StaffCop Enterprise v. 3.1.

User Manual

Thank you for choosing StaffCop Enterprise!

Below you can find detailed guide on how to make StaffCop Enterprise work most efficiently for your company.

For technical enquiries, please contact our Technical Support team

support@staffcop.com

Index

Introduction

StaffCop Enterprise is a bundled software for monitoring employee work time. Our software enables company executives, security officers, and system administrators to monitor almost all suspicious incidents occurring on employee workstations in real time, as well as in employee logs. Our bundled software enables you to realistically evaluate performance of your employees and find out their activities during their work time. This product is a perfect tool to detect insiders and data leaks.

QUICK START

./source/01/faststart.htm

StaffCop Enterprise main features include:

- Complete monitoring of network traffic (including encrypted traffic), e-mails (with attachments), IM messengers, and web sites;
- Monitoring various file operations (file system, clipboard, copying files to external data storages);
- Monitoring all employee activities at workstation;
- Key strokes monitoring (key logger);

StaffCop Enterprise main advantages are:

- Remote access to Admin panel from any place in the world via web interface;
- Flexible system of StaffCop Agents and aggregated data configuring;
- Access rights distribution by groups and users;
- Visual display of intercepted data as table, graph or diagram;
- Attractive pricing;
- Professional and polite technical support specialists;

StaffCop Enterprise is actively evolving project, we take into account all customers' requirements and consider proposals for improving the functionality on individual basis.

Support of Server installation on any virtual machine including **VirtualBox, Hyper-V, VMware.** Current User Guide contains information about installation on VirtualBox. Same way StaffCop Enterprise is installed on other virtual machines.

Installing StaffCop Enterprise Server under Linux OS

Installation of StaffCop Server on virtual machine VirtualBox running under OS Windows

System requirements

Minimal system requirements for admin part of StaffCop Enterprise:

Note: Admin part is supported by Mozilla, Firefox and Google Chrome browsers. Other browsers support is not guaranteed.

- OS: Linux 64-bit (Ubuntu, Debian, etc.). Installation to virtual machine is supported;
- Processor: Dual Core 1.8 GHz;
- RAM: 2 Gb;
- Hard disk space: from 10 Gb.

Recommended system requirements for server part of StaffCop Enterprise (support of 10-50 StaffCop Agents):

- OS: Ubuntu Server 14.04 LTS (16.04 LTS);
- Processor: Intel Xeon E5-2603 v3;
- RAM: 8 Gb;
- Required disk space: 30 Gb – for OS, 100 Gb for Database Management System (DBMS);
- Free hard disk space necessary for storing data is calculated according to the formula presented below.

Recommended system requirements for server part of StaffCop Enterprise (support of 100-200 StaffCop Agents):

- OS: Ubuntu Server 14.04 LTS (16.04 LTS);
- Processor: Intel Xeon E5-2603 v3;
- RAM: 16 Gb;
- Required disk space: 30 Gb – for OS, 200 Gb for Database Management System (DBMS);
- Free hard disk space necessary for storing data is calculated according to the formula presented below.

Recommended system requirements for server part of StaffCop Enterprise (support of 200-500 StaffCop Agents):

- OS: Ubuntu Server 14.04 LTS (16.04 LTS);
- Processor: Intel Xeon E5-1660V3;
- RAM: 32 Gb;
- Required disk space: 30 Gb – for OS, 400 Gb for Database Management System (DBMS);
- Free hard disk space necessary for storing data is calculated according to the formula presented below.

Note: For more convenience we recommend you to use RAID5! Keeping DB on SSD storage significantly increases response time of the admin panel due to increased speed of DB requests.

Use the following formula to calculate disk space on server for storing user data:

X = N x V,

1) Where **X** is required disk space;
2) **N** is number of StaffCop agents;
3) **V** is a volume of data aggregated by one StaffCop Agent, maximum 1 Gb per month.

Examples for one StaffCop Agent per month:

1. When default settings are applied in **Default Config**:

   Calculation of disk space for screenshots captured every 10 minutes:

   22 * 8 * (60/10) * 250 Kb = **~ 440 Mb**

   Where **22** – number of workdays per month;
   8 – number of work hours per work day;
   60/10 = 6 – number of screenshots per hour;
   250 Kb – average size of desktop screenshot in StaffCop Enterprise;

   Calculation of intercepted files with file size 10 Mb, provided that employee sends files via e-mail (5 e-mails or messages per hour):

   5 * **10** * **20** = **1000** Mb
   where **20** – number of workdays per month

   Or if 10 e-mails per hour:

   10 * **10** * **20** = **2000 Mb**
   where **20** – number of workdays per month

   Total size of data aggregated by StaffCop Agent per month: **1,3 Gb**

When operating the program with settings of **Total Control** configuration are set to maximum:

Calculating disk space for screenshots captured every minute:

20* 8 * 60 * 180Kb = 1728000 Kb

where **20** is number of workdays per month;
8 is number of work hours per day;
60 is number of screenshots per hour;
180 Kb – average size of desktop screenshot in StaffCop Enterprise.

