this page of the complex settings.
Example of secret value: JAR1Gz4mS8wm-USP9W5.RduR0zYY8MsT.~
7) On the left in the menu click on the item "API permissions".
8) Click on "Add a permission", then in the list that appears on the right, select "Microsoft Graph", next - "Application permissions".
9) Then select from the list:
Chat.Read.All
Group.Read.All
User.Read.All
And click "Add permissions"
10) Click "Grant admin consent for ..."

Contacts synchronization for MS Teams
If you do not sync contacts for MS Teams, when intercepting MS Teams messages, the report may contain the IDs of the users instead of their real contacts (example: ccd931c5-6378-477c-973b-83e4c8c07cf7). Synchronization can be used to solve this problem. During synchronization, the server of the complex will send requests to the MS servers (**https://login.microsoftonline.com** and **https://graph.microsoft.com**) to get information about contacts and groups. Further, the received information is cached locally at the server machine.

Attention! If access to the Internet from the server is possible only through a **proxy**, then it must be set in the initial server settings (available through the START menu).

6.2.2.18. Webex-integration

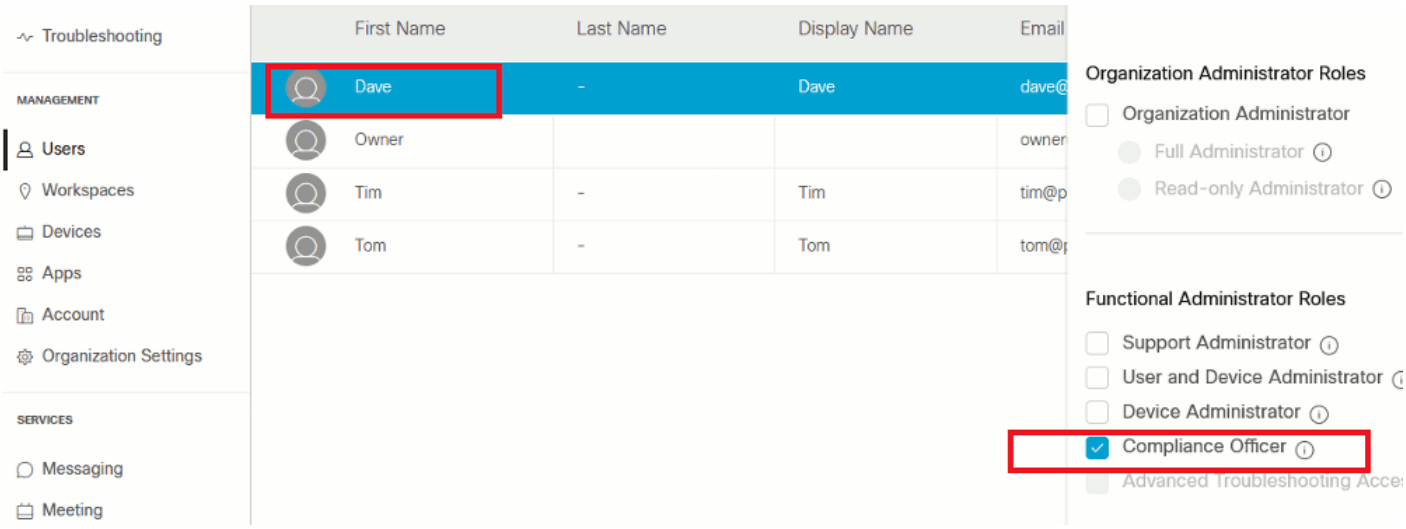
There is a possibility of periodic synchronization of messages sent by employees through **Cisco Webex Teams** with complex database (for report "Chats/Calls"). During synchronization, the complex server will read data from the Webex server (**https://webexapis.com**) periodically at a configurable interval (from 1 to 1440 minutes).
Note: this integration has nothing common with intercepting voice conversations and sent files!

To configure integration, you need:

1) Make sure that the complex server is installed and running. If you have several servers of the complex connected to the same database, then the integration will be performed only from the main server (set in the initial server settings).

2) For synchronization to work, it is necessary for employees to have an e-mail set in Webex accounts from the Active Directory (this usually always happens after synchronization AD and Webex). Comparison of the Webex user and the user in the complex will be done by e-mail (from report "E-mails" or "Dossier of employees").

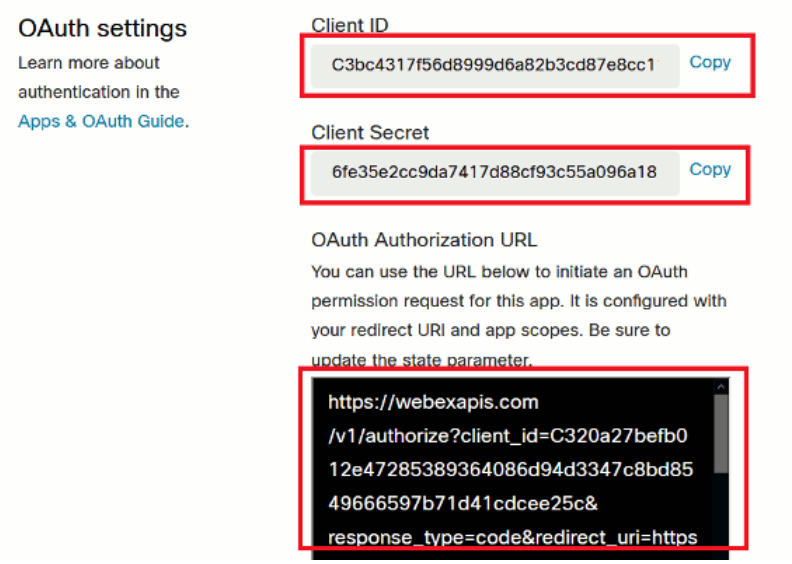
3) In the admin panel **admin.webex.com** under the administrator account must be assigned to one of the users role **"Compliance Officer"**. It can be any existing user or a newly created one. The role is assigned by clicking on the user's name and selecting on the right in the pop-up panel **"Administrator Roles"**.
Further, the integration will be performed with this user's account. Let's name this user **Compliance Officer**.



4) Log in to the portal **developer.webex.com** as **Compliance Officer** and create new integration: **developer.webex.com/my-apps/new/integration**

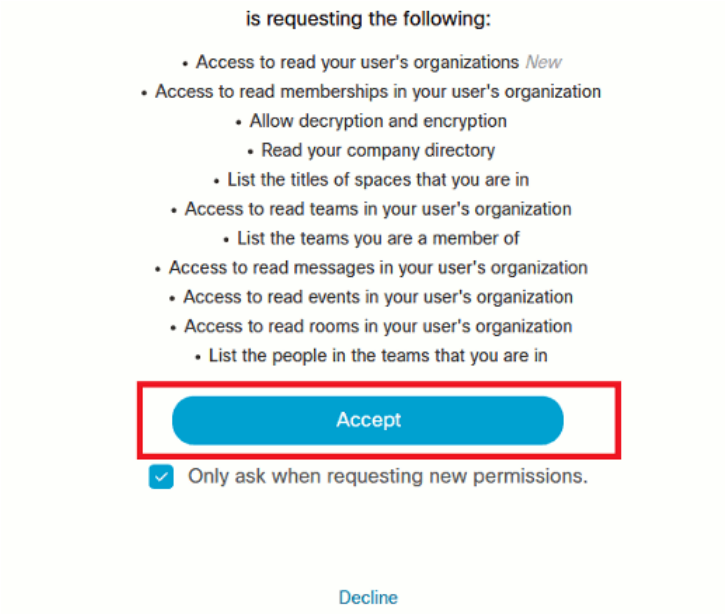
5) Then fill in the required fields arbitrarily: Integration name, Contact email, Icon, Description.
For the field **Redirect URI** specify: **https://IP_of_server_complex/scopd/cgi-bonline.exe?action=webex**
Please note, that only **https**-access to the web-server is allowed (set up here) and only **IP-address** (not DNS-name!)
Example: **https://192.168.1.100/scopd/cgi-bonline.exe?action=webex**
For the field **Scopes** select:
spark:organizations_read
spark:people_read
spark:rooms_read
spark:team_memberships_read
spark:teams_read
spark-compliance:events_read
spark-compliance:memberships_read
spark-compliance:messages_read
spark-compliance:rooms_read
spark-compliance:teams_read
Then click **"Add integration"**.

6) After creating the integration, you will be redirected to its page, from which you need to copy **Client ID** and **Client Secret** into the fields at this page of complex settings and then **save settings!**



7) Copy value of **OAuth Authorization URL** and paste it to the browser's URL field, next login as **Compliance Officer**.

8) Accept user rights assignment by clicking **Accept**.



9) At the last stage you will be redirected to **Redirect URI**, specified in step 5 and if everything was ok, then a message will be displayed about the configured integration and its expiration time (**3 months**).

10) **In 3 months** you need to renew the integration again.
Log in to **developer.webex.com** as **Compliance Officer** and go to the created integration: **developer.webex.com/my-apps**.
Further, the renewal can be done in three different ways:
Method 1: repeat steps 7-9.
Method 2: click at **"Regenerate the client secret"** and then repeat steps 6-9.
Method 3: delete current integration and create new one (steps 4-9).

Note: possible errors during synchronization can be viewed only through the server log.

Note: 3 months after (when the integration expires), a notification about this event will be sent to the system tray of the BOSS-Online module to all connected bosses.

Attention! If access to the Internet from the server is possible only through a **proxy**, then it must be set in the initial server settings (available through the START menu).

6.2.2.19. Reports generator - Parameters

Reports generator is intended for automatic reports generation on schedule without user's involvement.

The most important options in this tab:

Periodicity and time for reports generation
If periodicity is identified as Mon-Sun, Mon-Fri or Mon-Sat the reports will be generated within selected range. Timing amount in the report will equal to one day respectively.
If periodicity as "every Mon", "every Tue" is specified then the report will be generated once a week in the selected day. So the timing amount will equal to one week in the report respectively.
Attention! The day when the report is generated is not included into the report itself!
The weekly report file will be in several time bigger then the file with the day report!

Attention! Each manager is capable to enable or disable reports generator on his or her own **in the personal cabinet**.
Database administrator can forbid or allow certain manager to use automatic report generation in the managers' **Basic rights**.

See also **"Work schedule"** tab.

6.2.2.20. Reports generator - Reports (for bosses)

It is possible to set up the automatic reports generation for managers about all his or her subordinates.

Select the type of reports that you would like to see in the generated common report.
The more reports are selected the bigger file size will be in the final common report!
Additionally permissions for corresponding reports are set for each manager. So as a result the report will be generated only if it is selected on this page and the manager has corresponding permission rights for it!

Attention! Each manager is capable to enable or disable reports generator on his or her own **in the personal cabinet**.
Database administrator can forbid or allow certain manager to use automatic report generation in the managers' **Basic rights**.
So it is required to set corresponding right to the manager to enable such reports generator (option **"Enable auto generation of reports (for self)"**. It is necessary for manager himself or herself to make required settings **in the personal cabinet**.

6.2.2.21. Reports generator - Reports (for employees)

It is possible to setup reports sending to each employee about his or her activities.

These reports will be send only to those employees who has specified an **e-mail** in his or her **dossier** (the report will be sent to this e-mail).
At the same time e-mail sending option must be set up in the tab "Reports generator: Sending by e-mail".

It is necessary to specify at least one manager for automatic report generation for sending the reports to employees. The corresponding option must be selected in the manager's rights **"Enable automatic generation of reports (for subordinates)"**.

At the same time the administrator set up permissions for corresponding reports additionally for each manager. So the report will be generated only if it is selected on this page and is permitted for the manager in his or her permission rights!

Attention! Each manager is capable to enable or disable reports generator on his or her own **in the personal cabinet**. Database administrator can forbid or allow certain manager to use automatic report generation in the managers' **Basic rights**.

6.2.2.22. Reports generator - Saving to folder

The most important options in the tab:

Save reports in the folder
Specify the folder on the server where reports will be stored.
Attention! Do not specify root folder here (such as C:\, D:\ etc.)

6.2.2.23. Reports generator - Sending via FTP

The most important options in this tab:

Send reports to FTP server
It is possible to allow or prohibit reports sending to your FTP server.

FTP server
Specify FTP server for connection (without prefixes such as ftp:// etc.)

Port
Specify connection port (by default 21).

User/Password
Specify user's name and password on FTP server. Entry to the server will be performed with this user.

Use anonymous access
If your FTP server allows to use anonymous access and you don't want to enter FTP with a specific user it is possible to use this option.
User's name and password is ignored in this case.

Use passive FTP mode
Operation mode defines connection creation rules for data transferring via FTP protocol. It depends on your server.

Folder on FTP server to save reports
Specify the folder on FTP server where reports will be stored.
Attention! The folder must be existing one!
It is possible to indicate the path in the reference to current folder (usually it is root one) or in the reference to root (in such case it is advisable to put "/" at the beginning of the path).
If nothing will be specified reports will be created in the current folder (usually it is root one).
If only "/" is specified then they will always be created in the root folder.
Don't forget to put "/" instead of "\" (as usual in Windows system)!

Number of sending attempts
It is possible to set up how many attempts to try to send the report if it is not possible to perform by any reason from the first time.

6.2.2.24. Reports generator - Sending by e-mail

The most important options in this tab:

Enable sending by e-mail
It possible to forbid or allow sending reports to the managers'/employees' e-mail boxes and/or events/OTP-codes.

SMTP server
Specify SMTP server for sending thru. It is possible to use either your Internet provider server or any other available. If the provider server is used you need to clarify settings with it.
It is possible to use popular free of charge servers smtp.mail.ru, smtp.yandex.ru, smtp.gmail.com (for the last one **sending attached files may be blocked**!)

Port
Specify connection port (by default - 587) or it may be 25. For SSL connection please use port 465.

User/Password
Specify user name and password for SMTP authorization.
Usually user's name is the sender's e-mail.
If it is not required then it is necessary to check "Authentication is not required".

Authentication is not required
User's name and password will be ignored if it is selected.

From
Specify sender's return e-mail. **It must be obligatory** specified.
It must be **in the same domain as SMTP server** to avoid problems! For example while sending via smtp.gmail.com it must be as name@gmail.com as well as name@gmail.com must be user's name in this case.

Do not send mails larger then N megabytes
Specify maximum size of the sent.

Number of attempts while failing to send
It is possible to set up how many times the server will try to send the report if it fails to perform it from the first time by any reason.

Settings **sample**:

```
SMTP server: smtp.mail.ru
Port: 587
User: alex@mail.ru
Password: ******
From: alex@mail.ru
```

6.2.2.25. Reports generator - Sending to website

This functionality is no longer supported!

6.2.2.26. Reports generator - Sending to file sharing

It is possible to send reports for retention in the cloud file sharing services.
Configuration of the personal entry parameters into file sharing service is performed **in the personal cabinet** for each manager.

Attention! If access to the Internet from the server is possible only through a **proxy**, then it must be set in the initial server settings (available through the START menu).

6.2.2.27. Reports generator - Threats

On this page it is possible to enable automatic search of threats while generating reports (in the reports generator) or manual master report generation in BOSS program.
The threats itself are separate words (not phrases!) that will be searched in all generated reports (regardless the type of report).
Writing down of each new threat must start with a new line!
At the same time if **tildes "~"** are put before the word then algorithm of **inaccurate word comparison** will be used. It will take into account all possible misprints and language features.
Warning! Language morphology features are works only for **Russian** and **English** languages! Therefore, do not use the **tilde "~"** symbol before the words from other languages!

6.2.2.28. Notifications generator - Sending by e-mail

These options correspond to the settings on the page "Reports generator: Sending by e-mail".

6.2.2.29. Notifications generator - Sending by SMS

It is possible to setup sending events notifications via SMS to the managers' mobile phones and/or 2FA OTP-codes.
For sending events notifications the manager should allow it in his or her **personal cabinet** and specify phone number.
The path to external program with two obligatory parameters is indicated in the start command:
%PHONE% - mobile phone to sent SMS on it (UTF8 URL-encoded);
%MESSAGE% - SMS message text is sent (UTF8 URL-encoded).
The program must implement the sending.
The sending itself may be processed in any way. For example, via public paid SMS gateways by using of various http requests.

Below is an example of the command line for sending SMS through the popular gateway and the curl.exe utility, which is included in the complex:

```
curl.exe -k --silent "https://smsc.ru/sys/send.php?login=<LOGIN>&psw=<PASSWORD>&charset=utf-8&phones=%PHONE%&mes=%MESSAGE%"
```

6.2.2.30. Notifications generator - Integration with Telegram

It is possible to send notifications of events to the Telegram messenger, sending commands to the server from the bosses via the messenger or perform 2FA.

First, the administrator needs to create for the organization own Telegram-bot.
To do this, the administrator needs to add a bot with the name **@botfather** in his messenger's chat and send a message **/newbot**, then enter the unique name and unique username of your bot (username should end with "bot").
Example:
Name: MyCompanyNotifier
Username: MyCompany_bot

After that **@botfather** will create a bot for you and send HTTP API token in the chat message. Copy this token into the settings field **"Telegram bot token"** at this page.
Example of token: 123456:ABC-DEF1234ghIkl-zyx57W2v1u123ew11
Username of newly created bot should be copied into the **"Telegram bot username"** field.

1) To receive events notifications (or 2FA BOSS) boss should manually enable the appropriate setting and obtain **chat_id** in the **personal cabinet of the web-interface of the complex**.

2) To receive 2FA OTP codes for employees, administrator needs to complete additional settings here.

3) To send commands to the server it is needed to allow Telegram commands for the boss here, after that boss should manually obtain **chat_id** in the **personal cabinet of the web-interface of the complex**.
If you like, you can change the commands on this page in the appropriate fields.
Attention! The blocking and shutdown commands apply to all machines that are currently connected to the server! The bot does not issue additional warnings before execution!

Attention! The data is transferred to the **api.telegram.org:443** server via secure https-protocol through the server of the complex, so Internet access is needed to this Telegram server at the server machine (where the server of the complex is installed)!

Attention! After changing these settings, the rights settings for the users of the database, settings in the personal cabinet, the server needs about 1 minute to apply the settings!

Attention! If access to the Internet from the server is possible only through a **proxy**, then it must be set in the initial server settings (available through the START menu).

6.2.2.31. Notifications generator - 2FA (BOSS)

Each Database user has the opportunity to enable two-factor authentication (2FA) to enter BOSS-Online/Offline in the **Personal cabinet** of the web interface.
2FA is also possible **without the participation of the user in the personal cabinet settings**, which depends on the methods of implementing 2FA selected on this page:

Telegram (settings in the personal cabinet) - need to make settings here. Also, in the **Personal cabinet** of the web interface, user has to configure settings for Telegram (get chat_id and add a bot).

SMS (settings in the personal cabinet) - need to make settings here. Also, in the **Personal cabinet** of the web interface, user has to set his phone number for SMS receiving.

SMS (settings in the "Dossier of employees") - need to make settings here. Also in Dossier of employees in the contact list for the user, the phone number for SMS should be set.

Attention! The administrator can disable 2FA for a user on the page "Database users" (applicable only for 2FA methods with settings in personal cabinet!).