Calculating disk space for webcam shots captured every minute:

20 * 8 * 60 * 17 Kb = 163200 Kb

where **20** is a number of workdays per month;
8 is a number of work hours per day;
60 is a number of screenshot per hour;
17 Kb is an average size of web cam shot in StaffCop Enterprise.

Calculating intercepted files with size 100 Mb provided that employee sends five messages or emails per hour:

5 * 100 * 20 = 10000 Mb

where **20** is number of workdays per month

Calculating intercepted audio files recorded via microphone, each file is one hour recording and its size is 30 Mb:

If employee talks 2 hours per day in total, then total size is **60 Mb.**

Then total volume of this data aggregated by StaffCop Agent per month: **12.4 Gb**

Minimal system requirements for StaffCop Enterprise Agent:

- OS: Windows Vista, 7, 8, Windows Server 2003, 2008, 2012;
- Processor: Intel Celeron 1.8 Hz;
- RAM: 1 Gb (to work on terminal server for each user requires additional 256 Mb of RAM);
- Hard disk space: 5 Gb.

Recommended system requirements for StaffCop Agent:

- OS: Windows XP, 7, Vista, 8, 8.1, 10, Windows Server 2008, 2012;
- Any compatible processor. Recommended number of cores it should contain: 2+ ;
- RAM: from 1 Gb. Our recommendation: from 2 Gb and larger;
- Hard disk space on a system disk: from 10 Gb.

To install and configure StaffCop Enterprise bundle do the following:

1. Install the server part and StaffCop monitoring Agents;
2. Find out current IP address of StaffCop Enterprise server or CONFIGURE NETWORK;
3. In any modern Internet browser enter StaffCop Enterprise server IP address in address field (we recommend to use Google Chrome, Firefox, and Yandex);
4. Specify super admin password;
5. Access account under admin login and use newly created password (see above);
6. **Activate Trial Version** (Internet connection is required) or enter trail license key (use **Offline activation** option);
7. Select **Download Agent installer** using web interface in **Admin** menu;
8. Before installing StaffCop Agents on workstation please read integration guide;
9. Add StaffCop files and folders to antivirus exceptions if antivirus is installed on monitored workstation;
10. Install StaffCop Agent on employee workstation under admin account;
11. Installed StaffCop Agents connect to StaffCop Server automatically;

If you encounter technical issues, please contact our technical support at support@staffcop.com.

Read FAQ to find most popular questions of our clients.

Minimum system requirements for StaffCop Agent:

1. OS: Windows 8, Windows 7, Vista, Windows Server 2003, 2008, 2012.
2. Processor: Intel Celeron 1.8 GHz.
3. RAM: 1 Gb (to work on terminal server, RAM should be expanded by 256 Mb per each user).
4. Hard disk: 5 Gb.

Recommended system requirements for StaffCop Agent:

- OS: Windows 8, Windows 7, Vista, Windows Server 2003, 2008, 2012.
- Processor: Intel Core2Duo 2.2 GHz.
- RAM: 2 Gb (to work on terminal server, RAM should be expanded by 256 Mb per each user).
- Disk space: from 5 Gb.

ATTENTION! Because Microsoft officially stopped supporting OS Windows XP, users installing StaffCop Enterprise Agents on workstations running under this OS might encounter issues during installation and deployment.

Quick start

Complete the following steps to install and configure StaffCop Enterprise v.3.1:

1. Installation **and Uninstallation of StaffCop Enterprise** server part and StaffCop Agents;
2. Determine server IP address or CONFIGURE NETWORK;
3. Enter server IP address in the address bar of any modern browser (recommended Chrome, Firefox, or Yandex);
4. Specify super administrator password;
5. Access account under admin login using newly created password;
6. Activate **Trial version** (Internet connection is required) or enter **Trial license key** (offline activation is possible);
7. Select **Download Agent installer** in **Admin menu**;
8. If antivirus is installed on workstation, add StaffCop files and folders to Adding exceptions for antivirus software;
9. Types of StaffCop Enterprise **Agent installation** on employee workstation under account with admin rights;

Installed StaffCop Agents will connect to StaffCop server automatically.

In case you encounter any issues during installation, please contact our technical support team at support@staffcop.com

Frequently asked questions and answers regarding StaffCop can be found in FAQ section of our web site.

ATTENTION! Because Microsoft officially stopped supporting OS Windows XP, users installing StaffCop Enterprise Agents on workstations running under this OS might encounter issues during installation and deployment. We recommend installing StaffCop Agents according to **Ошибка! Источник ссылки не найден.**.