When 2FA is enabled, the user always has the additional option of using a **login by face photo**. To do this, the user have to first add one or more pictures of his face in his personal cabinet.
It is important to note that for this functionality to work, you need to configure access via https, because modern browsers block the use of web cameras through an insecure http-connection.

6.2.2.32. Client protection

When this option is enabled the software suite server will periodically check connection to clients' computers as well as standard **ping**. Based on information received it is possible to come to the conclusion about potential unauthorized deletion of the software suite client app on computers. If it happens it will be recorded in the report "Events: Computer" and a push notification will be generated (optionally) for managers in BOSS-Online (can be set up at "Events" page).
The event will be generated eventually in a couple of minutes (depends on the parameter "**Num cycles before event**"). Valid parameter values are from 0 to 9. The value 1 corresponds to a time of 6 minutes with the number of machines less than 100 (if there are more machines, then the time will be longer). If there is a lot number of false positives with a large amount of machines, then you can try to increase parameter value by 1-2.
The event will be generated periodically two times per day (till client app will be restored).
Attention! This option won't function in the situation when command **ping** is impossible to perform based on client computer name from server room (it usually happens when the client and the server are located in different networks).

6.2.2.33. Events

Here it is possible to select events for which notifications via BOSS-Online, E-mail, SMS to managers will occur.
Warning! E-mail/SMS are possible only for high-priority events!

Do not notify if event is older than (minutes)
When postponed mode is enabled or there is a long absence of connection between the client and the server, a situation may arise in which the notification of an event arrives in the instant notification channel much later than the event itself occurred, which does not always make sense. This setting actually sets the "lifetime" in minutes of notifications in such cases. Thus, instant notification will not occur if the event occurred before the set time.

6.2.2.34. Regular expressions

Here you can specify a list of your custom regular expressions that can be used in the complex when searching for threats (at tabs User: Threats, DLP: Rules).
The complex already has built-in templates: **@CREDITCARD@** (credit-card number), **@PHONE@** (phone number), **@EMAIL@** (e-mail). Thus, you can expand this list with your own templates.
Each expression begins with a **new line** and should have the following format:
@NAME1@=EXPRESSION1
@NAME2@=EXPRESSION2
@NAME3@=EXPRESSION3
...
Further, when using, it is enough to indicate only names in the format: **@NAME@**.

Note: Format of used regular expressions is **PCRE (Perl Compatible Regular Expressions)**. For testing you can use **regex101.com**

Note: Symbols to indicate begin and end of line **"^"** and **"$"** are ignored in expressions!

6.2.2.35. Work schedule

The most important options in this tab:

Public holidays
Choose days in which absence of employees will not be considered as absence in reports.

Shortened working day on pre-holiday days
Specify the time in minutes by which the working day will be shortened on pre-holiday days. This value is taken into account when calculating early exits in next reports: "Categories/deviations", "Consolidated", "Consolidated (lite)", "Timesheet", "PACS detailing".

Ignore lateness and early departure of less than (min)
Here you can setup max allowed late or early departure (in minutes) for the "Consolidated (lite)", "PACS detailing" and "Timesheet" reports. Set to 0 if no delays should be ignored.

Use break time in the % calculations
In BOSS-Offline reports, when calculating activity indicators or total time **as a percentage (%)** of the working day duration you can include or exclude the break time from the working day (divisor). So, when the break is included, the percentages will decrease, and vice versa - when excluded, it will increase.

Options for automatic reports generator
Specify the break in minutes, the beginning of the working day and the number of working hours (it is possible with a fractional part of an hour through a dot, for example 8.5 will be equivalent to 8:30, i.e. 8h30m) - this data is used in some types of reports.
See also **"Reports generator: Parameters"** tab.

See also **"Work schedules"**

6.2.2.36. syslog

It is possible to transmit messages about various events to an external system (for example, SIEM) via the syslog-protocol. In the "Server" field you need to specify "udp://server:port" (for the UDP protocol) or "tcp://server:port" (for the TCP protocol), also need to select the types of messages/events that will be sent to the server.

syslog-messages format description

Messages are transmitted in accordance with RFC5424 in the following form:

```
    SYSLOG-MSG      = HEADER SP STRUCTURED-DATA
    HEADER          = PRI VERSION SP TIMESTAMP SP HOSTNAME SP APP-NAME SP PROCID SP MSGID
    STRUCTURED-DATA = "[" SD-ID *(SP SD-PARAM) "]"
    SD-PARAM        = PARAM-NAME "=" %d34 PARAM-VALUE %d34
```

In general, messages duplicate the corresponding tables in the complex database as much as possible for greater compatibility.
Message example:

```
<134>1 2025-01-15T10:43:48.121Z SERVER-PC scopd-dlp - - [TReportUserEvents@60366 comp_loc="company.org"
comp_name="PC-0001" user_domain="COMPANY" user_name="user1" event_time="2025-01-15T10:10:12.012Z"
event_type="106" priority="1" description="\"D:\\filename.exe\" -> \"virustotal.com\""]
```

Description:

PRI=<134>
VERSION=1
TIMESTAMP=time in **UTC** of message transmission to server, but **not the time of occurrence of the event**! (the event may happen much earlier).
HOSTNAME=the machine name of the server from which the message is sent
APP-NAME=scopd-dlp
PROCID=
MSGID=
SD-ID=DB_table_name@60366
Note: DB_table_name now is TReportUserEvents, TReportCompEvents, but new ones may be added in the future.
Note: @60366 – IANA identifier
PARAM-NAME=name of the database table field, some may be present or absent, depending on the table itself.

Below are the main fields and their descriptions:
comp_loc – the domain of the computer on which the event occurred (example, “company.local”)
comp_name – NetBIOS name of the computer, on which the event occurred (example, “PC-001”)
user_domain – NetBIOS domain name of logged on user, for which the event occurred (example, “COMPANY”)
user_name – user login name (example, “user1”)
event_time – event time in **UTC** (in general, it can differ greatly from the TIMESTAMP of the package!)
event_type – event type, see below for constants explanation appendix
priority – event priority (0 – high, 1 - regular)
description – event description in text form (UTF-8)

Appendix: event codes (event_type)

```
100:  "exec app from threats list"
101:  "website from threats list"
102:  "input text from threats list"
103:  "print document"
104:  "copy to flash-drive"
105:  "copy to selected folders"
106:  "file send"
107:  "flash-drive insertion"
108:  "image in clipboard"
109:  "DLP: document reading"
110:  "DLP: document in clipboard"
111:  "DLP: text in clipboard"
112:  "DLP: PrintScreen"
113:  "DLP: copy to flash-drive"
114:  "DLP: copy to selected folders"
115:  "DLP: document send"
116:  "DLP: speech"
117:  "atypical behavior"
118:  "changes in hardware/soft"
119:  "possible client removal"
120:  "no face in front of webcam"
121:  "another face in front of webcam"
122:  "more than 1 face in front of webcam"
123:  "PC shutdown was postponed"
124:  "problem on the client PC"
125:  "changing microphone state"
126:  "critical app/site"
127:  "user logon"
```

```
128:  "blacklisted app execution"
129:  "DLP: document printing"
130:  "exec forbidden Linux command"
131:  "USB-device has been disabled"
132:  "DLP: file found"
133:  "crypto-address in the clipboard"
135:  "DLP: text on the screenshot"
```

6.2.2.37. Web-interface

Logo on the start page in svg-format

You can change the logo on the start web page to your own. Simply copy your logo's SVG tag into the field.
The logo will be activated the next time you log in to the web interface.
SVG requirements:
- the image should not have fixed dimensions, so **width=, height=** parameters should be removed;
- it is advisable to remove layer names or other parameters that contain non-Latin characters (for example, Cyrillic).

6.2.3. Client settings (computer):

6.2.3.1. Common settings

The most important options in this tab:

Operate in postponed mode
See **Postponed monitoring**

Perform periodic time synchronization of the clients' computers with server time
Periodically time will be synchronized with the server time on the clients' computers. That means that the time will be the same as on the server computer.
Following is recommended to avoid falsifications in the reports data!

Monitoring week days and time intervals
You can select week days when monitoring of clients' computers will be performed. Monitoring won't be performed in other days.
It is also possible to specify time intervals within which monitoring will be performed. Beyond this intervals monitoring won't be running.
The time intervals are set with comma or semi like: "hh:mm", "hh:m", "h:mm", "h:m", or "h".
Acceptable values for minutes: 0-59, for hours: 0-23.
Transition is possible across 0:00, e.g. interval beginning may be bigger than the end in absolute value.
Empty line identifies that there are no intervals and the monitoring won't be performed at all.
The interval such as 0:00-23:59 means that monitoring will be performed round-the-clock.
Interval examples: 8:00-13:00,14:00-17:00

Enable automatic update when the new version is available in the base
Similar to option in BOSS-Online "Update clients software" but only in the automatic mode. See "Software suite update" for more detailed information.
If the new version is put to the database after administrator's app update, in 1-2 hours after this new version will appear on the client's computers. Activation of the client's new version will happen only after client's computer **restart**!
It is possible to check the current version of the client's app via BOSS-Online function **"General information"**.

Perform automatic removal of the client's app
This option is aimed at synchronization with the domain. For example, in the corresponding domain security groups AD administrators have deleted a client computer from the monitoring list. In such case when synchronizing with AD (in manual or automatic mode) and this option enabled, the client app will be deleted from the computer some time later (from several minutes to several hours).
This option won't be effective if synchronization with AD has never been performed.
This option won't be effective either if client's computer is not joined into the domain.
After the client is deleted, the reports from the computer and all users of this computer in the database are also deleted only if option **"Keep reports after client uninstall"** is not turned on.

Key for uninstall from command line
If you intend to uninstall clients through the command line (for example, in the MS System Center), you need to set here the key (password with letters and/or numbers without spaces). See also here.

Set up new displayed name/client's service description
Whether lines are not empty it is possible to change name/client's service description.
Note: the change will come into force after client's computer restart.
Attention! Domain administrator can hide client service (see. here).

http-proxy configuration
Some options (for example, voice recognition) may require internet access via http-protocol from clients' computer (It is obligatory described in the information for each such option!). And in case in your organization it is required to use http-proxy, same settings should be set up here.

6.2.3.2. Monitoring - Machine time

It is possible to enable or disable monitoring computer's work time.
If it is disabled the data won't be recorded to the database.

6.2.3.3. Monitoring - Webcams

The most important options in this tab:

Receive and send the shots from the web-cameras to the server
If it is disabled the shots from the web-cameras won't be sent to the server.
This will allow to save network traffic.
If there are multiple webcams on the PC, the data is used from the webcam "by default".
Attention! In case this option is enabled web camera can not be used by other apps!

Make shots every N-seconds
Do not indicate very small value in order not to overload the network connection and do not occupy to much space with shot's files.
Specify zero to disable periodically shots.

Shots on user logon/logoff, system startup
When this option is enabled, if one of the listed events occurs, a shot will be taken.
This function will not work for a client installed on a terminal server!
If it is necessary to take only such, but not periodic shots, then for the interval of snapshots set 0.

See also server settings tab "Monitoring: Webcams"

6.2.3.4. Monitoring - Hardware control

You can enable or disable data transferring about computer's equipment to the server.
If it is disable this data won't be transferred to the database.

6.2.3.5. Monitoring - Chats-calls

What are the most important options in this tab:

Intercept messages of Bitrix24 chats
If this option is enabled, then Bitrix24 chat messages will be intercepted for the desktop application and the site.
When using the cloud version of Bitrix24, the server field should be left blank, and if you use the corporate server of Bitrix24, specify its name without prefixes https://, http:// and port number. If you use a non-standard port, you should add it to the page Network driver.
Attention! Network driver should be turned on for correct operation of this option.
Attention! After enabling the option, it will be activated the next time Bitrix client is started, or the Bitrix site is restarted on the client!

See also tab "Monitoring: Chats/calls" for the user.

6.2.3.6. Network driver

Network driver is used to intercept and control network traffic at low level.
If you turn off, there will be no interception of network data.
By default (implicitly) for interception added processes of popular web-browsers, mail clients, messengers, as well as standard ports of supported protocols (SMTP,POP3,HTTP(S),FTP(S)). In addition you can add non-standard TCP-ports (for example, proxy), and also exclude some ports. Similarly, with the processes for which monitoring is carried out. All the data must be specified in comma-separated list.

Unlike programs (processes) launched by the user, the network driver intercepts traffic from all services (this is made to support the interception when using some antiviruses), but there are situations when some services need to be added to exceptions list. In the **exclude services list** you need to specify exe-file of such services (not service name!). Masks also allowed. For example, *.* prohibits traffic monitoring from all services.

It is important to note that to intercept encrypted (SSL) traffic, program set the root certificate named **"Local NetFlt CA 2"** in the system. At the same time, some programs use their own root certificate databases, so they can issue a warning.
For the most browsers and e-mail clients, there will be no warnings if the client was installed when the windows of these applications were closed. Otherwise, you need to restart the client machine, or LogOff the session, or add the certificate to the trusted in the application itself (using warning window).

In **exceptions** list you can add hosts names or IP addresses for which the network driver will not be used. Typically, this can be done for sites that are sensitive to SSL certificate replacement.
Every exception in the list should start with a new line.
You can specify DNS-name (masks "*" and "?" are allowed), exact IP address (IPv4/IPv6), address with masks, as well as address ranges (only IPv4).
Examples:
134.17.23.*
192.168.1.15-192.168.1.20
10.10.1.5
*.dep.domain.com

It's important to note that to intercept visited URLs in browsers for reports, the network driver is not used!

In the old OS - Windows XP and Windows 7 the driver will not work!

Linux-client: options "Add processes" and "Exclude services" are not supported!

6.2.3.7. Selected observation

The most important options in this tab:

Monitor "only certain computer(s) user(s)" or "all except"
By enabling this option it is possible to specify computer's users who will be monitored or users will not be monitored.
It is possible to use the following **masks "*" and "?"** to specify user's name.
It is acceptable to specify users in the format like **user** and **domain\user** (in such case **the domain is specified in the short NETBIOS-format** - without dots!).
If this option is disabled **all computer's users** will be monitored.

Apply this restriction only to machines running Windows Server OS
In the current version this option is ignored and not used.

Attention! Group/profile settings for options at this page are ignored (only the "default" profile is used)!

6.2.3.8. Local storage

On this page it is possible to set up local storage. This local data storage is located on the clients' computer and is used when there is no connection with the server or in **postponded monitoring** mode. In such cases all monitoring data is stored in this database and is sent to the server when host becomes on-line or transfer postponed data when building reports in BOSS-Offline.

What are the most important options in this tab:

Storage time, max database size, traffic
Do not specify too big value as more space will be used on the disk of client's computer in the first place (because of shadow copy files mainly). Secondly, when trasferring data to the server the load on network traffic and server database may increase!

Separate retention period for shadow copies
If the parameter value is not -1, shadow copies (including screenshots, but excluding audio for autorecording) will be stored accordingly with this parameter, and all other data - using the "Store data in local storage no more than" parameter.
If the parameter value is -1, absolutely all data will be deleted using the "Store data in local storage no more than" parameter.

Do not perform, if free space is less than
Local storage will not be operable (data loss as result) if free disk space on clients' C: is less than value specified here.

6.2.3.9. Restrictions

The most important options in this tab:

Forbid writing to the removable drives (Flash)
When this option is enabled users aren't capable to save/copy the data on flash drives.

Deny FTP/FTPS-protocol
Disable file transfer (in/out) thru the FTP/FTPS
It is necessary to enable the Network driver

Deny SSH-protocol
Disable data transfer thru the SSH
It may be necessary to set this restriction if you need to intercept sending files via FTP/FTPS, so users can not be able to use SSH FTP (because this protocol is not supported during interception).
It is necessary to enable the Network driver

Do not allow connections through Wi-Fi, Bluetooth, USB-modem
All TCP-connections (via ports controlled by the network driver) through the specified devices will be prohibited.
It is necessary to enable the Network driver

Do not allow incoming RDP-connections
It will not be possible to connect to the computer remotely using the RDP protocol.
It is necessary to enable the Network driver

Deny access to the following websites
You can specify the list (each site from a new line) of DNS names (not URLs!) of websites that will be blocked through standard web browsers. Masks are allowed.
It is necessary to enable the Network driver

Shutdown the computer outside this interval
Usually the option is used to save energy. If the current time is outside the specified interval, the user machine will be turned off with a message shown to the user.
The user can either turn off the machine immediately, or extend the work for N-minutes with an indication of the reason. In this case an event with the reason text will be saved on the server for viewing through the "Events: user" report.
Format of the time intervals is described here.

See also user's settings tab "Restrictions"

6.2.3.10. Events

It is possible to set up the capability of saving different events into the report "Events" of the database.
To setup notifications to managers see **server** page "Events".

6.2.3.11. Search in files

You can enable indexing of document files on client machines for quick subsequent search documents by keywords or regular expressions within their content via BOSS-Online ("Search in files" function), as well as in the BOSS-Offline "Search in files" report (when periodic search is enabled).

Attention: make sure that the database user is allowed access to the "Search in files" functions for BOSS-Offline/BOSS-Online on the rights settings page!

Settings
The indexing process may take a long time, and the index itself can use significant amount of space on the system disk of client machines. There are many settings for different needs in this functionality:

providers.searchEngine.idlePeriod - time in msec after which the scanner enters the active scanning phase after the last user activity

providers.searchEngine.rescanPeriod - time in msec to repeat the scan cycle after the completion of the previous

providers.searchEngine.scanRateIdle - scanning intensity in the state of user inactivity (active phase) from 0.01 to 1.00

providers.searchEngine.scanRateUsed - scanning intensity in the state of user activity (passive phase) from 0.01 to 1.00

providers.searchEngine.scanRateForced - not used in current version

providers.searchEngine.scanRateFrozen - not used in current version

providers.searchEngine.maxFieldLength - max. number of words in the document to analyze

providers.searchEngine.maxDocCharsToAnalyze - max. size of the document retrieved from the index, used to find the best chunk or when directly querying the entire document

providers.searchEngine.maxSizeFile - max. file size to analyze in bytes

providers.searchEngine.maxSizeNest - max. archive size to analyze in bytes

providers.searchEngine.maxDepthDir - max. nesting depth of directories/folders when scanning

providers.searchEngine.maxDepthNest - max. nesting depth of archives into each other

providers.searchEngine.maxSizeIndex - max. index size in bytes

providers.searchEngine.minIndexFreeSpace - min. size in bytes of free space on the system disk, at which scanning and index formation is possible

providers.searchEngine.indexedFileLivetime - lifetime (in msec) of the indexed file in the database for the case when original file was deleted.
Attention! This parameter should not be less than the time of the full scan cycle, therefore it is not recommended to set the value less than 2-3 days!

providers.searchEngine.indexableFileTypes - indexable file types.
In the current version supported formats are: zip,7z,rar,txt,csv,htm,html,eml,mht,pdf,doc,docx,xlsx,pptx,odt,ods,odp,odg

providers.searchEngine.detectFileType - when enabled, the file type will be recognized by its signature, not the extension in the name.
Attention! Enabling this parameter increases the indexing cycle time, as well as significantly increases the size of the index on disk!

providers.searchEngine.excludeFileMasks - exclude file masks from scanning process

providers.searchEngine.excludeDirMasks - exclude folders (without paths) from scanning process (masks also allowed)

providers.searchEngine.storeIndexedContent - whether or not to store the contents of the found fragments in the index (true - increases the size of the index, but allows you to show fragments of the found text, and not just the path to the document, false - does not save)

providers.searchEngine.includePath.1 - path for scanning. Specify asterisk * to scan all the drives (with exception of network drives). To search for a specific logical disk, you need to specify a path of the form \\?\C:\
it is not allowed to use here environment variables (%variable%)!

providers.searchEngine.includePath.2 - if necessary, you can specify the second, third, etc. paths for scanning

providers.searchEngine.ignoreRemovableDisks - if set to false, then removable disks will also be scanned in all disks scan mode

providers.searchEngine.minTimestampFile - specify date in the format YYYY-MM-DD and files modified earlier this date will not be indexed

providers.searchEngine.regExpOverlapSize - maximum string length that can be found using regular expressions

providers.searchEngine.regExpMatchLimit - the maximum number of matches that can be found for one regular expression in one document

providers.searchEngine.textAnalyzer - language analyzer used to break text into terms, possible values: Standard, Czech, Dutch, English, French, German, Russian

providers.searchEngine.fragmentsLimit - the maximum number of text fragments that can be returned in search results for one document

Note: each time these settings are changed, the index is completely rebuilt, i.e. the accumulated data is deleted and the scanning process starts over.