Working with StaffCop Enterprise

General information

StaffCop Enterprise is a client-server application comprised of two main modules: **Server module** and **Agent**.

StaffCop Enterprise Server is used to receive, store, and view data aggregated by StaffCop Agent. System administration, monitoring rules configuring, data viewing and analysis are done via user-friendly web interface.

StaffCop Enterprise Agent is a system service operating on employee workstation. It aggregates all necessary data and then transfers it to StaffCop Server.

Working in distributed networks

Distinctive feature of **StaffCop Enterprise** architecture is that monitored workstation does not have to be connected to the local network all the time. For correct work of our software, you need only access to StaffCop Server via Internet or open TCP port 443. When disconnected from Internet, StaffCop Agent aggregates data and then transfers it to server as soon as monitored computer is connected to the Internet.

For example, when your employee goes on business trip with his laptop computer, you do not lose control over his or her activities on the laptop, and monitoring the laptop continues in a regular mode.

StaffCop Agent

StaffCop Agent is a service operating on employee workstation. It aggregates various data and transfers it to StaffCop Server.

The Agent is installed on employee workstation locally or remotely (via embedded remote installation utility), or deployed via group policies (GPO) of Active Directory. To be able to install the Agent you need to have rights of local (domain) administrator.

The Agent operates in stealth mode and invisible to employee.

The Agent aggregates data and creates logs about employee activities in secured folders inaccessible to regular user. When it transfers them to StaffCop Server, it automatically deletes them on monitored workstation in order to free disk space.

The Agent transfers data via encrypted channel (openSSL) to the Server. Data is transferred as packages, their maximum size and interval of data transfers are specified in the Agent configuration settings. Be default maximum size of each package is 1 Mb, and interval of data transfer to the server is 30 seconds.

The Agent uses any port to send reports to StaffCop Server, by default it is port 443 (https) which is opened in most cases. It enables the Agent to transfer reports immediately after installation without configuring network specifically for this purpose. To use alternative port you should specify it during StaffCop Enterprise installation.

During installation, you can specify address and ports of main and alternative servers too. If main server is inaccessible, the Agent transfers data to alternative address. For example, you can specify internal server IP of enterprise local network as the main server address, and external server IP accessible via Internet, which will be receiving data from the Agents, as alternative server.

Open TCP port 443 is required for data transfer over the network.

If there is no connection between the Agent and the Server, the Agent aggregates data in local database and transfers it to the Server as soon as connection is established. By default, maximum size of local database is 1 Gb. When this limit is reached, the Agent starts overwriting data in cycles each cycle deleting the oldest records.

StaffCop Server

StaffCop Server collects, stores, analyzes and displays data collected from StaffCop Agents.

Install the Server on computer running under Ubuntu Server. It stores PostgreSQL database data.

Unlike most of our competitors, we do not use Microsoft or Oracle solutions, but use open source software so that our clients do not have to make additional purchases of third-party software such as operation system or databases. The cost of StaffCop license is calculated just by number of StaffCop Agents included in the license (or users on terminal servers), one Agent is installed on one workstation.

The server part has smart web interface (admin panel), accessible via Internet. We recommend you to use modern Internet browsers with HTML5 support, such as Google Chrome and Firefox. Operations via Internet Explorer is not supported (errors might occur).

Read detailed description of web interface functional in StaffCop Enterprise Interface section of the current guide.

Open port TCP 443 is required to connect the Server with the Agents.

By default port 80 and 443 are used to access web interface. If necessary, you can change the ports in settings.

Time zones on StaffCop Server and monitored workstations should be the same for correct display of the Agents time zone in admin panel, and for receiving monitored events info with actual date/time. You can check and configure time and time zone on the server using console commands described in StaffCop commands.

Installation and Uninstallation of StaffCop Enterprise

Types of StaffCop Enterprise installation

StaffCop Enterprise consists of two parts: StaffCop Server and StaffCop Agent.

The Server is installed either on PC running under Linux 64-bit, or on any virtual machine (for example, VirtualBox) running under Linux 64-bit. It takes just several minutes to install. Note, in case when you install the server part on virtual machine, performance of admin panel might go down.

After you install the server part, StaffCop Agents should be installed on workstations that will be monitored. In current version of StaffCop Enterprise you can launch multiple automatic installation or manual installation.

Multiple automatic installations is most preferable type of install. This is the most quick and obvious method to deploy StaffCop Enterprise. In this case, complete installation process will take minimum time and installation time depends very little on a number of workstations in client network. Usually it takes just few minutes to complete.

In case multiple installation of StaffCop Agents is disabled, you can install the Agents manually. Installation time is directly proportional to the number of workstations in your network.

StaffCop Server installation

System requirements

Minimal system requirements for admin part of StaffCop Enterprise:

Note: Admin part is supported by Mozilla, Firefox and Google Chrome browsers. Other browsers support is not guaranteed.

- OS: Linux 64-bit (Ubuntu, Debian, etc.). Installation to virtual machine is supported;
- Processor: Dual Core 1.8 GHz;
- RAM: 2 Gb;
- Required disk space: from 10 Gb.

Recommended system requirements for server part of StaffCop Enterprise (support of 10-50 StaffCop Agents):

- OS: Ubuntu Server 14.04 LTS (16.04 LTS);
- Processor: Intel Xeon E5-2603 v3;
- RAM: 8 Gb;
- Required disk space: 30 Gb – for OS, 100 Gb for Database Management System (DBMS);
- Free hard disk space necessary for storing data is calculated according to the formula presented below.

Recommended system requirements for server part of StaffCop Enterprise (support of 100-200 StaffCop Agents):

- OS: Ubuntu Server 14.04 LTS (16.04 LTS);
- Processor: Intel Xeon E5-2603 v3;
- RAM: 16 Gb;
- Required disk space: 30 Gb – for OS, 200 Gb for Database Management System (DBMS);
- Free hard disk space necessary for storing data is calculated according to the formula presented below.

Recommended system requirements for server part of StaffCop Enterprise (support of 200-500 StaffCop Agents):

- OS: Ubuntu Server 14.04 LTS (16.04 LTS);
- Processor: Intel Xeon E5-1660V3;
- RAM: 32 Gb;
- Required disk space: 30 Gb – for OS, 400 Gb for Database Management System (DBMS);
- Free hard disk space necessary for storing data is calculated according to the formula presented below.

Note: For more convenience, we recommend you to use RAID5! Keeping DB on SSD storage significantly increases response time of admin panel due to increased speed of DB requests.

Use the following formula to calculate disk space on server for storing user data:

X = N x V,

1. Where **X** is required disk space;
2. **N** is number of users.
3. **V** is a volume of data aggregated by one StaffCop Agent, maximum 1 Gb per month.

Examples for one StaffCop Agent per month:

1. When default settings are applied in Default Config:

Calculation of disk space for screenshots captured every 10 minutes:

22 * 8 * (60/10) * 250 Kb = **~ 440 Mb**

Where **22** – number of workdays per month;
8 – number of work hours per work day;
60/10 = 6 – number of screenshots per hour;
250 Kb – average size of desktop screenshot in StaffCop Enterprise;

Calculation of intercepted files with file size 10 Mb, provided that employee sends files via e-mail (5 e-mails or messages per hour):

5 * 10 * 20 = 1000 Mb
where 20 – number of workdays per month

Or if 10 e-mails per hour:

10 * 10 * 20 = 2000 Mb
where **20** – number of workdays per month

Total size of data aggregated by StaffCop Agent per month: 1,3 Gb

When operating the program with configuration are set to maximum:

Calculating disk space for screenshots captured every minute:

20* 8 * 60 * 180Kb = 1728000 Kb

where 20 – number of workdays per month
8 – number of work hours per work day
60 – number of screenshots per hour
180 Kb – average size of desktop screenshot in StaffCop Enterprise

Calculating disk space for webcam screenshots captured every minute:

20 * 8 * 60 * 17 Kb = 163200 Kb

where **20** is a number of workdays per month;
8 is a number of work hours per workday;

60 is a number of screenshots per hour;
17 Kb is an average size of desktop screenshot in StaffCop Enterprise.

Calculating intercepted files with size 100 Mb provided that employee sends five messages or emails per hour:

5 * 100 * 20 = 10000 Mb

where **20** is a number of workdays per month

Calculating intercepted audio files recorded via microphone, each file is one hour recording and its size is 30 Mb:

If employee talks 2 hours per day in total, then total size is **60 Mb.**

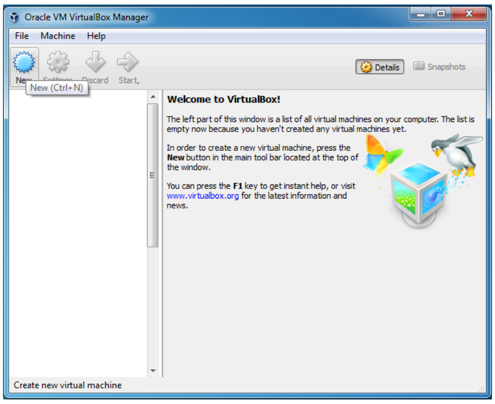
Then total volume of this data aggregated by StaffCop Agent per month: 12,4 Gb

Installation of StaffCop Server on virtual machine VirtualBox running under OS Windows

Complete the same steps to install StaffCop Server on other virtual machines.