Enable periodic search
When enabled, it will periodically search for the query **"Search query"** every **"Search interval"** hours, the result will be sent to the server for "Search in Files" report.

Max search results
How many search results (actually documents in which the query was found) to use. Results are sorted by relevance. Possible values - from 1 to 255.

Retrospective of results (days)
If a request is found in a document, then it makes no sense to send information about this document to the server in each iteration of the search (so that there are no duplicate results in the report). This parameter indicates how many days to store information about the results found (if you specify 0, then the information will be stored indefinitely), i.e. after this number of days, the result will be stored to the report.

Search query
The search query is specified here.
A line break in the query is equivalent to space character.
A full description of the request format can be found here: https://lucene.apache.org/core/2_9_4/queryparsersyntax.html, but a slight extension of this syntax is also used.

Examples:

Search of words **test and software** in a single document:
test AND software

Strict comparison search (should be specified using double quotes):
"word1 word2"

Search of **docx** documents, in which there is a match for the regular expression **@IPv4@** and contain word **"personal"**:
type:docx AND @IPv4@ AND personal

Search file by it's **md5** checksum:
digest:3fcdcb42d0797d0b08c52e9d214b4ad2

Search of encrypted files (for example, password-protected archives):
flags:encrypted OR flags:unsupported

Note: searching for regular expressions is only possible from **this list**, specifying the desired regular expression in the format **@NAME@** (**names are case sensitive!**)
If you need to find **any** from regular expressions ("OR" condition), then you need to use **@||@**
If you need to find **all** regular expressions ("AND" condition), then you need to use **@&&@**

6.2.4. Client settings (user):

6.2.4.1. Common settings

The most important options in this tab:

Operate in postponed mode
See **Postponed monitoring**

Type of monitoring
When monitoring with notice is selected the user will see a message in the system tray every time with the system startup. The text of the message can be changed.

Monitoring days of the week and time intervals
You can select week days when monitoring of clients' computers will be performed. Monitoring won't be performed in other days.
It is also possible to specify time intervals whithin which monitoring will be performed. Beyond this intervals monitoring won't be running.
The time intervals are set with comma or semi like: "hh:mm", "hh:m", "h:mm", "h:m", or "h".
Permitted values for minutes: 0-59, for hours: 0-23.
Transition is possible across 0:00, e.g. interval beginning may be bigger then the end in absolute value.
Empty line identifies that there are no intervals and monitoring won't be performed at all.
The interval such as 0:00-23:59 means that monitoring will be performed round-the-clock.
Interval examples: 8:00-13:00,14:00-17:00

6.2.4.2. Monitoring - Face recognition

Here you can enable periodic facial recognition of employees via webcams for the same named report in BOSS-Offline and generation events when they are enabled at the tab "Events".

Prohibit closing/sealing the webcam
When this option is enabled, the user's workstation will be locked with a message in case system detects that webcam was sealed/closed during taking picture.

Lock workstation in case of no face or unknown
When this option is enabled, the user's workstation will be locked with a message in case system detects that during taking picture there is no face in front of the camera, or it belongs to an unknown person or another employee.
See also server settings for faces recognition.

Note: When Postponed monitoring is enabled, face recognition will not occur, but shots from webcam will still go to the report!

6.2.4.3. Monitoring - User time

You can enable or disable the monitoring over user's working time (entries/exits in/out of the system).
If this option will be disabled these data won't be sent.
This option is especially relevant for terminal sessions. Thanks to this option it is possible to control when the user starts and finish the work each day as the option of **computer time** monitoring is unlikely be informative for terminal server.

Minimum activity interval time (in seconds)
After each mouse click, scroll or key press, the user will be considered as active for the specified time (for the "User Time" report). Valid range: 30 to 600 sec.

6.2.4.4. Monitoring - Applications-sites

The most important options in this tab:

Perform the monitoring of the running apps and websites
If this option is disabled the information about user's running programs/websites won't be sent to the database as well as the text typed by the user.

List of corporate websites
It is possible to specify websites that won't be included to the report "Websites" as they will be in the report "Programs". Usually this option is needed in the company where employees use corporate websites mails or others.
Each website must be specified from the new line! It is possible to specify both full and partial URL.
Examples:
http://corp.mail/mail
1c.ourcorp.com
Attention! When changes are made to the list of corporate websites, information about the active time in the reports "Consolidated" and "Apps/Sites" may be different within the current day. Correct calculation will start only from the next day!

Monitoring of lock screen app
When enabled, it is possible to intercept the entered user passwords when unlocking the screen!

Disable activity and text monitoring for applications/sites
You can set exceptions for the activity monitoring and keylogger as one or more logical conditions for identifying a particular application/site (rules for creating conditions see **at this page**)

Transmit app icons to the database
If this option is disabled app icons won't be transferred to the database. They won't be seen in the reports as well. This option helps to save the network traffic slightly.

Frequency of data transfer to the server (in minutes)
How often the accumulated monitoring data (including keylogger text) will be transferred to the server. Specify the interval in minutes from 1 to 15.
The parameter makes sense to use only in conjunction with the report Global search, for example, reduce the interval, to more accurately go to the desired screenshot when searching for text in the keylogger. If the "Global Search" report is not used, then there is no point in changing the parameter, because decreasing the number slightly increases the load on the database.

Transmit data for the Global Search report when the active window changes
If this option is enabled, every time the active window is changed, its title and URL will be sent to the server for writing to the database in order for the Global Search report to work, which must be enabled. See resp. options on the settings page for the server.
Attention! Enabling this option increases the load on the database!

Do not transmit the title of the current window to the program "BOSS-Online"
This option also helps to save the network traffic slightly.

Allow TeamViewer sessions monitoring as well as similar programs
In case this option is disabled the activities and typed text in the remote TeamViewer sessions won't be recorded.
When this option is enabled program actions which imitate clicks and pressing keys may get monitored.
This option doesn't influence on RemoteDesktop sessions!

6.2.4.5. Monitoring - Keylogger

The most important options in this tab:

Perform monitoring of the typed text on the keyboard
If this option is disabled user's typed text won't be transferred to the database.

Transmit passwords for applications entered by users
Attention! We can not guarantee that when you turn this option off, all applications will stop collecting passwords! This functionality is very specific for each app individually.

Disable text monitoring for applications/sites
You can set exceptions for the keylogger as one or more logical conditions for identifying a particular application/site (rules for creating conditions see **at this page**)

Max paste length in symbols via CTRL+V/SHIFT+INS
If text being pasted from the clipboard (via standard key combinations) exceeds the specified parameter in length, it will not be added to the intercepted text.
It usually doesn't make sense to treat huge clipboard pastes as user-entered text.
If you specify 0, this will completely exclude the addition of pastes from the clipboard to the intercepted typed text.
Max allowed parameter value - 100000.
Pastes from the clipboard via context menu are never added to the intercepted typed text!

6.2.4.6. Monitoring - Clipboard

The most important options in this tab:

Perform monitoring of the text/images in the clipboard
In case this option is disabled the text content and images from user's clipboard won't be transferred to the database. Monitoring of the files in the clipboard is set up in the tab "File operations".
It is necessary to enable the option "Shadow copy" **to capture images** in the clients' and server settings!

Add "watermarks" to the PrintScreen-image
There is a possibility of hidden marking of images copied from the screen by pressing **PrintScreen** or using **Snipping tool** application. The purpose of this marking is the possibility of subsequent identification of the employee, his PC and the date, if this image ever will be discovered in open sources or in some other way will be received by the company's security personnel. Typically, sensitive screen data or data of commercial value is captured and sent.
To obtain information from the "watermarks" on the image, you need to click "View watermarks" button and select an image file for analysis, after information about the found employee and date will be displayed, or 0 results if there are no watermarks or it was not possible to extract them. Sometimes (very rarely) more than one result can be returned. In addition, technical debugging information is also issued (for the technical support).
It should be noted that the algorithm for working with watermarks takes into account the possibility of resaving screenshots in quality-loss format (JPEG), and also allows image resizing by resize operations (for example, when sending via messengers). The actions described above reduce the probability of successful extraction.
Attention! If a third-party utility for intercepting PrintScreen is installed on the PC, correct interception and processing of this PrintScreen-functionality cannot be guaranteed!
Attention! When using **Snipping Tool**, the "watermark" is applied to the clipboard image, not to the copy that can be saved to a file from the application! Also, for too small screen fragments, the operation of the algorithm is impossible!

Forbid clipboard with the active Remote Desktop window
It is possible to enable this option so while working with the remote server via Remote Desktop users won't be able to copy images/text/files through the clipboard to their local computer from the server. At the same time it is necessary to disable the clipboard usage in Remote Desktop settings while connecting to the remote server. In this case the clipboard of the remote session itself will function in the usual mode.
This option requires installation of the client part of the complex on the computer where the Remote Desktop window is opened, and not on the remote PC/server!

Forbid clipboard when copying from RDP session
Enabling this option when working with Remote Desktop (RDP), users will not be able to copy images/text/files from the remote desktop via the clipboard to their local computer.
This option requires the installation of the client part of the complex on a remote computer, and not on a local one!
Attention! The restriction will only work if after the copy operation **RDP window is minimized by the user to the taskbar** (for subsequent switching to the destination window on local PC for the Paste-operation)

Exclude the following apps from interception
You can set applications for which clipboard prohibitions and monitoring will not be in effect.
It is necessary to specify the names of executable files (without path) separated by commas. Example: winword.exe,notepad.exe,chrome.exe

Monitor crypto-addresses in the clipboard
When you enable the option and crypto wallet address found in the clipboard, as well as an enabled event at the "Events" tab, an event will be generated for the "User Events" report.
List of supported blockchains and coins:
Bitcoin, Ethereum, BNB (Ethereum), Finiko token (Ethereum), Enjin coin (Ethereum), Holo (Ethereum), Polygon (Ethereum), Shiba Inu (Ethereum), USDK stablecoin (Ethereum), UNI (Ethereum), BUSD stablecoin (Ethereum), USDT (Ethereum), USDC (Ethereum), DAI (Ethereum), Tron (Ethereum), USDT (Tron), USDC (Tron), BNB (BNB Smart Chain), USDT (BNB Smart Chain), USDC (BNB Smart Chain), DAI (BNB Smart Chain)

API-token used for analysis
There is also an optional ability to analyze crypto addresses for risks of use (from 0% to 100%) and issue a short risk tag code.
To implement this feature, integration with the SHARD online service is provided. You need to obtain an API token via the form and add it at this page.
When a crypto address is detected in the clipboard, a request will be made from the client machine to the server https://shard.ru to obtain risk information, this information will be reflected in the "User Events" report.
You can also block copying to the buffer of dangerous addresses whose risk is higher than the required one. If you set -1, then each address will be blocked, and if you set it to 100, then no blocking will occur.

6.2.4.7. Monitoring - Screenshots

The most important options in this tab:

Receive and send screen shots to the server
If this option is disabled screen shots are not transferred to the server and this allow to improve network traffic.

Make shots every N-minutes/seconds/milliseconds
Do not specify too small value in order not to load the network and not to occupy to much space with shots files.
Note: when saving screenshots in the database, caching is used, so the result will appear in reports with a delay of 5 minutes!

Only if differs from prev. at least N-pixels
When enabled, a comparison of the current and previous screenshots is used (pixel by pixel). If the difference in pixels exceeds this value, the picture will be taken and transferred to the server, otherwise it will not. Enabling allows you to save traffic and load on the server/database without saving similar or identical screenshots.

Only if the last activity was less than N-sec ago
When this option is enabled, screenshots will not be taken if the last user activity (keyboard/mouse) was earlier than the selected interval (in seconds) from the scheduled time of taking a screenshot at the current moment.
Enabling it allows you to essentially not create the same or very similar screenshots when the PC is in idle state.

Add. screenshots when active window / browser tab changes
Also take a screenshot every time when the active window or browser tab changes in addition to periodic screenshots.

Save shots only in the report BOSS-Offline
It is possible to view shots in the report "Screenshots" of BOSS-Offline. In this case it is necessary to **enable shadow copy for clients' computers and server!**

Save shots only in the folder on the server
Sometimes it is useful to view users' screenshots not only through reports in BOSS-Offline but also directly from the server folder with the breakdown by users. In such case this option must be enabled and shadow copy is not necessary to run. As the shadow copy is necessary to review screen shots through reports. It is also required to set up the folder and other folder options in the server settings "Monitoring: Screenshots".

Save shots in the report and in the folder simultaneously
Merging above mentioned options.

Shots options
Number of options which allow to set up shots saving.
With the help of these options it is possible to improve the load on the network traffic and decrease the space that occupied by shots at the cost of images quality. That's why it is important to select parameters based on your requirements.

6.2.4.8. Monitoring - Screenshots (extra)

It is possible to choose for which apps or websites special screenshots will be done "by content changing" in order not to miss important text or other information in the window.

"Interval of checking for window content" determines how often the window content to be compared with the previous one, i.e. actually determines the maximum frequency of screenshots making.

"Minimum number of differing pixels" used in the comparison of the current and previous contents of the window (pixel-by-pixel). If the pixels difference exceeds this value, the window shot will be taken.

In rules for apps/sites can be used:

1) Variables:
@exe@ - exe-file of app without path;
@class@ - window class (use this tool to determine windows classes: download);
@url@ - full site URL;
@title@ - window title.

2) Logical operators: **OR**, **AND**

3) Brackets **(** and **)**.

4) Comparsion operators: **=** (equal), **!=** (not equal), **LIKE** (comparsion using masks).
Allowed masks: **%** (zero, one or more than one symbol) and **_** (only one symbol).

Attention! During comparsion of strings operators **=**, **!=** are case sensitive and if you don't need this sensitivity (for example, comparsion of file names), use operator **LIKE** instead!
Attention! Strings in rules must be specified in **single quotes**!

Thus it is possible to organize a flexible rules-based test for a particular application/site.

Example 1: rule for app with exe-file "app.exe", window class "WndClass_0" and window title should includes words "Workbench" or "Setup":

```
(@exe@ LIKE 'app.exe') AND (@class@='WndClass_0') AND ((@title@ LIKE '%Workbench%') OR (@title@ LIKE '%Setup%'))
```

Example 2: rule for site "https://work.company.com":

```
@url@ LIKE 'https://work.company.com%'
```

6.2.4.9. Monitoring - Printing

The most important options in this tab:

Perform monitoring of the documents printed on printers
If this option is disabled the information about users' printed documents on printers won't be transferred.

Monitoring in the user's context
Administrator's rights are required for **network** printers monitoring. The user won't be able to monitor if he or she hasn't got these rights or rights are restricted. In such case it is required to specify that monitoring will be performed in the context of the other user-administrator. It is also necessary to specify this administrator's domain (if available), name and the password (it won't be functioning with empty password!).
For example, in case if administrator's user with the name "Administrator" is available on all clients' machines it is required to check the password is not empty and it is similar everywhere. After it is inserted into this option.
Do not mix up this user with the user on the server! This inserted user maybe either part of the domain or be located on local clients' computers.
If the user has already been working with administrator's rights there is no need to specify anything!

Attention! While using Shared printers:
It is required to use special app (downloaded here) for monitoring of the shared printers. This app must be installed on print-server(s) to which printers are connected. In such case the option "Perform monitoring of printed documents on the printer" may be disabled (if all printers are shared).
It is required to specify certain users in the printer access settings in the **terminal** sessions. Do not leave the field **"Everyone"**!

Attention! It is necessary to enable the option "Shadow copy" to **capture printer's files** in the **clients' and server** settings! Printer's files are presented not in the original but as spooler files (.spl/.shd). It necessary to use third party apps to review them.
It is possible to search in the internet "SPL Viewer".
Example apps:
http://www.lvbprint.de/html/splviewer1.html
http://www.prnwatch.com/pviewer.html
There is also a possibility of **repeated spooler file sending to the printer** for original documents analysis on the hard copy. Use free of charge app for this **PrintSPL** which you can download here.

Attention! these settings will come into force after clients' computer restart!

Intercept printing inside processes
This additional option can be enabled if you need to block printing when DLP is triggered and/or apply watermarks to documents.
In this case you need to specify list of executable programs (separated by commas) in which you need to intercept printing in this way.

Put a watermark while printing
Ability to overlay text on top of the entire print page in the form of a domain name and user name.
The font format should be specified as follows:
FontName,FontSize,FontWeight,R,G,B
FontName - font family name;
FontSize - font size;
FontWeight - font weight (from 100 to 900);
R,G,B - color components (from 0 to 255 each).

6.2.4.10. Monitoring - File operations

You can enable or disable the monitoring over different file operations on the different types of drives.
File operations such as: reading, writing, deleting or copying into the clipboard.
It is also possible to monitor selected folders. In such case it is required to specify the list of such folders using semicolon as a divider (it is possible to use environment variables %variable% for Windows).
All copy operations to removable drives as well as copying to **selected folders** and clipboard are sensitive to **shadow copy**.
See also tab **"Shadow copy"**.

Show progress window for heavy file operations
If copying a large number of files using slow resources (network / flash), it may take a long time to pre-process and analyze.
In such moments for user maybe better to see not just the hourglass cursor, but window with text "Files processed: NNN".

6.2.4.11. Monitoring - Sending files

On this page it is possible to set up a possibility to monitor sending files via websites as well as mailing programs (Outlook, Mail, Bat, LotusNotes, Thunderbird) and desktop-chats Skype, Telegram, WhatsApp, Trillian, Viber, Mail.ru Agent, QIP, Lync, MS Teams, Slack, Webex Teams, Myteam, VKTeams, Zoom, eXpress, iMazing, YandexMessenger, WeChat Desktop, MTS Link Desktop, Jazz Desktop, New Outlook, Max. Also FTP/FTPS traffic is monitored.
Attention! In the current version there is no FTP-file transfer blocking. Instead, you can completely block FTP traffic in the settings!

Unconditionally prohibit sending files
Prohibits sending any files in the above-described applications and browsers.