To install Server module on virtual machine VirtualBox, you have to send request to receive StaffCop Enterprise distributive by filling out [contact form for downloading trial version](). After this is done, an e-mail containing the link to StaffCop Enterprise distributive will be send out to you automatically. Before deploying virtual machine, make sure that processor has 64-bit architecture and virtualization is enabled in **BIOS** settings.

1. Launch **VirtualBox** by clicking **New**;



Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

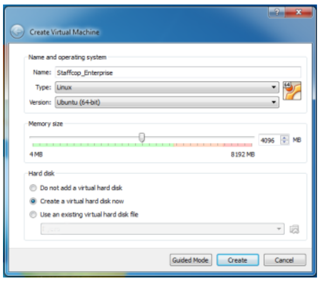
In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for the latest information and news.

Create new virtual machine

Figure 1.

2. In the new window enter name (any name) of a virtual machine. Specify **Type: Linux, Version: Ubuntu(64bit)**. Click **Next**;
3. Specify memory volume dedicated for virtual machine operations (recommended from 1Gb). Click **Next**;
4. Create new virtual hard disk and click **Create**;



Create Virtual Machine

Name and operating system

Name: Staffcop_Enterprise

Type: Linux

Version: Ubuntu (64-bit)

Memory size

4096 MB

Hard disk

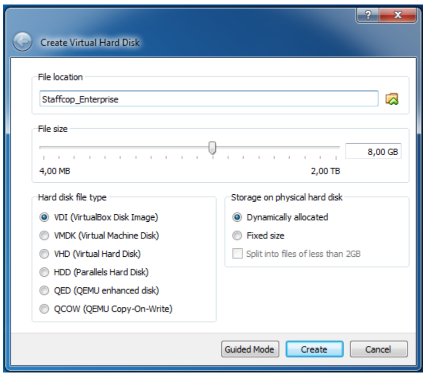
○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

Figure 2.

5. We recommend you to select dynamic virtual hard disk in case you will need to extend volume of data storage in the future. Click **Create.**



Create Virtual Hard Disk

File location

Staffcop_Enterprise

File size

8,00 GB

Hard disk file type

● VDI (VirtualBox Disk Image)

○ VMDK (Virtual Machine Disk)

○ VHD (Virtual Hard Disk)

○ HDD (Parallels Hard Disk)

○ QED (QEMU enhanced disk)

○ QCOW (QEMU Copy-On-Write)

Storage on physical hard disk

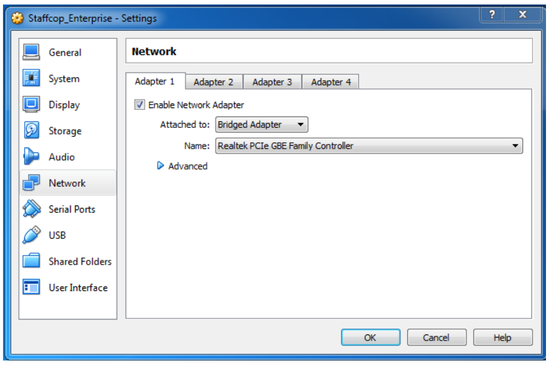
● Dynamically allocated

○ Fixed size

□ Split into files of less than 2GB

Figure 3.

6. After configuring new virtual machine, open its settings by clicking **Settings** icon, and specify **Type of connection: Bridged Adapter** in **Network** parameters. Click **Oк**;



Staffcop_Enterprise - Settings

Network

Adapter 1

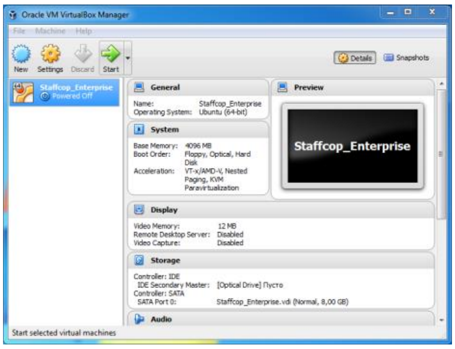
☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Realtek PCIe GBE Family Controller

Figure 4.

7. Click **Start** to launch virtual machine you created;



Name: Staffcop_Enterprise
Operating System: Ubuntu (64-bit)

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

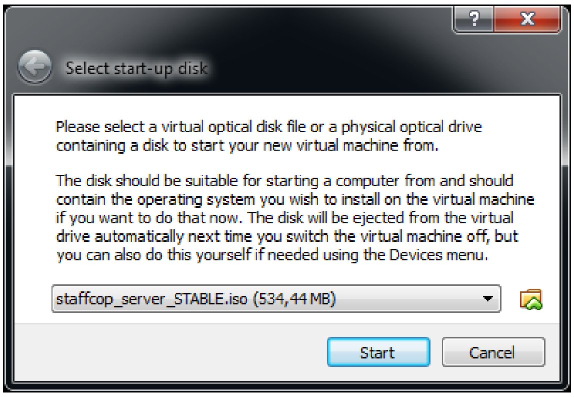
Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Controller: IDE
IDE Secondary Master: [Optical Drive] Пусто
Controller: SATA
SATA Port 0: Staffcop_Enterprise.vdi (Normal, 8,00 GB)

Start selected virtual machines

Figure 5.