Do not prohibit for ...
Allows you to set exceptions not only for the "Unconditionally prohibit sending files" option, but also for blocking sending when DLP triggered.

Windows: Disable alternative sending methods via ContextMenu
Allows to disable "Send" and "Share" items in the Windows Explorer context menu. It is recommended that the user log out and log in back again for the changes to take effect!

See also "Corporate sites"

6.2.4.12. Monitoring - Mail

On this page it is possible to set up capturing incoming and outcoming emails in the mail clients and web.
It is necessary to enable the Network driver

Supported clients and protocols:
Outlook - all mails (Exchange/SMTP/POP3/IMAP);
Lotus Notes - only outgoing;
Thunderbird, TheBat, Mail - all mails (SMTP/POP3);
Web clients: the list of supported websites may vary from version to version, and you will also need to configure the proxy if it is used on client machines to access the Internet.

Do not monitor correspondence with these e-mails
You can specify a list of e-mail addresses, mails with the presence of which in the "To", "Copy", "CC", "From" fields will not be monitored.

List of masks for internal (corporate) e-mails
You can specify a comma-separated list of masks for corporate e-mails.
Example:
*@company.org, *@int.company.org
This list will be used to generate the corresponding event with additional notification in the system tray.

Outlook: monitor only default storage
Turn on the option if Outlook performance problems are observed on client machines - it will monitor not all storages, but only the main one (default).

Outlook: do not intercept mails
Select only appointments from the Outlook calendar (if the corresponding option allows it) and do not intercept mails. Typically this option is for debugging purposes.

Outlook: do not intercept appointments
Select only mails from the Outlook (if the corresponding option allows it) and do not intercept appointments from calendar. Typically this option is for debugging purposes.

Outlook: monitor folders for DLP-attachments
This option is an extension of file analysis for occurrences of confidential data (see the settings on the "DLP" tab)
Acc. with the monitoring interval setting Outlook folders ("Appointments", "Tasks" and "Drafts") are scanned and, if detected an attachment file that meets the criteria set on the "DLP: Rules" tab, an event "DLP: file found" is generated (should be enabled at the "Events" tab). If the deletion option is enabled, the attachment file will be deleted and a notification about the deletion will be sent to the user in the system tray.

Attention! It is necessary to enable "Shadow copy" in the clients and server settings for capturing emails!

6.2.4.13. Monitoring - Chats-calls

On this page it is possible to set up capturing incoming/outcoming messages and voice calls in the messengers:
Lync - messages and voice;
Skype - messages and voice;
Skype Web - messages;
Slack - messages and voice;
Slack Web - messages;
MS Teams - messages(*) and voice;
MS Teams Web - messages(*);
Viber - messages(*****) and voice;
Telegram Web - messages(***);
Telegram Desktop - messages and voice;
Zoom Desktop - voice;
WhatsApp Desktop - messages and voice;
WhatsApp Web - messages;
Webex Teams Desktop - voice;
Webex Teams Desktop/Web - messages(**);
Bitrix Web - messages;
Bitrix Desktop - messages and voice;
Myteam Web - messages;
Myteam Desktop - messages and voice;
VKTeams (Cloud) Web - messages;
VKTeams (Cloud) Desktop - messages and voice;
Yandex Messenger Web - messages;
Yandex Messenger Desktop - messages and voice;
eXpress Desktop - voice;
eXpress Desktop/Web/Mobile - messages(****);
TrueConf Desktop - voice;
TrueConf Desktop/Web/Mobile - messages(****);
Dion Desktop/Web/Mobile - messages(****);
WeChat Desktop - voice;
MTS Link Desktop - voice;
Jazz Desktop - voice;
Max Messenger Web - messages;
Max Messenger Desktop - voice;
Mail.ru Agent Desktop - voice.

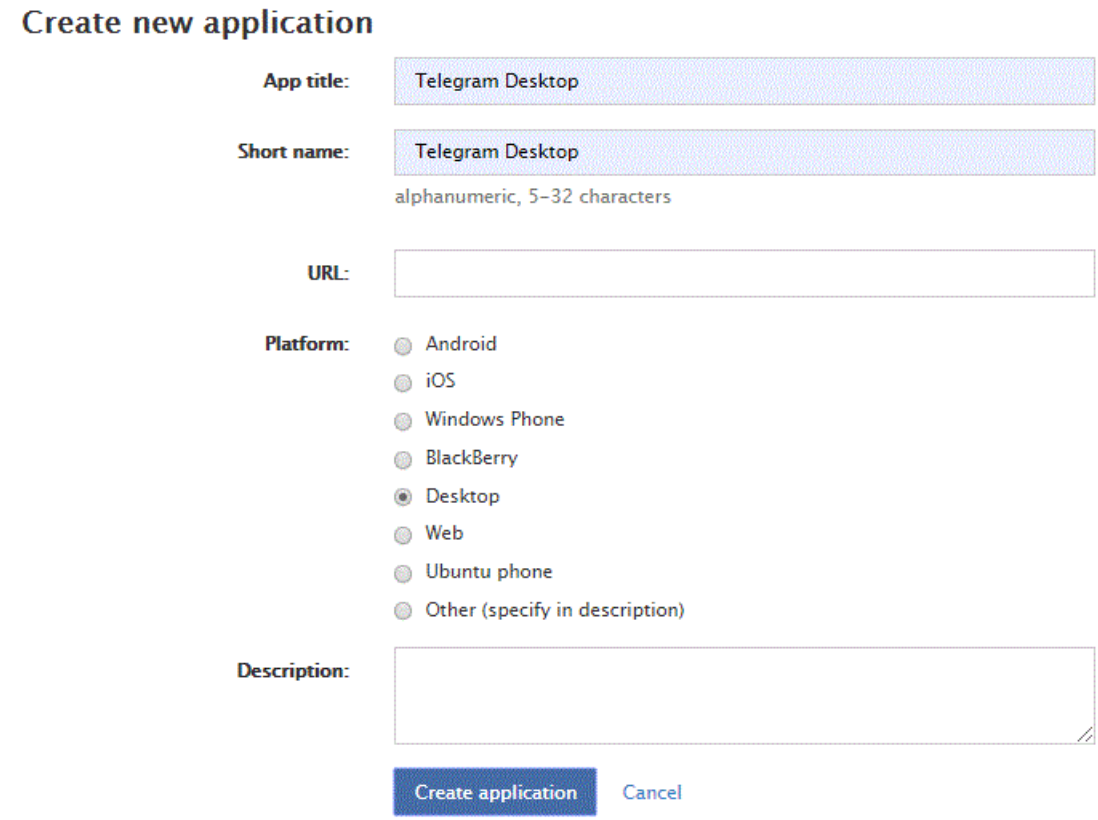
It is necessary to enable the Network driver

The most important options in this tab:

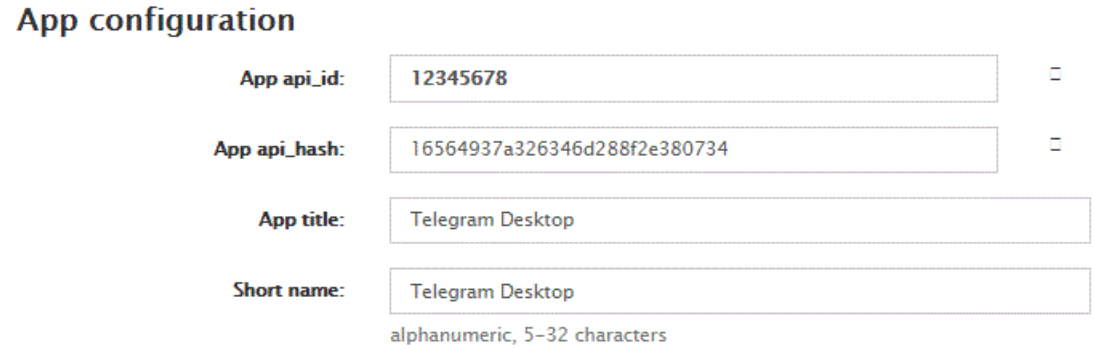
Capturing and saving voice conversations
Audio files will be transferred to server in shadow copy mode (reviewing in the report "Chats/calls").
Attention! It is necessary to enable the option "Shadow copy" in the clients and server setting for capturing voice!

Audio speech into text conversion
Attention for Google engine: enabling this option you automatically agree that employees' voice conversations (at the time of the speech begins in the app) will be transferred to the external servers of Google company in the real time (via http/https protocols) for analysis and processing.
You must familiarize and accept Google confidentiality policy: https://policies.google.com/privacy
Also enabling this option you agree to use it only in legit cases as it is stated in the licence agreement for this product (with its installation).
Attention for own neural network server: voice traffic from client machines will go to the server configured here.
Common note: an outgoing traffic on the employee's computer will be about 0.25 Mb/s while performing the processing.
Attention! In case in your organization it is required to use **proxy** for Internet access from clients computers then required settings have to be done in the tab **"Common settings" for computer**!

Intercept Telegram Desktop messages
Important: when this option is enabled, at the client machines where Telegram Desktop is installed and launched **re-login will caused** (i.e. the Telegram application will offer the user to re-enter the phone number and receive a confirmation SMS), however, this action will need to be performed by the user **only once**!
Also for interception it is need for **administrator** to obtain **api_id/api_hash** and copy them into the settings fields.
For the **api_id/api_hash** retrieval you need to:
- have an active Telegram account and enter to web-site **https://my.telegram.org**
- next go to the **"Api development tools"**
- create new app as shown:



- next copy/paste api_id/api_hash:



Important: if a proxy with authorization is used on client PCs, then you need to configure proxy settings at this tab for interception of **Telegram Desktop**!
Note: the account for creating the Telegram application is in no way connected with the accounts whose messages will be intercepted and there are no requirements for it.

(*) - to receive real **MS Teams** contacts instead of IDs, it is recommended to make settings on **this page**. Also, only interception of messages for corporate Teams users is supported, but personal Skype, Live logins cannot be intercepted in Teams.

(**) - need to set up integration here.

(***) - when you first turn on/install the client, interception will not be possible immediately, but after max. 1 hour (this is due to browser data caching).

(****) - need to set up integration here.

(*****) - the ability to intercept Viber Desktop conversations depends on the time of the initial installation of Viber on the PC.

6.2.4.14. Monitoring - Shadow copy

The most important options in this tab:

Transmit users' copies of the sent/outgoing files and screenshots to the server
It is possible to monitor users' sent files content to the internet as well as files copied to removable drives or folders selected by the user on the page "File operations" (it is mainly needed to prevent important information leakage). In such case these files or its parts (if files are big) will be saved on the server and it will be possible to review them through **"Sending files"** and **"File operations"** (clicking the corresponding link).
This option has sense only if **monitoring of file operations and/or sent files** mode is enabled respectively.
This option is also necessary for monitoring **incoming/outgoing emails**, **screenshots**, **voice conversations** and may be other reports in the future.

Interested file types
Specify file masks separated by comma which will be transferred to the server. It is required to indicate *.* for all files.

Maximum file size and its part for retention
If required file is less then selected size it will be sent completely otherwise only its part will be sent (first N-bytes) or empty file (it depends on the option **"Send empty files if the size is exceeded max"**). The bigger selected size the bigger the load on the network. So it is recommended not to select too big number!
In the current version max size is limited to **512 MB!**
Note: this option is ignored when sending screenshots to the server!

Do not process if the empty space is less then N-megabytes
Shadow copy won't be performed if empty space on the user's PC is not enough on the system disk (usually C:).

See also server settings tab "Monitoring: Shadow copy"

6.2.4.15. Monitoring - Black box

In this mode all user actions (video from the screen and sounds) will be stored in local files on his machine in encrypted form.
File storage settings are made on this page.
Each file is a record of **one hour** duration in mp4 format.

Record video from the screen
The video is recorded from the currently active monitor (on which the mouse cursor). An important parameter for video recording is **interval between frames** - with larger values files are smaller and less CPU-load on the client machines, and vice versa. The minimum value is 1 second, the maximum value is 3600 seconds.
The average size of the hour-duration file with the default settings is usually **near 300 MB**.

Record audio from the microphone
Add continuous recording from the microphone (used system-default microphone of the client machine).

Record audio from the speakers
Add continuous recording from the speakers of the client machine.
Attention! On some sound cards, sometimes when this option is enabled, the situation may occur of "looping" sounds (or silence) after the completion playing of some other sounds. The situation ends after the any sound played again. If this is often case, then it is better to disable this option.

Attention! All of this "black box" functionality will not work if the **Windows Media Foundation** is not installed on the system. By default, it is not installed on all server OS'es, as well as on older Windows XP operating systems.

6.2.4.16. Monitoring - Geolocation

The option of sending data about the location of the computers makes sense for laptops with Windows 8 and higher, which can change their locations.

Attention! When enabled on the client machines, the geolocation icon in the system tray may appear for a short time!

If there is a need to determine the external (public) IP, as well as the city/country based on it, then you can enable access to an external server. By default, the server used (ifconfig.co) is publicly accessible and supports http/https access. However, it might make sense to place this functionality on your own public server, in this case all the necessary installation information can be found on the website ifconfig.co
If it is necessary to use a proxy to access the Internet from client machines, then the settings must be made on this page.

6.2.4.17. Monitoring - Autorecording

The most important options in this tab:

Perform permanent audio recording from the microphones
In case this option is enabled audio recordings from clients' computers will be sent to server.
Warning! When option is enabled at **MacOS**-machines, a one-time warning about microphone recording will be displayed, which user can accept or decline. This fact allows to detect client software!

The new file every N minutes
Allow to split files for more convenient analysis (from 1 to 60 minutes).

Threshold
If the sound level is greater than the background noise level by at least the selected number of decibels, then only in this case is a further analysis of the sound for the presence of speech will performed. The smaller this number, the higher sensitivity (and vice versa).

See also server settings tab "Monitoring: Autorecording"

Allow speech to text recognition for BOSS-Online
Attention for Google engine: by enabling this option you automatically agree that employees' voice conversations (at the time of the corresponding request from the BOSS-Online) will be transferred to the external servers of Google company in the real time (via http/https protocols) for analysis and processing.
You need to study and accept Google privacy policy: https://policies.google.com/privacy
Also enabling this option you agree to use it only in legit cases as it is stated in the licence agreement for this product (with its installation).
Attention for own neural network server: voice traffic from client machines will go to the server configured here.
Common note: an outgoing traffic on the employee's computer will be about 0.25 Mb/s while performing the processing.
Attention! In case in your organization it is required to use **proxy** for Internet access from clients computers then required settings have to be done in the tab **"Common settings" for computer**!

6.2.4.18. Restrictions

The most important options in this tab:

Prohibit use of USB-devices
If this option is enabled users won't be able to work with selected USB-devices. A message will be displayed in the tray about the impossibility of using device, and also event will be generated if enabled.

Whitelist of USB-devices
You can set exceptions when blocking USB devices, in this case you need to add the USB-path of device (each per new line). You can find these values in the "File operations" report (when copying files to a flash drive), as well as in the "Events: user" report (for flash drive insertion / device blocking events, but only in case these events are enabled at this settings tab).
List example:

```
USB\VID_0952&PID_11D4\MSFT2546493643654
USB\VID_AD07&PID_0316\A117000036428772623
```

Ignore sticky keys (activity imitation)
When you enable this option and hold down a key on the keyboard for a long time, its sticking will ignored, this prevents the ability to simulate an activity.

"Black" and "white" lists of applications
You can specify application list for the prohibition/permission of execution, respectively (**for Linux only "black" list is supported!**).
Each application should be specified from a new line and represent either the full path to the executable file, or only the executable file name itself without a path, or application description in Windows.
You can use environment variables (Windows-only).
Examples:

```
%WinDir%\Syswow64\regedit.exe
bad_app.exe
Microsoft Office Word
/usr/bin/mc
mc
```

If the application should be forbidden, a tray message will appear on the user's machine, and the application will be closed.
Windows: it's important to note that only applications **with windows** fall under control, but hidden system applications - do not!

Prevent commands execution in Linux terminal
You must specify a list of commands (each on a new line) that will be prohibited from running in the **graphical** Linux terminal. There is no support for non-graphical sessions (console) in this case!
See also **"Events"** tab group.
Attention! You can specify special pseudo-command **kill_agent** to prohibit the most common methods of deleting the client part of the complex.
Examples:

```
sudo vi -c ':!/bin/sh' /dev/null
sudo openvpn --config "$LFILE"
nc -l -p $LPORT -e /bin/sh
kill_agent
```

See also computer settings tab "Restrictions"

6.2.4.19. Threats

It is possible to set up threats sensitive to the program.
Each threat must be written with the new line!
The threat may be: **entry to a website**, **running programs**, **typed words**.
It is possible to specify:
- full or partial website address,
- website heading (or its part),
- program heading (or its part),
- EXE file program name (if the path has to be specified it is require only with environmental variable such as %variable%),
- program description (it may be partial),
- single word (not a phrase!), at the same time if symbol **tilde "~"** is specified at beginning this identified **inaccurate words comparison** algorithm will be used.

Warning! Language morphology features are works only for **Russian** and **English** languages! Therefore, do not use the **tilde "~"** symbol before the words from other languages!
- templates: **@CREDITCARD@** (bank card number input), **@PHONE@** (phone number input), **@EMAIL@** (e-mail address input)
- own templates based on **regular expressions**

Response to threats is set up in the settings tab **"Events"**.

6.2.4.20. DLP - Common settings

On this page it is possible to set up **DLP (data leak prevention)** in documents/images/voice.

If the user performs one of selected actions with the certain objects **in the inner text of which** there is one or several coincidence from the rules list then the event will be notified. This event may be recorded to the report "Events" and an immediate push-notification will appear in BOSS-Online. The events are set up in the tab **"Events"**.
It is also possible to allow or forbid certain activities, and/or perform document classification.

The following file formats are currently supported when extracting text from documents: **docx, xlsx, pptx, odt, sxw, ods, odp, doc, xls, ppt, rtf, csv, txt, pdf, zip, jpg, png, gif, tif**.
Please note that document analysis (especially large archives or OCR text recognition on images) can be time-consuming, and user operations may be blocked during this period. To indicate to the user that document analysis is currently in progress, there is an option **"Show waiting indicator after N-msec"**. This option allows you to specify the time in milliseconds after the analysis process begins for a small window to appear on the screen and disappear immediately after completion. If you specify a time of **-1** msec, the window will never appear!

Attention! It is required that corresponding monitoring options **must be enabled** for DLP processing on the homonym settings tabs (for example, clipboard monitoring, file operations etc.)

Attention! DLP processing is oriented on file output but not on the input. So, for example, such action as copying files from removable drives won't be recorded!

Attention! In the current version there is no FTP-file transfer blocking. Instead, you can completely block FTP traffic in the settings!

Attention! It is worth mentioning that any DLP may be skipped so the software suit cannot guarantee prevention from leakage in all possible cases.

Attention! Parsing **.pdf** files will not work on terminal servers.

Attention! For **block/classify printing** you need to turn on option "Intercept printing inside processes" at this settings tab.

The **"Perform classification"** options will only work if the corresponding DLP option is enabled!
When enabled, the document is sent to the server for classification into categories. The categories themselves are configured on this page.
The classification result can be viewed in the **"Files Classification"** report.

When the **"Turn on DLP for periodic screenshots"** option is enabled, each screenshot (settings here) will be analyzed when OCR here is enabled, and if text from the sensitivity block is found in the text on the screen, a corresponding event will be generated and the screen will be optionally locked.
It is important to note that enabling this option can significantly increase the server load, so it should be used with great caution!

If the option **"Send shadow copies of documents only if DLP analysis is triggered"** is enabled, it will not be possible to download the document through reports in BOSS-Offline if a DLP-event has not been triggered in it. This allows you to save network traffic and server disk space if you are interested in shadow copies of important documents only.

See also "Sending files"

6.2.4.21. DLP - Quarantine

Move blocked files to quarantine
If the option is enabled and sending/copying the file was blocked in accordance with the DLP-settings, the file will be moved to the local "quarantine" storage on the client machine.
See quarantine settings here.

6.2.4.22. DLP - Rules

Here you can configure the rules for DLP-triggering.
For general settings and their descriptions, see here.

In case some important company files change seldom or do not change at all, it makes sense to grab "file hashes" and not to fill the sensitivity list manually. For details see "File hashes".

It is also possible to **mark important documents using hidden marks** (you have to use special utility), to protect them or control sending of these documents (or their parts) outside the company.

How to fill in the block "sensitivity":
- each new elements of the list must start **with the new line**;
- if an accurate coincidence is required it is possible to specify a word or a phrase without prefixes;
- if **inaccurate word search** is required it is possible to specify single words (**not phrase!**) with prefix "~";
Warning! Language morphology features are works only for **Russian** and **English** languages! Therefore, do not use the **tilde "~"** symbol before the words from other languages!
- it is possible to use following templates: **@CREDITCARD@** (bank card number), **@PHONE@** (phone number), **@EMAIL@** (e-mail-address), **@FACE@** (face photo, see also "DLP: OCR" and "OCR on server");
- own templates based on **regular expressions**;
- **marks**, with which documents can be marked (the mark must be enclosed between the characters '#': #mylabel123#, **only English alphabet letters and numbers are allowed, case matters**!).

There are also situations when different elements of the "sensitivity" block require different reactions. For example, if less than five passport numbers are found in a document, then do not consider this as a threat at all and do not generate an event, but allow blocking of file transfer only if there are 50 passport numbers or more. But at the same time, the situation should be different for credit card numbers: triggering and blocking when at least one is found.
For such cases, it is possible to enter threshold values for each list element (two numbers separated by commas after the name: the first is the detection threshold, the second is the blocking threshold).
Please note that blocking in this case will only occur if the corresponding blocking settings are enabled in the settings at this page!
An example for the above case (assuming that the regular expression @passport@ is created):
@passport@,5,50
@CREDITCARD@,1,1
If threshold values are not specified, **(1,1) is assumed as the default**.
For **digital document marks** this option has no meaning and implies (1,1).

If you need to prohibit sending files **by format, and not by text inside the file**, we recommend that you refer to the settings "DLP by file formats"

Option **"Search at most N-matches for each regular expression"**: introduced for optimization, so as not to waste time searching for expressions if a certain number of them have already been found. Specify 0 to remove restrictions.

Additional rules for DLP-triggers
Additional DLP triggers are present in this block.
For file group-oriented values, **-1** can be set to disable the option.
"Additional" means that these rules will **supplement** the sensitivity list, but will not overlap it in an "AND" manner.
It should also be noted that the option for the number of files output during copy operations in Explorer may not always work, since Windows Explorer often breaks the copy operation into copying one file at a time, and accordingly, it is not always possible to know the original number of selected files!

6.2.4.23. DLP - By file formats

There are situations when DLP analysis does not require extracting text from a document and analyzing it for occurrences (see sensitivity block), but rather looking at the file format as a whole.
For example, prohibiting CAD drawing files from being sent or much more. In this case, it is convenient to enable the necessary formats on this tab.
As a result of DLP triggering in this case, the **"Events: User"** report will show the DLP event type **"by_formats"**.
Note: This analysis is not sensitive to the file extension (it can be any), detection occurs by signatures, headers, and other features, however, for some proprietary formats, format recognition is only possible by file extension.

6.2.4.24. DLP - OCR

Use text recognition on images (OCR)
If this option is enabled, then during DLP operations, if there are individual images or images inside document files, the image will be converted into text for subsequent text DLP analysis.
Basic DLP settings on the client are made on this page, and the OCR process itself occurs on the server, settings here.

Maximum wait time per document in seconds
It is important to understand that the OCR process can take a significant amount of time, so sometimes it makes sense to set a maximum wait time (for the entire document).
For example, if the server is under heavy load and the timeout expires, the OCR result will be returned as **"OCR timeout"**, which you can optionally use in DLP sensitivity lists. The user will then be able to resend the file (if sending blocking is configured).
If sensitivity to the phrase **"OCR timeout"** is not set, then in the case of a timeout, this will simply mean that not all images in a document with graphic images will be recognized and text extraction will be incomplete.
To display the document analysis process to the user, a small window will appear on the screen. Settings are configured on this page.

Minimum and maximum image size in bytes
For optimization, you can specify a range of image sizes for popular graphic formats in bytes, so as not to waste OCR time on obviously "useless" images.

Enable caching on clients
This saves time by eliminating the need to send previously successfully OCR-ed images to the server. This is especially useful when an employee submits the same document multiple times. The images themselves are not cached on the client, only their short hashes are stored.

6.2.4.25. Critical apps-sites

If your company uses applications or sites, copying or photographing data from which is highly undesirable, then it makes sense to use this protection.
In the **list of conditions for apps/sites** it is necessary to setup the trigger conditions (see description **here**), and then select restrictions/actions.
Attention! The critical applications will also automatically include those in which documents were opened for which a **DLP trigger** was performed with the **"Turn on DLP for documents reading"** option enabled.
When a user starts an app/site from the list, then restrictions/actions from the marked ones will occur. Also, when a ban occurs, it will generate **an event**.

Do not show window content during screencasting
When this option is enabled, any programs or browsers that continuously capture or take screenshots will not see or broadcast the contents of the critical application window. Instead of the window content there will be a black rectangle. This option also affects the capture of screenshots by the complex itself, i.e. it will not be possible to get screenshots of these windows either.

Disable PrintScreen
Disables PrintScreen, Alt+PrintScreen, ...

Disable clipboard
Full restriction of clipboard usage with cleanup.

Put a watermark on the screen
The ability to overlay translucent text over the entire screen in the form of a domain name and user name. These texts do not interfere with working with applications, but reduce the employee's desire to take a photo of the screen in this case.
Font format described below:
FontName,FontSize,FontWeight,R,G,B
FontName - font family name;
FontSize - font size;
FontWeight - font weight (from 100 to 900);
R,G,B - color components (from 0 to 255 each one), transparency in this case is determined by the overall brightness of the color (i.e. closer to black - more transparent text, and closer to 255 - opaque).

Turn on webcam LED-indicator
Simply turning on webcam LED-indicator without recording video.

Lock workstation in case webcam is busy
If the webcam is busy by some other application at the time when a critical application/site is active, then locking workstation will occur.

Lock workstation in case webcam is closed
If the webcam is closed at the time when a critical application/site is active, then locking workstation will occur.

Lock workstation upon attempt to take screen photo
If someone tries to take a photo of the screen with a smartphone when a critical application/site is active, then locking workstation will occur.
For this option to work, you need to make settings on **this page**.
You can also adjust the recognition **threshold** in percent (from 50 to 99). The lower the value, the more false positives can be.

Ignore lack of connection to the server
To track attempts to take photos of the screen, a permanent connection of client machines with the server of the complex is required.
If there is no connection to the server and the option "Lock workstation upon attempt to take screen photo" is enabled when a critical application/site is active, then the default blocking will be performed. However, if you enable this option, no action will occur.

Debug mode: do not perform Lock
When this option is enabled, in case of an event that requires workstation locking, the lock itself will not be performed, but an event will be sent to the server, and all windows of critical applications/sites will be minimized, and message will be displayed to the user.

Quiet mode: without Lock and popups
When this option is enabled, if an event occurs that requires the workstation to be locked (Lock), there will be no locking, but an event will be sent to the server, windows of critical applications/sites will not be minimized, and no messages will be displayed to the user.

Attention! The list of conditions for apps/sites is not multi-line! Thus, if you need to describe several conditions, use the **OR** connector between them, and not try to insert a newline.

6.2.4.26. Atypical behavior

In this tab it is possible to trace employee's atypical behavior based on number of criteria.
If such behaviour happens an event will be generated in correspondence with the settings in the tab **"Events"**.
Monitoring interval in this option one can specify the survaillance time during which all criteria, set up later, are counted.
If during this time any of this criteria exceeds indicated value in the settings an event will happen.
If a value **0** is indicated then this criterion won't be used.
ShadowCopy file is a file that corresponds to the type of file (file extension) which is set up in the tab **"Shadow copy"**.
"Selected folders" these are such folders which are set up in the tab **"File operations"**.

Attention! It is required to enable corresponding settings in the following tabs **"Shadow copy"**, **"File operations"**, **"lipboard"**, **"Sending files"**, **"Applications/sites"** for this option to work.

6.2.4.27. Events

It is possible to set up the capability of saving different events into the report "Events" of the database.
To setup notifications to managers see **server** page "Events".

6.2.4.28. Events (video)

For most events(*) (turn on and off in the tab **"Events"**) the current screenshot of the user's screen is also taken, which is transmitted to the server along with the event.
It is possible to replace a screenshot by video from the user's screen.
This requires:
- mark the events you need to record video(*) in this tab;
- make sure these events are enabled (see tab **"Events"**);
- turn on option **"Record video of events"**;
- configure option **"Interval between frames"** (from 1 to 60 sec);
- configure option **"Video duration"** (from 5 to 600 sec).

Note: since video recording takes time, it will not become available in the **"Events"** report earlier than after **"Video duration"** seconds!

Note: video files are transferred as regular shadow-copy files, so make sure in the tab "Shadow copy" set sufficient max file size (otherwise the video file will be truncated). For example, at average values, a minute video file usually takes no more than 5-6 MB.

(*) the list of events for which screenshots/videos are saved depends on the version of the complex and may change.

6.2.4.29. Events (extra)

When a series of events(*) occur (toggled on and off at the **"Events"** tab) it is possible to use additional options. For this, it is necessary to check resp. events at this tab and configure the options you need.

Note: You also need to make sure these events are enabled (at the **"Events"** tab).

(*) list of events for which additional options are supported depends on the version of the complex and may change.

Lock workstation
The computer will be locked with the standard system lock screen followed by a login password.

Notify message text
Optionally, you can specify the text that will be displayed in a tooltip or system message when an event occurs.

Requiring textual justification for an action
If the event involves a restrict, then when the option is enabled, the user will be prompted for a text justification for the action.
Next, the user can choose not to enter (followed by a prohibition of the action), or enter a rationale (the action will be allowed). It will be possible to view text justifications in the report **"Events: user"**.

6.2.4.30. Outsourcing

On this page it is possible to allow an employee to enable or disable his or her personal monitoring by himself or herself. This option may be useful while working in the "outsourcing" mode on the employee's personal computer.
When this mode is enabled an icon appears in the tray through which it possible to enable or disable monitoring.

6.2.4.31. 2FA (employee)

It is possible to enable two-factor authentication (2FA) on client machines when various events occur.
You have to select a 2FA method and one or more events.

Method: IMEI code of the smartphone
This method does not use a server call and works only within the client machine.
The user will be asked to enter the IMEI code of the phone, and then use parts of this IMEI code as OTP codes.
This method has low reliability, but is quite simple and does not require access to the server or installation of any additional apps on smartphones.

Method : SMS/e-mail/Telegram
These methods use a call to the server, then server initiates the sending of OTP codes via the selected channel.
It is important to make preliminary settings on the corresponding pages: e-mail, SMS, Telegram

Enable at LogOn
The OTP code will be requested each time the user logs into the system.

Enable when unlock or run as administrator
The OTP code will be requested each time user unlocks the screen or after running a program that requires administrator rights.

Enable when critical application/site starts
The OTP code will be requested immediately after each launch of a critical application or website. See settings here.

Turn on periodically
The OTP code will be requested periodically with the specified period in minutes.

First start: when 2FA is first activated on a client machine, the user will be prompted to enter initial information about the code delivery channel, and on subsequent launches, the 2FA code request itself will be performed!

Attention! For **emergency screen unlock** and reset of user 2FA settings, you need to use the function in BOSS-Online *"Admin functions (user)" - "Reset 2FA"*

Attention! 2FA will not work in Safe Mode!

Important! It is not recommended to experiment with 2FA in the case where the client and server are installed on the same machine, as there may be a potential problem with unlocking the screen due to incorrect settings or the inability to receive an OTP code!

6.2.4.32. Quarantine-files

This page configures local storage of files on the client machine in encrypted form.
Files can come from various sources. In the current version this files are from **"Black box"** and blocked by **DLP-policies** (when **quarantine** is enabled).

Path to the folder to save
This path can contain environment variables for user and computer (e.g., %USERPROFILE% is "C:\Users\user_name\"). You can also use network paths, however this extremely not recommended due to possible performance problems!
Attention! Root paths like C:\, D:\ are not allowed here!
In the LogOff state, the value of %USERPROFILE% is usually "C:\Users\Default\".

Do not perform, if free space is less than
If there is less than N-megabytes of free space on the disk where the files are stored, the files will not be saved.

Recorded data max storage time
This is a retrospective for saving of old records.

Key for files encryption
It is recommended to encrypt files and not leave this field blank (AES-256 encryption is used).
Files have unreadable name and **.dump** extension.
After decrypting the file name becomes readable (original) and it becomes open for the applications.
If the encryption key was not used, then after decryption, the file name is simply converted into a readable one.
To decrypt it is necessary to use the utility **dumpdecrypt** with the same key.
Attention! If you enter the wrong key, the file will be corrupted and can not be restored!

Note: It is quite convenient to use the **"Files Browser"** function in BOSS-Online (menu "Admin-functions (computer)") to download quarantine files from a remote client machine.

6.2.5. Groups

Users and computers groups have to be used if you **don't want clients' settings to be the same for all** computers/users. And it is required to personalize individual settings for certain users/computers.
In such case it is necessary to link these groups with created settings profiles. To create settings profiles it is required to click on **pop-down menu** near buttons "For computers", "For users".

For example: it is required for certain users to set up screen shots capture frequency one time in a minute and for the rest - one time in 10 minutes.
In such case press the settings key button "For users" and set up screen shots frequency in the usual way one time in ten minutes.
Then press "Profile 1" in the pop-down menu near the settings key button "For users" (as an example) and in this profile settings you can set up screen shots frequency one time in one minute.
Then press the key button "Groups" and match required users with profile 1.

Attention! Only settings that you have changed in this profile will be saved for profiles. Other settings are taken from the basic. For example, if in profile 1 you have changed only screen shots frequency and later changed file size of the shadow copy in the basic settings then the file size of the shadow copy will automatically be taken from basic settings for profile 1!

Note: if the profile destination is "empty" basic settings will be used (without profiles).

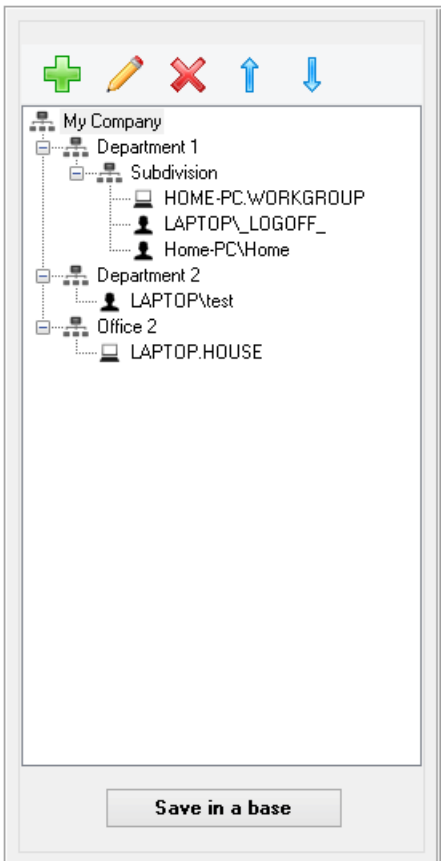
Note: in this window users and computers lists are taken from the database so they may be empty just after the software suite installation. It is necessary to wait 5-10 minutes till the data will start getting into the database from clients' computers.

6.3. Company structure

On this page it is possible to create company hierarchical structure optionally identifying departments, subdivisions and etc. Users and computers can be added to each department which haven't been distributed yet. The lists with users/computers itself (that are in the right colon) will be available only after receiving first monitoring data into the database (e.g. in 5-10 min after first installation of the client apps on users' computers).
There is no need to distribute all. Each user or computer may be either in the hierarchy or non distributed into the list. It can not be in both simultaneously!
Hierarchy is used while been displaying in BOSS-Online, BOSS-Offline. It is very convenient assigning access rights for directors to their departments.

Do not forget to push **"Save in a base"** to apply new settings!

Attention! Only **database administartor** has rights to save the structure!

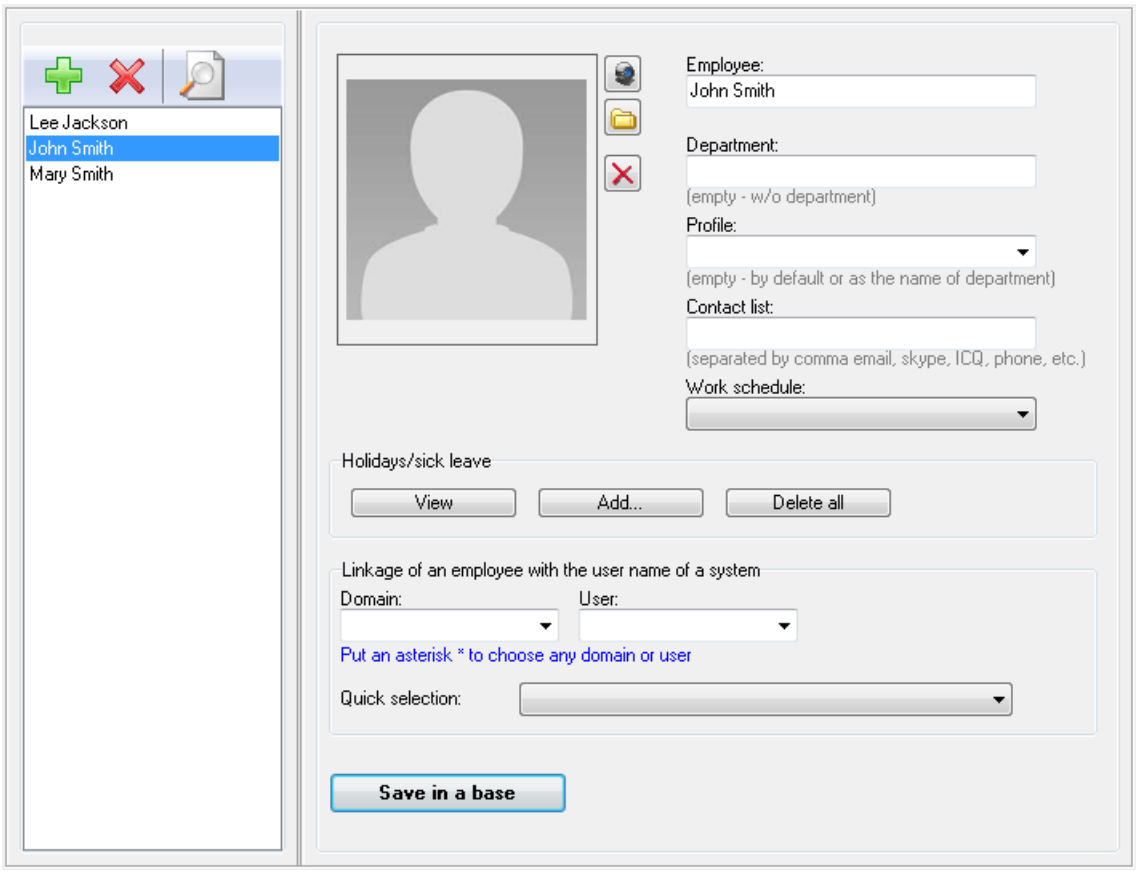


6.4. Work schedules

It is possible to set personal working day schedules for each employee or employee groups. You need to assign personal work schedule at the page **"Dossier"**.
If an individual work schedule is not assigned, then the data from the default work schedule will be used, but if it not set, data from the next page: **"Work schedule"** (with automatic generation of reports) or from the **BOSS-Offline interface** (with manual reports building).
Work schedule data is used in some BOSS-Offline reports to calculate absenteeism, latenesses, and other characteristics.