8. Boot disk selection window will open. Specify path to downloaded **Staffcop.iso** by clicking **file** icon to the right from disk letter;



Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.

The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.

staffcop_server_STABLE.iso (534,44 MB)

Figure 6.

9. Click **Start**;

10. Specify system language, keyboard layout (Figure 7 – 14) in the next dialog window. Installation will be conducted in auto mode (Figure 16);

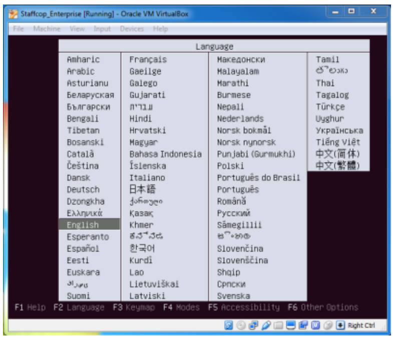
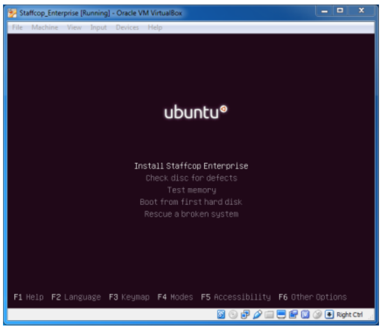
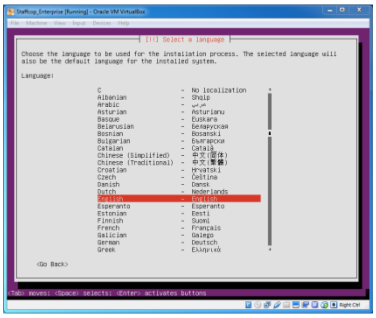


Figure 7.


Staffcop_Enterprise [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ubuntu
Right Ctrl

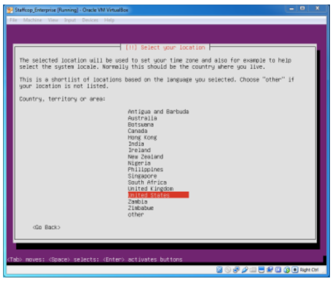
```
Install Staffcop Enterprise
Check disc for defects
Test memory
Boot from first hard disk
Rescue a broken system

F1 Help  F2 Language  F3 Keymap  F4 Modes  F5 Accessibility  F6 Other Options
```

Figure 8.


Staffcop_Enterprise [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

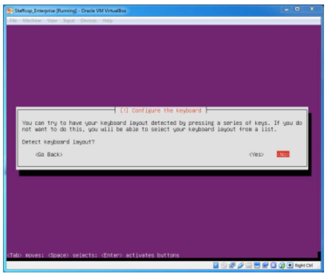
```
[!!] Select a language

Choose the language to be used for the installation process. The selected language will
also be the default language for the installed system.

Language:

             C                        -  No localization
             Albanian                 -  Shqip
             Arabic                   -  عربي
             Asturian                 -  Asturianu
             Basque                   -  Euskara
             Belarusian               -  Беларуская
             Bosnian                  -  Bosanski
             Bulgarian                -  Български
             Catalan                  -  Català
             Chinese (Simplified)     -  中文(简体)
             Chinese (Traditional)    -  中文(繁體)
             Croatian                 -  Hrvatski
             Czech                    -  Čeština
             Danish                   -  Dansk
             Dutch                    -  Nederlands
             English                  -  English
             Esperanto                -  Esperanto
             Estonian                 -  Eesti
             Finnish                  -  Suomi
             French                   -  Français
             Galician                 -  Galego
             German                   -  Deutsch
             Greek                    -  Ελληνικά

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 9.


Staffcop_Enterprise [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

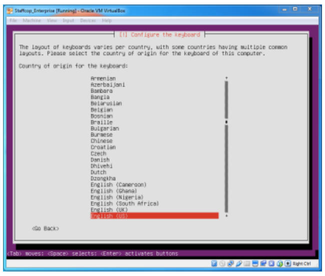
```
[!!] Select your location

The selected location will be used to set your time zone and also for example to help
select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if
your location is not listed.

Country, territory or area:

                         Antigua and Barbuda
                         Australia
                         Botswana
                         Canada
                         Hong Kong
                         India
                         Ireland
                         New Zealand
                         Nigeria
                         Philippines
                         Singapore
                         South Africa
                         United Kingdom
                         United States
                         Zambia
                         Zimbabwe
                         other

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 10.


Staffcop_Enterprise [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

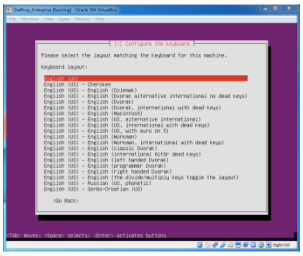
```
[!] Configure the keyboard

You can try to have your keyboard layout detected by pressing a series of keys. If you do
not want to do this, you will be able to select your keyboard layout from a list.

Detect keyboard layout?

    <Go Back>                                                    <Yes>    <No>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 11.


Staffcop_Enterprise [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
[!] Configure the keyboard

The layout of keyboards varies per country, with some countries having multiple common
layouts. Please select the country of origin for the keyboard of this computer.

Country of origin for the keyboard:

                  Armenian
                  Azerbaijani
                  Bambara
                  Bangla
                  Belarusian
                  Belgian
                  Bosnian
                  Braille
                  Bulgarian
                  Burmese
                  Chinese
                  Croatian
                  Czech
                  Danish
                  Dhivehi
                  Dutch
                  Dzongkha
                  English (Cameroon)
                  English (Ghana)
                  English (Nigeria)
                  English (South Africa)
                  English (UK)
                  English (US)

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

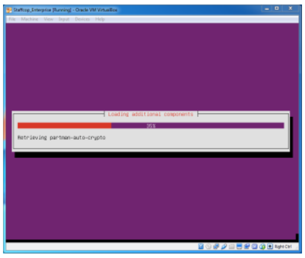
Figure 12.



Staffcop_Enterprise [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
[!] Configure the keyboard

Please select the layout matching the keyboard for this machine.

Keyboard layout:

English (US)
English (US) - Cherokee
English (US) - English (Colemak)
English (US) - English (Dvorak alternative international no dead keys)
English (US) - English (Dvorak)
English (US) - English (Dvorak, international with dead keys)
English (US) - English (Macintosh)
English (US) - English (US, alternative international)
English (US) - English (US, international with dead keys)
English (US) - English (US, with euro on 5)
English (US) - English (Workman)
English (US) - English (Workman, international with dead keys)
English (US) - English (classic Dvorak)
English (US) - English (international AltGr dead keys)
English (US) - English (left handed Dvorak)
English (US) - English (programmer Dvorak)
English (US) - English (right handed Dvorak)
English (US) - English (the divide/multiply keys toggle the layout)
English (US) - Russian (US, phonetic)
English (US) - Serbo-Croatian (US)

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 13.

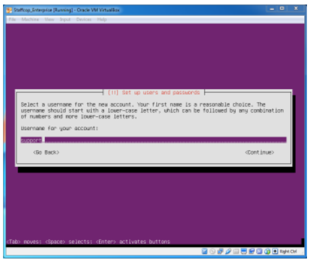


Staffcop_Enterprise [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Loading additional components
35%
Retrieving partman-auto-crypto
```

Figure 14.

11. Specify **Username**;

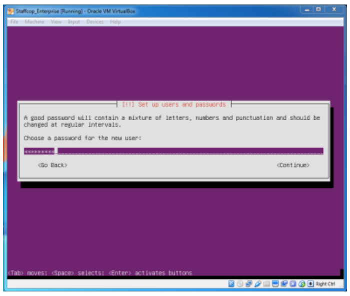


Staffcop_Enterprise [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
[!!] Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The
username should start with a lower-case letter, which can be followed by any combination
of numbers and more lower-case letters.

Username for your account:

support

    <Go Back>                                                        <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 15.

12. Choose a **password** for the new user;



Staffcop_Enterprise [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
[!!] Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be
changed at regular intervals.

Choose a password for the new user:

*********

    <Go Back>                                                        <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 16.

13. Specify your time zone.

Note: Password to admin part may contain any symbols except: “ ’ $ /

After installation is complete, enter login/password to virtual machine. Open any web browser and enter StaffCop Server IP address. **StaffCop Enterprise** admin panel will open.

Note: To determine IP, execute the following command **sudo ifconfig**.

Removing StaffCop Enterprise Server from VM VirtualBox

To remove StaffCop bundle, access StaffCop Enterprise Server console on VM VirtualBox and use the following command: sudo apt-get purge staffcop.