6.5. Dossier of employees

On this page it is possible to create a profile for each employee optionally. In such way you can see employees' surnames instead of system user names in BOSS-Online and BOSS-Offline.



Department
It is used to sort and display in the BOSS-Offline/BOSS-Online lists.

Profile for risk analyzer
It is needed for report **Risk analyzer**. One can correlate an employee with a certain profile for analyzer.
If it is not done and the field remains **empty** when building the report the profile will be chosen in the following order:
- if the profile is found and its name **coincide with employee's department** then it will be used;
- **"by default" profile**.

Contact list
It is possible to specify the list with different employees contacts separated by comma. It is used when the report "Contacts" is built and reports are sent employees themselves.

Work schedule
see here

Holidays/sick leave
The ability to set personal vacation/holidays or sick leave days so absences on these days won't considered truancy in the reports.

Linkage of an employee with the user name of a system
It is possible to put "*" (without quotation marks) for domain or user for this field to be ignored.

Don't forget to press **"Save in a base"** to apply new settings!

6.6. Sync with AD

Synchronization is defined as automatic maintenance of all staff's and company's data integrity that are saved in the software suite configuration in the current state. Everything is designed in such way that administrators do not need to do double work in Active Directory - there will be no need to change this data in suite configuration. Examples: An employee leave the job or added new one, company structure has been changed, a manager has now more subordinates, etc.
The administrator sets up automatic synchronization once and after there will be no need for administrator to visit settings tabs "Database users", "Company structure", "Dossier of employees". By setting up synchronization once everything will be done automatically (by receiving data from Active Directory and writing them down into suite configuration database).

Important:
- Synchronization is only possible when using **Microsoft SQL Server** (without additional settings) or **PostgreSQL** (**to synchronize rights, you need advanced settings**).
- The administrator may perform synchronization settings as well as synchronization itself from his computer which is join or not join to the company's domain.
- If there are several administrators in the company each of them can work on his computer with these settings.
- Logging into the Global Settings program can be performed within DB administrator account or by a specially created user through the "Utilities" main menu item.
- An account is required in a domain that has read permissions from Active Directory.
- If during synchronization you need to synchronize client installations, then the machine used for synchronization must be joined to the domain, and also account in the domain must additionally have rights to copy files, write to the registry and start services on the remote machines within domain.
- For remote access to the domain controller, you must open an LDAP port on it (usually TCP 636 for secure LDAPS, or 389 for unsecured connection).
- During the synchronization of the company hierarchy, all manual changes made earlier in this section will be deleted!
- During the synchronization of access rights, all logins from AD (not SQL-logins) previously added manually in this section will be deleted!
- During the synchronization of employees dossiers, all previously manually added in this section will be deleted!
- **Microsoft SQL Server**: to be able to login into BOSS with domain accounts, PC with the complex server and PC with the SQL-server must be joined to the domain!

"Login" tab

If the Windows user used to execute global settings program does not have needed rights in the domain for synchronization, you can specify the domain logon settings in this tab.

"Domains" tab

The list of company's domains is specified here that need to be synchronized.
Trust must be established between domains.
Domain's controller is not required for indication (required only for remote access).
Software suite server may be only one for all domains or different (in case of using several servers). For rules on filling out this field, see here.

"Objects" tab

Groups, OU or single computers/users are specified in this tab for the next synchronization types:

1) Clients' installs synchronization - groups/computers are specified where client app has to be installed. So in the process of synchronization client app is installed on those computers where it is not installed before. It is also possible to delete clients' app automatically although settings are performed in the settings tab **"Common settings"** for computer. The option clients' app **automatic update** is also there.

2) Synchronization of selected monitoring - groups/users are specified for which selective monitoring will be performed. Thus, list of users on this page will not need to be filled in manually. During synchronization the list will be updated automatically!

3) Manager' rights synchronization - groups/users are specified in one out of next roles.
Managers' **roles** :
"Supervisor" - reports about all company's staff are accessible for this director (all domains).
"Super user" - access only to reports about staff of current domain.
"User" - rights are set manually. After synchronization in the settings tab "Database users" it is necessary to choose departments or staff manually that will be monitored by this manager.
"Manager" - access to reports about himself and his staff. What does it mean? If **"Manager"** is set in AD for some staff then the field **directReports** will appear for this manager. It will be used to set access rights. E.g. this manager can monitor **only his subordinates and their subordinates (and so on recursively on subordination hierarchy below)**.
Sometimes it is convenient to synchronize the **"Manager"** role using reverse search logic, i.e. do not specify specific managers, but search for them through all domain users by analyzing a certain AD attribute (usually **manager**) of each employee (i.e. from employee to his manager). In this case you need to select the type **"AD-attribute for "Manager" role"** and specify the desired AD attribute (usually **manager**). If it is allowed to have **several managers for a single employee** in the AD structure, you need to add each attribute as a separate object.
Role priorities: if one manager has few roles at the same time the priorities are set in the above mentioned order.
In the synchronization process data in the tab **"Database users"** are filled.

Attention! Do not use standard groups **"Domain computers"** and **"Domain users"**! Specify domain itself in the same format (DC=...,DC=...) instead.

"Profiles" tab

Same as "Objects" tab, but specify only groups, OU or single computers/users to link them with cliets' profile settings. See section **"Groups"** in suite settings.
This tab serves for synchronization with Active Directory, istead of fill in section **"Groups"** in suite settings manually.
See also the "delete before sync" option in the **"Settings"** tab!

"Departments" tab

In big companies sometimes it is required to perform synchronization only with chosen departments/subdivisions in AD and not with its full hierarchy. In such case it is necessary to choose needed AD departments in this tab (chosen department will automatically include all departments of the lower level!). Whether this list is empty then synchronization will be done for all domain(s) hierarchy completely.

"Client machines" tab

It is possible to see the list of workstations with already installed clients' apps and those workstations where clients' app has to be installed.
There is an option to choose and install clients' apps manually.
Remote installation is performed in this way.

"Settings" tab

Synchronization parameters are set up here:
"Ignore disabled accounts" - if computer's account or AD user is disabled then synchronization won't run for it.
"Ping machines before client setup" - recommended to make installation faster (if computers are turned off).
"Ping timeout" - time in msec waiting for response from the client machines. If there are frequent 11010 errors in the logs when machines are turned on, then it makes sense to increase this value.
"Company title" - used with hierarchy synchronization as its upper level.
"Build groups-based hierarchy" - ignore the actual location of computers/users in the Active Directory hierarchy and instead build a hierarchy using the groups in which the computers/users are located.
"Dossiers sync options" - specify AD attributes names for profile synchronization.
"Default base rights for roles (rights sync)" - optionally you can set the basic rights by default when synchronizing rights for a particular role. To do this, create a database user with an SQL-login (not a Windows-login!) on the tab "Database users" and set the basic rights you need, next select or enter its login in acc. field for the desired role on this page. It is important to note that these rights will be assigned to the database user when it is first created during synchronization, but not subsequent updates (if it has already been created) during the next synchronization cycles!
"Delete before synchronization" (for the clients settings profiles) - By default, before synchronizing client settings profiles, all user-profile and computer-profile mappings already set in the database are deleted and then synchronization with the addition to the database is carried out. In such scenario, manually set mappings for machines and users outside the domain (as an example) will be removed every time after the successfull synchronization with the domain. To solve the problem, specify the masks for users/computers separated by commas, which should be removed before synchronization. For example, you want to update only the mappings for the users/computers of the domain named "COMPANY" when synchronizing, and you are going to configure the rest manually, in this case, you need to specify in the config line: ***.COMPANY,COMPANY*** (for the computer, the format is NAME.DOMAIN, and for the user DOMAIN\NAME).
To specify exceptions, you should use the "exclamation mark" symbol (example: *.COMPANY,!PC01.COMPANY,!PC02.COMPANY)
"Log cleanup settings" - log clearance also happens during synchronization process.

"Sync" tab

Synchronization may be performed manually (new console process will be created) or to add the task to Windows **job scheduler** for automatic synchronization according to the timetable.
Important: the task in the planner must be performed from **Windows current user's account**!

"Log" tab

It is possible to look through the automatic and manual synchronization results as well as to trace settings changes.

After successful synchronization it will be possible to **change manually** the following parameters that are not liable to synchronization:
- in the tab "Database users" all users with SQL logins (not Windows logins).
- in the tab "Database users" for users with Windows logins "Basic rights".
- in the tab "Database users" for users with Windows logins "Additional restrictions" for roles "Users".
- in the tab "Dossier of employees" all users profile that are not included into domain(s).
- in the tab "Dossier of employees" parameter "Profile".

How to set up automatic reports sending to the managers/employees

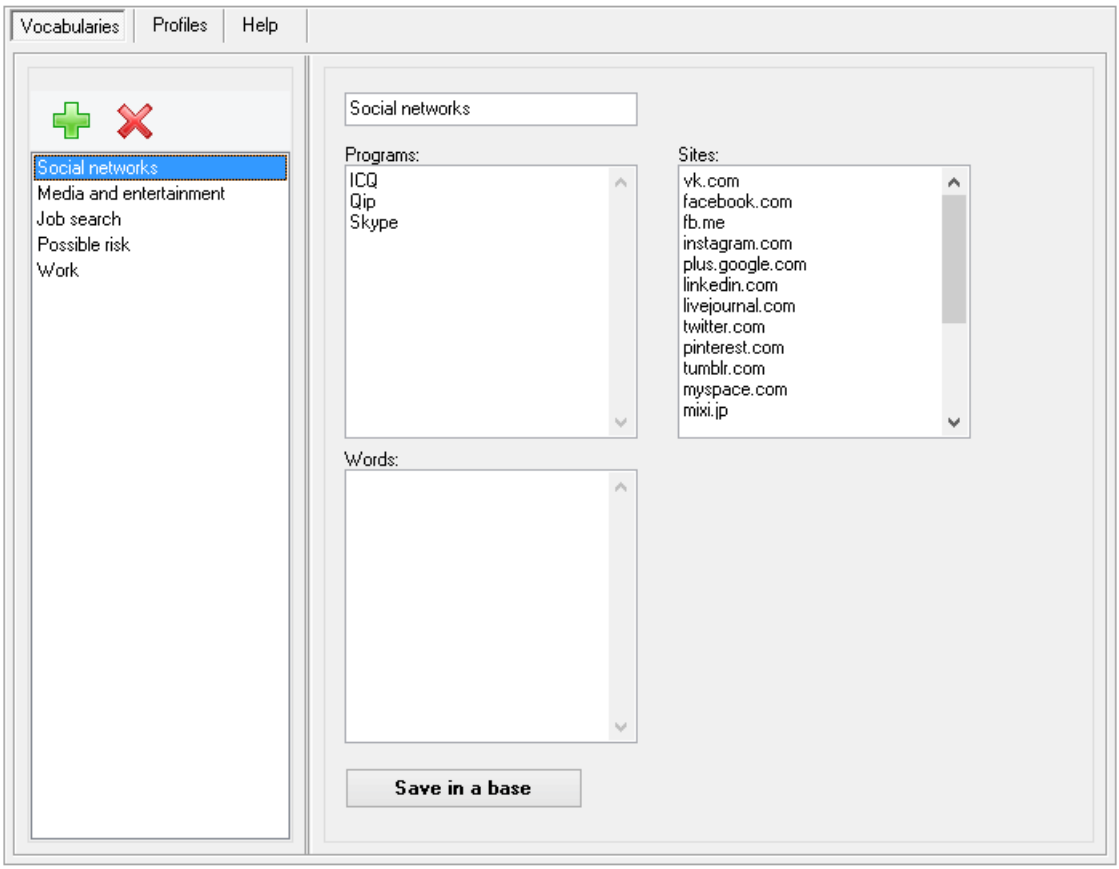
After successful synchronization it is possible to set up managers' rights for reports sending automatically (tab **"Database users"**) if required.
Then these managers have to login into their **"Personal cabinet"** at least once (via web-interface BOSS) and enable reports auto-generator there.

It is required to specify e-mail address in the AD personal card for staff to be able to receive reports on e-mail **about their own activities**. It is also necessary to enable corresponding settings in their manager's rights (**It is preferable to enable this permission for the manager from upper hierarchy subordination level and not for many lower managers**).
Reports generator options **must be set up** in the server settings (**"Reports generator"** section).

6.7. Risk analyzer

"Risk and productivity analyzer" is an intellectual tool which automatically detects potential risks for company in the everyday staff's activities. It can be passing critically important data to the rivals, looking for a new working place (job), productivity decrease etc. Risk analyzer performs scanning of all gathered information about staff's activities and shows which risks certain employee has as well as based on which events. Within the staff's productivity analysis this tool shows how exactly employees spend their working time and it gives opportunity to evaluate efficacy of a certain activities. The analyser is accessible via BOSS-Offline.

Vocabularies:



The vocabulary itself can not be evaluated as "useful" of "harmful" activity as it depends to which employee it will be applied to. For example, acidities in social networks for marketing specialist are not the same as for accountant!
"Sensitivity lists" are set up in each dictionary. Each element must be written down **with a new line**!
Here belongs:

1) Programs. Specify full program name in such way that it will reflected either in the Windows task manager (column "Description"), or in the report "Programs" (in the report description is specified in the quotation marks above window heading). Also full path to the program executable is allowed (it is necessary also to specify it exactly in the same way as in the report "Programs") or just the executable itself without a path (but with a backslash as the first character).
Examples:
Microsoft Office Word
Photoshop
%ProgramFiles% (x86)\Google\Chrome\Application\chrome.exe
\winword.exe

2) Websites. Specify only domains and sub-domains **without prefixes http://, www. and URI**. In case domain is specified of an upper level then its sub-domains will also considered (if these sub-domains are not indicated separately).
Special strings of the form **%variable%** are used for implicit searching in the built-in internal dictionary, and only if searching in the domains entered here was unsuccessful.
Examples:
facebook.com
msdn.microsoft.com

3) Words. Specify single words (**not phrases!**) which will be sensitive for search. If tilde "~" is put in front of the word then **the word search will be inaccurate** (taking into account typographic errors and language peculiarities).
Don't forget to specify each word **with a new line!**
Examples:
~manager
job

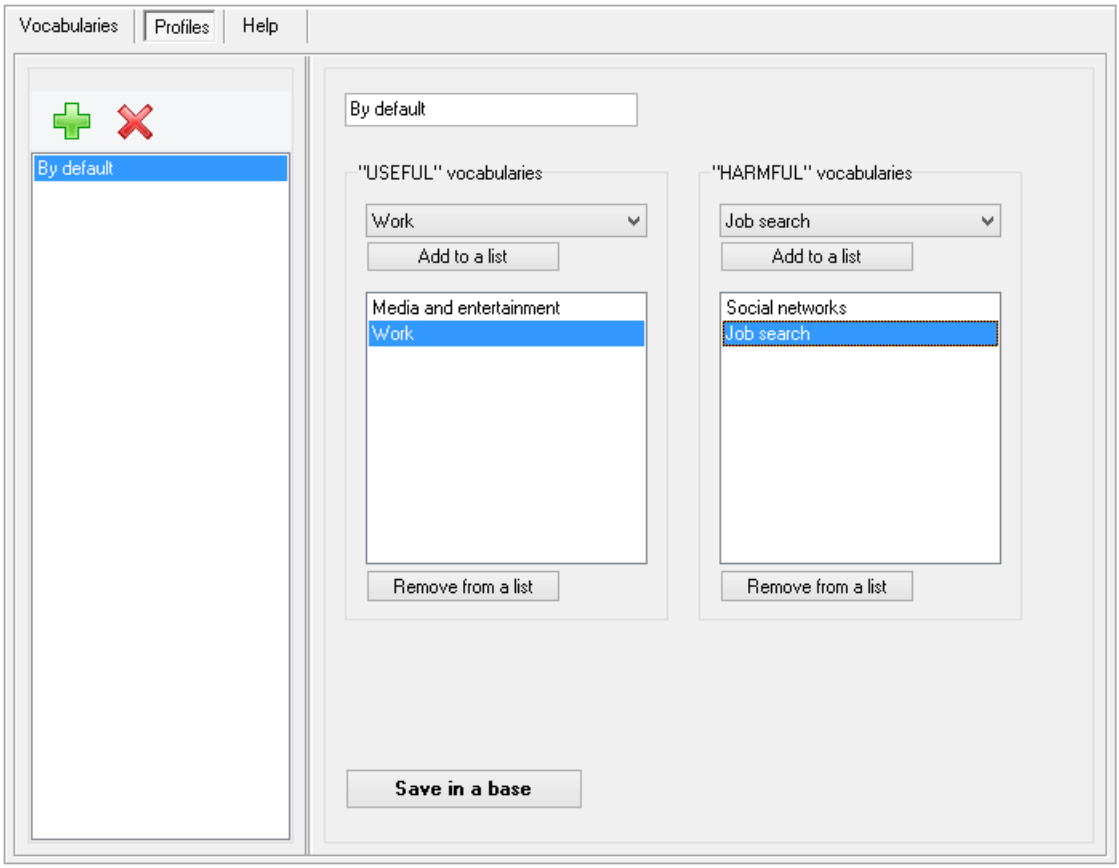
Attention! There is no point to place the same element from the list in several dictionaries (it will be used in the first dictionary).

Attention! Changes in dictionaries come into force only for new monitoring data. It means that old stored data from the database won't be processed in the new dictionaries!

Don't forget to press **"Save in a base"** to apply new settings!

Button **"Import from preinstalled vocabularies"** intended for importing data from the default vocabularies into the current vocabulary with the ability to replace the current data or add to it.

Profiles:



Profiles include certain vocabularies with features **"useful"** or **"harmful"**. It is not required for all vocabularies to be in the profile. Only needed one can be enabled.
Profile **"By default"** is always available and it can not be deleted.
It is possible to create different profiles based on personal needs.
For instance, one profile may be created for each employee from the department.
There is a field **"Profile" in the employee's dossier** to match certain employee with needed profile. For more details about choosing profiles for employees see here in the settings tab "Dossier of employees".

Don't forget to press **"Save in a base "** to apply new settings!

6.8. Report templates

Report "Search"

On this page it is possible to create templates for the database search report for quick search of users by constant criteria. You can create one or more templates of different types.
For each created template you need to add search criteria for which the information will be filtered, also you can select the sorting type of the output results as well as the condition "AND" or "OR" to combine the search criteria.

Important points:
1) When specifying a file name. You can specify a file name with or without masks. However, if you use masks, you can not specify the path to the file (only the name is allowed). If there are no masks, then you can specify the full or partial name of the file or the path to it.
When using **file hashes** it is possible quickly select from drop-down list desired file or specify special word ***IMPORTANT*** (means select any file from the file list with hashes).
2) When specifying search strings. In this case 3 variants of comparsion are possible:
- "equal to": complete coincidence;
- "contains": you can specify part of the string/text, and if you specify the **"~" (tilde)** symbol before **a single word (not text!)**, then an **inaccurate search** of the given word will be processed. Combinations are also possible to search for **near located** words/text using a special separator **NEAR** (example: **~boss NEAR low salary NEAR ~accountant**);
- "begins with": the string starts with the specified part.
3) You can not enter the comparison value explicitly, but use variables of the form **%name%**, in this case, respectively "name" appears in the BOSS-Offline report for user input. Thus, you can specify different values each time not from Global Settings app, but directly in the BOSS-Offline. Example: **%Enter file name%**
Attention! Variables **%name%** cannot be used when generating report thru the Report Wizard. In this case templates containing such variables will be excluded from the search!

Attention! If BOSS-Offline is already running and the change is made in the variables **%name%**, then for applying new values it is necessary to reload the BOSS-Offline page through the exit-login or pressing the "Refresh list" button.

6.9. File hashes

If the contents of certain important company files (with which employees work) changes rarely or does not change at all, it makes sense to take from these files special hashes for more convenient search of operations with them and receive notifications of events.

If you cannot add files manually here, there is an opportunity to configure automatic scanning/updating hashes (see. here)

If you are using file hashes, it is not necessary to set text sensitivity for files on the tab DLP: Rules, because comparsion occurs quickly by hash, not file content.
Also employee can multiple times **rename file**, but in reports original file name only be shown (for possibility of search here).
It is possible to have more than one hash for the same file (the same number of file changes).

Attention! Max hashes count **is limited to 500**!

Attention! Changes made here will be received by clients **after 4-5 minutes**!

6.10. Tariffs

This tab is intended to set up rates for different services.

6.11. List of users

Users lists tab is designed to delete old (unnecessary) records about users/computers from the database. Deleted users and computers cannot be accessible in the **BOSS-Offline** reports. Do not confuse it with clients' app removal from staff's computers - **these are different operations**!

6.12. Work with DB

Tab **"DB maintenance"** is designed to optimize a set of database operations.
In case reports have started to be generated much slower it makes sense to run the database reindexing.

The **"Tables export"** tab provides an intuitive interface for exporting popular database tables related to the complex settings. If a table is not in the list, but it is in the database and needs to be exported, the name can be added.
Output format does not have to match the type of the current DB.
The export output will be one or several files in the format of a standard SQL-script, for subsequent launch through any utilities for working with SQL-scripts, or for use at the **"Import of SQL-scripts"** tab to import previously exported table data into the database.

Attention! After importing the table **TDBUsers ("Database Users")** you have to execute the **"Database Configuration Wizard"**, it will add the created users to the database and assign them rights. In this case, only domain users will be created, but SQL users will not (they must exist in the database before the import)!

6.13. SQL-console

SQL concole tab is designed for advanced administrators in order to perform SQL requests directly to software suite database if required.

6.14. Journal

This tab is designed to look through the log of all entries to the settings app and BOSS (Online/Offline), also settings changing and other important actions.

7. Other:

7.1. Remote employees

If your employees must constantly or temporarily work remotely and using a VPN is not possible, you can configure remote monitoring via Internet using an external connection to the complex server.

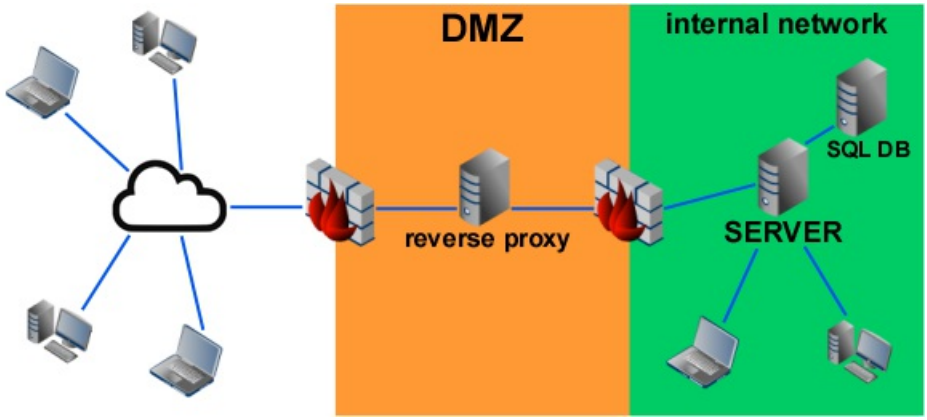
You need to obtain **external static IP-address** or use **DynDNS** or similar solution for the server.
In case your server is not accessible in Internet because of NAT/router, port-forward can be configured (see example here).
By default server uses TCP-port 13289

When installing the **client part**, it is recommended to specify the external server IP in the connection line, separated by comma after the internal IP. In this case, the client will automatically reconnect to the external address if there is no connection with the internal corporate server.

See also: **Server behind the DMZ**

We also recommend looking at the setting **"Work in Outsourcing mode"**.

7.2. Server behind the DMZ



It is not always safe for remote employees to open server ports on the Internet due to network attacks.
As a solution to the problem, you can use **reverse-proxy in the "Demilitarized Zone" (DMZ)**.
The proxy will redirect TCP traffic from remote clients to the server in the intranet.
Thus, with massive network attacks, the complex server will be less vulnerable.

As a proxy-server you can use **nginx in reverse-proxy mode (ngx_stream_proxy_module)**.
Below is an example of settings for nginx when proxying from external port 12345 to internal complex server:22222

```
stream {

 server {
  listen 12345;
  proxy_pass server:22222;
 }

}
```

When installing the **client part**, it is recommended to specify the external proxy IP in the connection line, separated by comma after the internal IP. In this case, the client will automatically reconnect to the external address if there is no connection with the internal corporate server.

7.3. Remote monitoring via internet

With the help of software suite capabilities Scopd can receive all required monitoring reports to e-mail or FTP. So you will be aware of what's going on in the office from any place on the world. But sometimes it is useful to monitor employees "online" or view "fresh" reports being outside of the office.
To make it possible please see the description below.

It is required to open **HTTP-ports 80/443** (used by the web server program **\Program Files (x86)\httpd\bin\httpd.exe**) on the server computer.

Although in most cases your server is connected to internet via proxy or NAT (in the simpliest case via router) so connection to real IP address via http won't work out. To solve this problem it is necessary to set up **port-forwarding** e.g. to specify in the router settings all TCP traffic redirection via http port 80/443 from external network (internet) to external local IP-address inside company's network.
On the following web-site you may find description for all main router models how to set up port-forwarding.

After all settings are performed open any web browser on any computer or smartphone and type in the address bar:
http(s)://<DNS_name_or_IP_server>/scopd

For example:
http://95.135.21.16/scopd
or
https://mycompany.org/scopd

How to setup access via **https:** see here

Note: it is required to insert IP address on some mobile devices (smartphones) not server name (if it is local).

7.4. https-access configuration

During the installation of the server part of the complex, a self-signed SSL certificate is automatically generated to access the server machine (https://**localhost** and https://**DNS_machine_name**). The certificate is also added to the **trusted zone** on Windows(*).

If you access the server machine **from a remote machine**, then the certificate must be added to the **trusted zone** on this machine.
It can be done by execution on this computer next command (**with administrator rights**)(*), (**):

```
certutil -addstore Root "server.crt"
```

File **server.crt** should be copied from the server machine (Windows: C:\Program Files (x86)\httpd\conf\server.crt, Linux: /etc/ssl/crt/stkh/server.crt).

To add certificate into the trusted zone **in domain** it is necessary to perform next steps:
https://technet.microsoft.com/en-us/library/cc754841.aspx

(*) **Attention!** For **Firefox** you must manually add the self-signed certificate to the exclusions list!
(**) **Attention!** For **Chrome** you must close all browser windows after adding certificate to the trusted zone!

7.5. Server transfer

In order to transfer the software suite server and SQL-database to another machine without losing any stored data, the following steps should be performed:

1) Using the "Change Server" function of the BOSS-Online specify a new server machine for all online machines (for non-online machines either a remote installation with indication of a new machine or a repeated manual installation should be used).
Attention! If the transfer is performed out of hours and there are no online-machines (or there are few of them), or if the data losing during the transfer is not critical, then this action can be performed at the end of the server transfer process.
2) Install SQL-server on a new machine (**SQL version should strictly match the old one!**).
3) Install the administrative part of the software suite on the new machine.
4) Use "Export database" tool in the Global settings menu on the old machine to export the database into a file (for PostgreSQL - pg_basebackup/pg_restore).
5) Use the "Import database" menu item on the new machine to import the database from the previously exported file.
6) Start "Database initial configuration" utility on the new machine.
7) Enter the "Global settings" app on the new machine and re-create all the users of the database (through their initial removal).
8) Transfer the shadow copy folder and (if any) the screenshots, web-camera shots, and audio folders from the old machine . If **the paths on the machine differ**, they are needed to be changed in the settings "for server".
9) Install the software suite server on the new machine.
10) If the automatic reports generation was used for the managers, it is necessary to enter the "Private cabinet" of the managers to define settings.
11) Repeat the action 1) for all other machines (if any).

7.6. Client service

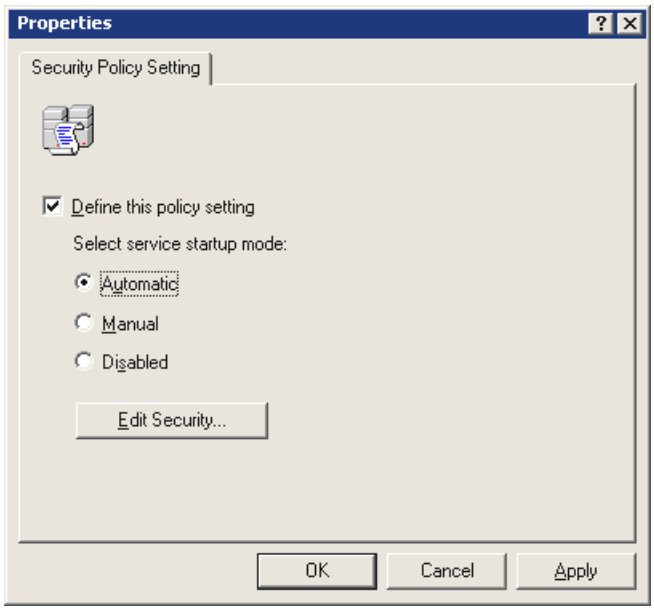
Domain administrator can hide client service from employees:

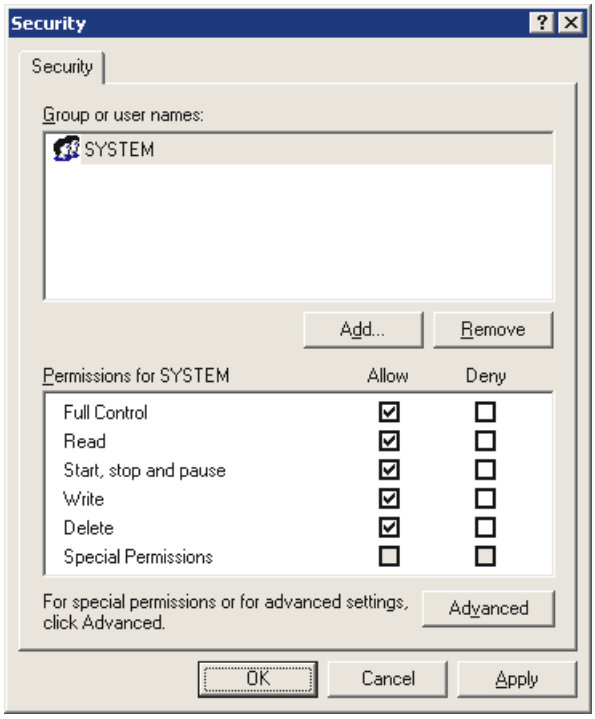
1) If client part is not installed on the domain controller (in most cases it is not installed), then needed to temporarily install the service-emulator with same name as on client machines. To do this take **inst_client.exe** from "Remote installation" (option 4), next execute this command in console with administrator rights on the domain controller:

```
inst_client.exe -temp -install
```

after that program will display **service name** and result of operation.

2) Open **Group Policy Object Editor** for existing domain group policy or create new GPO object for Organizational Unit (OU), in which client computers are located. In GPO editor **"Computer Configuration" -> ["Policies"] -> "Windows Settings" -> "Security Settings" -> "System Services"** find in the list service name was created at the previous step (application inst_client.exe will report service name).
For this service it is needed to change policies: setup **Automatic** startup type and remove from access rights **Administrators** and **Interactive**, leave only **System**:





3) Remove service-emulator:

```
inst_client.exe -temp -uninstall
```

4) In order to not wait for the group policy update on the remote machines after reboot, next command can be executed

remotely:

```
gpupdate /force
```

or use **Group Policy Management Console (GPMC)** for the remote update. See here for the details.

Attention! The service will disappear from the list on the client machine only if it was already installed at the time of applying the policies, but if it is installed later, then the next group policy update on this machine is required after the client part is installed.

7.7. LDAP for PostgreSQL

In order to be able to log into the PostgreSQL database with logins from AD (via LDAP), you need to make a number of settings.

On the LDAP server (usually a domain controller):
For an unsecured connection, it is enough to open the **TCP 389** port, for a secure (LDAPS) - **TCP 636** and install an SSL certificate (not considered here).

In the "pg_hba.conf" file of SQL-server:
First of all, you need to allow non-domain users to login with a SQL password (for compatibility), and **critical important** to do this for the internal server user of the complex **stkhintuser**. You can also leave the login **postgres** and others.
For all other users, LDAP integration must be enabled. **Accordingly, the order of the lines matters!**
Below is an example:

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# postgres login:
host    all             postgres        0.0.0.0/0               scram-sha-256
host    all             postgres        ::/0                    scram-sha-256

# internal user login:
host    stkh            stkhintuser     0.0.0.0/0               scram-sha-256
host    stkh            stkhintuser     ::/0                    scram-sha-256

# for LDAP (non-secure):
host    all             all             0.0.0.0/0               ldap ldapserver="dc1.mydomain.company.org" ldapprefix=""
host    all             all             ::/0                    ldap ldapserver="dc1.mydomain.company.org" ldapprefix=""

# for LDAPS (SSL-secured), option 1:
host    all             all             0.0.0.0/0               ldap ldapserver="dc1.mydomain.company.org" ldapprefix="" ldaptls=1
host    all             all             ::/0                    ldap ldapserver="dc1.mydomain.company.org" ldapprefix="" ldaptls=1

# for LDAPS (SSL-secured), or alternate option 2:
host    all             all             0.0.0.0/0               ldap ldapserver="dc1.mydomain.company.org" ldapprefix="" ldapscheme=ldaps
host    all             all             ::/0                    ldap ldapserver="dc1.mydomain.company.org" ldapprefix="" ldapscheme=ldaps
```

After changing the settings, you need to **restart** the SQL server service!
Next, to log in, you need to use the username in the format NETBIOS_DOMAIN\username (for example, **MYDOMAIN\john.smith** for the domain mydomain.company.org)

7.8. SSL-encryption for SQL

It is possible to encrypt traffic from the complex server and/or the global settings program to the SQL-server.

MS SQL Server
1. In the SQL server connection windows you have to specify a prefix **ssl://** before the server name.
For example: ssl://server-sql
2. It is necessary to make settings at the SQL server itself to install certificates (see here)
Note: if the certificate is self-signed and not added to trusted, then a connection error will be received.

PostgreSQL
The connection to the SQL server uses a secure, encrypted SSL connection (if enabled on the server), or plain without encryption (if not enabled on the server). To enable SSL on the server, just set the parameter **ssl=on** in **postgresql.conf**, and also copy certificate files **server.crt, server.key** to the same folder (usually, when installing on Linux, a certificate is created automatically and nothing additional needs to be done).
More details here:
https://www.postgresql.org/docs/current/ssl-tcp.html

7.9. Data synchronization tool

The **stcsvsync** tool creates an SQL script for synchronize settings based on data provided in .csv table and several types of conversion.

Tool can be downloaded here

General rules

Input data must be provided as **.csv** (divider - semicolon "**;**"). File encoding **UTF-8**.

Output data will be in **UTF-8** encoding.

Errors and warnings will be sent to **STDERR**, output data without setting output file - to **STDOUT**.

Tip: if you just starting to use the tool, avoid [**-of -o**] parameters. In that case output format will be set as TEXT, and you'll get visually appealed data on screen, and can evaluate results before making database changes.

Common command line parameters

-i [**--input**] - input file. Base functions won't be available if not set.

-o [**--output**] - output file. Result will be seen at terminal window if not set.

-of [**--output-format**] - format for output data **TEXT** (default), **MSSQL**, **PGSQL**.

-t [**--type**] - type of data conversion. **D** - Employee Dossier, **G** - Group Settings, **H** - Company structure, **M** - Meetings, **P** - PACS, **S** - Managers, **V** - Holidays / sick leave.

-tt [**--template**] - get .csv template for choosen conversion type [**--type**].

How to get template .csv file for company structure:

```
> stcsvsync -t H -tt
```

```
id;parent;name;[user;[NB_domain]];[computer;[FQ_domain]]
```

Template for employee profiles:

```
> stcsvsync -t D -tt -o dos_template.csv
> cat dos_template.csv
```

```
user;[NB_domain];[fio];[department];[contacts];[profile]
```

Command line parameters

short	full	conversion type	description
-h	--help		show usage
-i	--input		input file name
-o	--output		output file name
-of	--output-format		Output format: [MSSQL | PGSQL | TEXT] default: TEXT
-t	--type		Conversion type: D | G | H | M | P | S | V (Dossier, Group Settings, Hierarchy, Meetings, PACS, Subordination, Vacation)
-ns	--no-sort	[all]	disable sorting before output
-tt	--template	[all]	produce .csv template for provided conversion type
-hl	--header-lines	[all]	number of lines represents header in .csv file [0..] default: 1
-dnb	--domain-netbios	[all]	**NB_domain** in NETBIOS format. Applies when **NB_column** is omitted
-dfq	--domain-fqdn	[GH]	Domain name (**FQ_domain**) FQDN format. Applies when **FQ_domain** is omitted
-ci	--column-id	[GHS]	**id** column number
-cp	--column-parent	[HS]	**parent** column number
-cn	--column-name	[H]	**name** column number
-cu	--column-user	[all]	**user** column number
-cc	--column-computer	[GH]	**computer** column number
-cnb	--column-domain-netbios	[all]	**NB_domain** column number
-cfq	--column-domain-fqdn	[GH]	**FQ_domain** column number
-cf	--column-fio	[D]	**fio** column number or **format string** or **constant string**
-cd	--column-department	[D]	**department** column number or **format string** or **constant string**
-ct	--column-contacts	[D]	**contacts** column number or **format string** or **constant string**

-cpr	--column-profile	[D]	**profile** column number or **format string** или **constant string**
-nd	--no-depth	[S]	forbids to manage subsequent hierarchy nodes
-cb	--column-boss	[S]	**boss** column number
-bv	--boss-value	[S]	**boss** column match value
-dbu	--db-user-template	[S]	Existing SQL user login, which rights will be copied to created users
-cvb	--column-value-begin	[MPV]	**begin date** column number
-cve	--column-value-end	[MPV]	**end date** column number
-cvr	--column-value-reason	[MV]	**reason** column number

Company Structure

(see referenced topic at "Global settings" here)

ATTENTION: target SQL-script will completely delete existing company structure, and deploy new structure afterwards!

Hierarchy nodes can represent groups (departments), users and computers

You can get different kind of company structure, based on single input file.

1. Company Structure (departments only)

```
> stcsvsync -i example.csv -t H -ci A -cp B -cn C
```

2. Departments + users

```
> stcsvsync -i example.csv -t H -ci A -cp B -cn C -cu D -cnb E
```

3. Deparments + computers

```
> stcsvsync -i example.csv -t H -ci A -cp B -cn C -cc F -cfq G
```

4. Departments + user + computer (full structure)

```
> stcsvsync -i example.csv -t H -ci A -cp B -cn C -cu D -cnb E -cc F -cfq G
```

Example of full organization structure built from example.csv

```
> stcsvsync -i example.csv -t H -ci A -cp B -cn C -cu D -cnb E -cc F -cfq G
```

base table **produced structure**

Table **example.csv**

	A	B	C	D	E	F	G	H
1	**id**	**parent**	**name**	**user**	**netbios_domain**	**computer**	**fqdn_domain**	**boss**
2	1	1	Company					
3	2	1	Department 1					
4	3	1	Department 2					
5	4	2	Sub department 1.1					
6	5	1	Sub department 1.2					
7	6	5	Sub department 1.2.1	user1	COMPANY	computer1	company.com	yes
8	6	5	Sub department 1.2.1	user2	COMPANY	computer2	company.com	
9	6	5	Sub department 1.2.1	user3	COMPANY	computer3	company.com	
10		5		user4	COMPANY	computer4	company.com	
11		4		user5	COMPANY	computer5	company.com	yes
12		4		user6	COMPANY	computer6	company.com	
13		1		COMPANY\user7		computer7.company.com		
14		2		user8	COMPANY	computer8	company.com	yes
15		3		user9	COMPANY	computer9	company.com	

```
Company
  COMPANY\user7
  COMPUTER7.company.com
  Department 1
    COMPANY\user8
    COMPUTER8.company.com
    Sub department 1.1
      COMPANY\user5
      COMPANY\user6
      COMPUTER5.company.com
      COMPUTER6.company.com
  Department 2
    COMPANY\user9
    COMPUTER9.company.com
  Sub department 1.2
    COMPANY\user4
    COMPUTER4.company.com
    Sub department 1.2.1
      COMPANY\user1
      COMPANY\user2
      COMPANY\user3
      COMPUTER1.company.com
      COMPUTER2.company.com
      COMPUTER3.company.com
```

Lines 2-6 tells only about groups (departments).
Lines 7-9 besides hierarchy tells about user and computer.
Lines 10-15 don't contain any departments info, but only add users and computers.

Do notice how different results are produced for line 9 and line 10.
Line 10 add user **user4** and computer **computer4** to parent Node 5 (Sub department 1.2).
Line 9, despite having same parent 5 (Sub department 1.2), adds **user3** and **computer3** to Node 6 (Sub department 1.2.1), which is descendant of Node 5.
You should keep this in mind when constructing the initial table.

Line 13 shows how to use Domain name with users and computers in same cell (so you don't need to have separate column for domains).

Synchronizing managers

(see referenced topic at "Global settings" here)

The tool expects that there is a template user in the settings, whose rights will be copied when creating new users.
Create this user without using the "****" character in his name (see the following note below)

ATTENTION:
target SQL-script will delete users, whose names contain "****" character. For example **DOMAIN\username**.
Tool has no way to check if template user exists or not [**--db-user-template**]. Otherwise, the newly created user will have empty set of rights, and you will have to set the rights manually trough the "Global settings".

```
> stcsvsync -i example.csv -t S -ci A -cp B -cn C -cu D -cnb E -cb H -dbu template_user
```

user8 is a Manager for all users and computers of **Department 1** and all subsequent groups, users and computers
user5 is a Manager for all users and computers of **Sub department 1.1** and all subsequent ...
user1 is a Manager for all users and computers of **Sub department 1.2.1** and all subsequent ...

You can change default behavior with key [**--no-depth**]

```
> stcsvsync -i example.csv -t S -ci A -cp B -cn C -cu D -cnb E -cb H -nd -dbu template_user
```

user8 is a Manager for **user8**
user5 is a Manager for **user5**, **user6**
user1 is a Manager for **user1**, **user2**, **user3**

Employee profiles

(see referenced topic at "Global settings" here)

Table **userinfo.csv**

	A	B	C	D	E	F	G
1	**user**	**netbios_domain**	**lastname**	**firstname**	**department**	**e-mail**	**phone**
2	user1	COMPANY	Smith	John	it	john@company.com	111-222-33-44
3	user2	COMPANY	White	Jane	it	jane@company.com	111-222-33-45
4	user3	COMPANY	Harrison	Harry	it	harry@company.com	111-222-33-46
5	user4	COMPANY	Robbins	Oscar	management	oscar@company.com	111-222-33-47
6	user5	COMPANY	Davis	Miles	sales	miles@company.com	111-222-33-48
7	user6	COMPANY	Morgan	Audrey	sales	audrey@company.com	111-222-33-49
8	COMPANY\user7		Jones	William	sales	william@company.com	111-222-33-50
9	user8	COMPANY	Ross	Bennett	management	bennett@company.com	111-222-33-51
10	user9	COMPANY	Groves	Ella	management	ella@company.com	111-222-33-52

Command line examples:

```
> stcsvsync -i userinfo.csv -t D -cu A -cnb B -cf "%D %C" -cd E -ct "%F, %G" -cpr "profile1"
```

For FIO* [**--column-fio**] we use *formula* "**%D %C**". Interpreted as follows: *value from 4th column, space, value from 3rd column.*

*Term "FIO" means "full name" - first name, middle name, last name.

Department [**--column-department**] we use column number **E** (which means column 5). Formula "**%E**" will give same result.

Contacts [**--column-contacts**] *formula* "**%F, %G**". Value from 6th column, comma, space, value from 7th column.

Profile [**--column-contacts**] *constant* "**profile1**"

Output:

```
COMPANY\user6
        FIO:        Audrey Morgan
        Department: sales
        Contacts:   audrey@company.com, 111-222-33-49
        Profile:    profile1
COMPANY\user8
        FIO:        Bennett Ross
        Department: management
        Contacts:   bennett@company.com, 111-222-33-51
        Profile:    profile1
COMPANY\user9
        FIO:        Ella Groves
        Department: management
        Contacts:   ella@company.com, 111-222-33-52
        Profile:    profile1
COMPANY\user3
        FIO:        Harry Harrison
        Department: it
        Contacts:   harry@company.com, 111-222-33-46
        Profile:    profile1
COMPANY\user2
        FIO:        Jane White
        Department: it
        Contacts:   jane@company.com, 111-222-33-45
        Profile:    profile1
COMPANY\user1
        FIO:        John Smith
        Department: it
        Contacts:   john@company.com, 111-222-33-44
        Profile:    profile1
COMPANY\user5
```

```
        FIO:        Miles Davis
        Department: sales
        Contacts:   miles@company.com, 111-222-33-48
        Profile:    profile1
COMPANY\user4
        FIO:        Oscar Robbins
        Department: management
        Contacts:   oscar@company.com, 111-222-33-47
        Profile:    profile1
COMPANY\user7
        FIO:        William Jones
        Department: sales
        Contacts:   william@company.com, 111-222-33-50
        Profile:    profile1
```

Vacations and sick/leave

(see referenced topic at "Global settings" here)

ATTENTION target SQL-script will delete all from database table with info about vacations and sick/leave days and creates new records provided by .csv table.

Table **vacations.csv**

	A	B	C	D
1	**user**	**begin**	**end**	**reason**
2	DOMAIN\j.smith	14.01.2024		1
3	DOMAIN\j.smith	15.01.2024		1
4	DOMAIN\j.smith	16.01.2024		1
5	DOMAIN\j.smith	17.01.2024		1
6	DOMAIN\j.smith	19.01.2024		1
7	DOMAIN\j.smith	20.01.2024		1
8	DOMAIN\j.smith	21.01.2024		1
9	DOMAIN\j.smith	25.01.2024	30.01.2024	1
10	DOMAIN\w.johnes	01.02.2024	17.02.2024	2
11	DOMAIN\robbins	28.02.2024	12.02.2024	3
12	DOMAIN\j.smith	29.01.2024	12.02.2024	1
13	DOMAIN\j.smith	07.02.2024		1
14	DOMAIN\j.smith	09.02.2024		1
15	DOMAIN\j.smith	07.01.2024	15.01.2024	1

Command line example:

```
> stcsvsync -i vacations.csv -t V -cu 1 -cvb 2 -cve 3 -cvr 4
```

```
DOMAIN\j.smith:  [2024-01-07 (1) 2024-01-17] [2024-01-19 (1) 2024-01-21] [2024-01-25 (1) 2024-02-12]
DOMAIN\w.johnes:  [2024-02-01 (2) 2024-02-17]
DOMAIN\robbins:  [2024-02-12 (3) 2024-02-28]
```

DOMAIN\username [**--column-user**], period begin date [**--column-value-begin**] are mandatory!

Period end date [**--column-value-end**] can be omited (will mean one-day leave)

Reason [**--column-vacation-reason**] must be integer. If omited or can't be reinterpreted as integer - will be zero.

Date can be in one of following: dd.mm.yyyy, dd/mm/yyyy, dd-mm-yyyy, yyyy-mm-dd, yyyymmdd. (Here: dd - day of month [1..31], mm - month number [1..12], yyyy - year in 4 digit form)

NOTE: any cases of duplicate dates or overlapping periods will be resolved.

Import records from Physical Access Control System (PACS).

ATTENTION target SQL-script will NOT delete any PACS data, as far as sequential imports are supposed. In case of errors or need to repeat import of last records - contact DB administrator, make sure data to delete to contains current period and current users only!

Table **pacs.csv**

	A	B	C
1	**user**	**entry**	**exit**
2	DOMAIN\j.smith	15.01.2024 09:00:00	15.01.2024 18:00:00
3	DOMAIN\j.smith	16.01.2024 09:00:00	16.01.2024 18:00:00
4	DOMAIN\j.smith	17.01.2024	17.01.2024 18:00:00
5	DOMAIN\w.johnes	22.01.2024 08:00	22.01.2024 17:00
6	DOMAIN\robbins	22.01.2024 08:00	22.01.2024 17:00
7	DOMAIN\j.smith	21.01.2024 09:00	21.01.2024 18:00:00

Command line example:

```
> stcsvsync -i pacs.csv -t P -cu 1 -cvb 2 -cve 3
```

```
DOMAIN\j.smith:
        [2024-01-15 09:00:00 - 2024-01-15 18:00:00] 9h
        [2024-01-16 09:00:00 - 2024-01-16 18:00:00] 9h
```

```
        [2024-01-17 00:00:00 - 2024-01-17 18:00:00] 18h
        [2024-01-21 09:00:00 - 2024-01-21 18:00:00] 9h

DOMAIN\w.johnes:
        [2024-01-22 08:00:00 - 2024-01-22 17:00:00] 9h

DOMAIN\robbins:
        [2024-01-22 08:00:00 - 2024-01-22 17:00:00] 9h
```

DOMAIN\username [**--column-user**], datetime begin (entry) [**--column-value-begin**], datetime end (exit) [**--column-value-end**] are mandatory!

Assigning settings profiles to users and computers (GroupSettings)

(see referenced topic at "Global settings" here)

Settings profile number must be set through **id**, use **-ci** with corresponding column number.

Table **groupsettings.csv**

	A	B	C	D	E
1	**user**	**nb_domain**	**computer**	**fqdn_domain**	**profile_id**
2	DOMAIN\j.smith				8
3	k.anderson	DOMAIN			9
4			laptop152	domain.local	12
5	w.jhones	DOMAIN			10
6	DOMAIN\robbins				3
7			SERVER-FS3.domain.local		2
8			WSADF34RT	domain.local	11

Command line example:

```
> stcsvsync -i example.csv -t G -cu A -cnb B -cc C -cfq D -ci E
```

```
8         DOMAIN\j.smith
9         DOMAIN\k.anderson
3         DOMAIN\robbins
10        DOMAIN\w.jhones
12        LAPTOP152.domain.local
2         SERVER-FS3.domain.local
11        WSADF34RT.domain.local
```

Meetings, appointments, interviews

Table **meetings.csv**

	A	B	C	D
1	**user**	**begin**	**end**	**reason**
2	DOMAIN\j.smith	14.01.2024 12:00	14.01.2024 13:30	Daily meeting with Devs
8	DOMAIN\j.smith	21.01.2024 10:30	21.01.2024 12:00	Project N meeting
10	DOMAIN\w.johnes	01.02.2024 14:30	01.02.2024 15:00	unplanned
11	DOMAIN\robbins	28.02.2024 10:00	28.02.2024 10:15	job interview

Command line example:

```
> stcsvsync -i meetings.csv -t M -cu 1 -cvb 2 -cve 3 -cvr 4
```

Datetime can be in one of following: dd.mm.yyyy hh:mm[:ss], dd/mm/yyyy hh:mm[:ss], dd-mm-yyyy hh:mm[:ss], yyyy-mm-dd hh:mm[:ss], yyyymmdd hh:mm[:ss]. (Here: dd - day of month [1..31], mm - month number [1..12], yyyy - year in 4 digit form, hh - hours [0..23], mm - minutes [0..59])

Running SQL-scripts

You can run scripts in any familiar way, if you have one.
NOTE: don't forget to include the database name (stkh).

Example for **MSSQL-tool sqlcmd**:

```
> sqlcmd -d stkh -i script.sql -o output.txt -U dbadmin -P "*******"
```

```
> sqlcmd -d stkh -i script.sql -o output.txt
```

Example for **PGSQL-tool psql**:

```
> psql -d stkh -f script.sql -o output.txt -U postgres
```

ATTENTION! In case of synchronization of Managers (Subordination), after executing SQL-script you have to execute **"Database configuration utility"** (it will add new logins for Managers and assign them rights).

7.10. Document marking utility

The utility is designed to mark important documents with hidden tags in order to protect them or control the sending of these documents (or parts of them) outside the company.

Tool can be downloaded here

Usage instructions (**simple case/quick start**):

1. Copy the required .docx/.xlsx/.pptx/.pdf to the "__in" folder (without additional folder hierarchy!)

2. Edit the parameters in the mark_multi.cmd file:
__INTENSITY (from 1 to 100, sets the marking intensity, i.e. actually affects the number of marks)
__MARKSTRING (mark string to identify markings, English letters and numbers only, case sensitive, max. 63 characters)

3. Execute mark_multi.cmd

4. After successful execution, marked documents will be located in the "__out" folder.

5. In the complex settings, on the "DLP: Rules" tab, in the **"Sensitivity"** section, add the string set to **__MARKSTRING**, enclosed between the # symbols (for example, **#MyLabel1#**)

Usage instructions (**advanced**):

Refer to the scripts **mark_single_** description inside the files.
The script can be executed in different conditions, in any complex architectures using any administrative automated tools or manually.

Note: to **check marks** in the document use execution with parameter:

```
stmark check <filename_to_check>
```

7.11. Getting started with Astra Linux

Documentation for this topic is not available in the current version!

8. FAQ:

8.1. License issues

What are restrictions for demo version?
You are able to work without any restrictions only with one client computer.

What are restrictions for the trial version?
You are able to work without any restrictions with 50 clients' computers for no more then for 2 weeks.

How are licenses spent?
The total number of **simultaneous unique connections** of clients to the server is licensed.
Connection uniqueness is a pair of **"domain+username"** (or "PC name+username" if there is no domain) of a user session when working on a PC with the client part installed (if the PC is turned off, the license is not consumed).
For example, if a user is logged in simultaneously on two PCs (with clients installed on them) under the same login, then these two connections will only use one license, not two!
It also doesn't matter if the client is installed on a terminal server or a regular workstation, however, an inactive (disconnected) terminal session is taken into account in the same way as an active one.
The licenses are **competitive** and are not tied to hardware or PC names, user logins.
Thus, if the total number of concurrent unique connections exceeds the number of licenses in the license key by N, monitoring data from the remaining N-connections will not be saved to the database and will not be reflected in the reports. It is impossible to say exactly what these N-connections will be, they can change constantly over time when the remaining connections to the server are reconnected.

How fast will I receive the key after payment?
It depends from the payment method. Usually it happens within one working day. You can find more details in the manual which is sent after ordering.

Will I receive license agreement in the hard copy about legal purchase?
Yes, of course. It is issued in accordance with your needs.

Is it possible to buy more licenses to already purchased?
Of course. While filling in order form select "To buy more".

Do incoming updates free of charge?
Yes, but only within one version N.xx

Whether MSSQL_Express, PostgreSQL and MySQL are free of charge?
Yes, they are.

8.2. General questions

Is it necessary to have a dedicated server for software suite?
Yes, it is needed. Although downtime in its performance is possible. In the rest time it must be always plugged in (or at least during employees' works).
It may also be administrator's computer if dedicated is not available.

Does the program violate human rights?
No, it doesn't. Open surveillience mode with push message to the user is available in the program and turned on by default. In this push message you can notify the user that he or she is monitored.

8.3. Technical questions

How to install new client's version on all computers at the same time?
See part "Software suite update"

How client's app will be functioning if SQL server database is disabled?
The client's app is constantly trying to support connection with server but it can make caching of data if required (e.g. to work without server).

Is client app necessary to be installed for all users if terminal server is used?
No. It is installed once under administartor's account.

Whether clients' part can be installed for each system user individually?
No. It is installed once under administrator's account on current computer.

Why the monitoring of printed documents is not functioning?
See help on the page printer's monitoring settings in the administrator's part settings.

I am not capable to enter web-server from mobile smartphone. Why?
It is required on some mobile devices to put IP address not server name (if it is local) in the browser address line.

How to open SPL printer files?
See description here

How to set up access to the web via https (SSL)?
see here

Why did some programs issue a warning about an untrusted root certificate?
see here

We use an antivirus. Why Internet connections are blocked after installing the client?
see here

9. Technical support:

9.1. Technical support

Technical support page