Installing StaffCop Enterprise Server under Linux OS

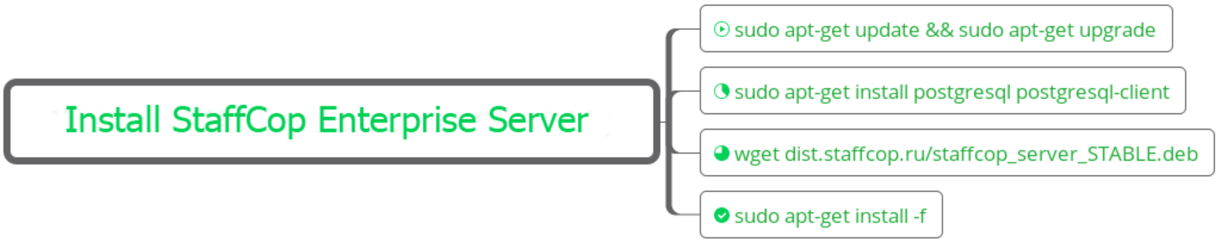

Install StaffCop Enterprise Server
sudo apt-get update && sudo apt-get upgrade
sudo apt-get install postgresql postgresql-client
wget dist.staffcop.ru/staffcop_server_STABLE.deb
sudo apt-get install -f

Figure 17. Install StaffCop Enterprise Server.

The easiest way to install StaffCop on existing and clean (i.e. without additional programs, graphics, web servers, LAMP and etc.) Ubuntu server, is the following:
wget -P /tmp/ -N dist.staffcop.com/utils/installR.sh && sudo bash /tmp/installR.sh

To install StaffCop Enterprise Server manually on already installed Linux OS (64bit), install postgreSQL packets by executing the following commands step-by-step:

1. sudo apt-get update && sudo apt-get upgrade;
2. sudo apt-get install postgresql postgresql-client;
3. Download StaffCop Enterprise installation pack by executing the following command: wget http://www.staffcop.com/img_distr/staffcop_server_STABLE.deb ;

4. After the download will be completed, execute installation command:
   sudo dpkg -i staffcop_server_STABLE.deb;

5. sudo apt-get install -f

   Installation is executed automatically. You just have to specify StaffCop Server IP address (or leave this field empty to use the current one) and password for accessing the server under admin account.

   Note: Password to admin part may contain any symbols except: “ ’ $ /

   Open any web browser and enter StaffCop Server IP address to open StaffCop Enterprise admin panel.

Note: If web interface of admin panel is not displayed correctly, then execute the following command: sudo staffcop init.

Removing StaffCop Enterprise Server under Linux OS

To remove StaffCop bundle on the server part, execute the following command:

```
sudo apt-get purge staffcop
```

Possible issues occurring during StaffCop Enterprise Server installation and how to fix them

In most cases, upgrade process is conducted smoothly.

Sometimes issues occur due to incorrect settings of operation system.

- In order to install StaffCop Enterprise correctly Internet connection is required. Before launching the installation, please check if your server is connected to Internet.

- Before installation, please check if there is enough free space on your hard disk.

Installation of StaffCop Enterprise Agent

System requirements

Minimum system requirements:

1) OS: Windows 8, Windows 7, Vista, Windows Server 2003, 2008, 2012.
2) Processor: Intel Celeron 1.8 GHz;
3) RAM: 1 Gb (to work on terminal server RAM should be expanded by 256 Mb per each user);
4) Disk space: 5 Gb.

Recommended system requirements:

- OS: Windows 8, Windows 7, Vista, Windows Server 2003, 2008, 2012.
- Processor: Intel Core2Duo 2.2 GHz;
- RAM: 2 Gb (to work on terminal server RAM should be expanded by 256 Mb per each user);
- Disk space: 5 Gb.

ATTENTION! Because Microsoft officially stopped supporting OS Windows XP, users installing StaffCop Enterprise Agents on workstations running under this OS might encounter issues during installation and deployment.

Adding exceptions for antivirus

In order for antivirus not to consider StaffCop Agent as threat, add the following file paths to the list of exceptions in this antivirus software:

For 32-bit systems:

Folders:

- c:\Windows\System32\TimeControlSvc\
- c:\Windows\System32\TimeControlSvc\Proxy\
- c:\Windows\System32\config\systemprofile\AppData\Roaming\TimeSvc3\

Files:

- c:\Windows\System32\TimeControlSvc\dpinst_32.exe
- c:\Windows\System32\TimeControlSvc\vmnetdrv32.exe
- c:\Windows\System32\TimeControlSvc\vmnetdrv64.exe
- c:\Windows\System32\TimeControlSvc\sysprotect.exe
- c:\Windows\System32\TimeControlSvc\Proxy\NtControlSvc.exe
- c:\Windows\System32\TimeControlSvc\Proxy\PCController.exe
- c:\Windows\System32\TimeControlSvc\Proxy\ProxyConfigurator.exe
- c:\Windows\System32\TimeControlSvc\Proxy\RegisterLSP.exe
- c:\Windows\System32\TimeControlSvc\Proxy\RegisterLSP64.exe
- c:\Windows\System32\TimeControlSvc\Proxy\RunHiddenConsole.exe

For 64-bit systems:

Folders:

- c:\Windows\SysWOW64\TimeControlSvc\
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\
- c:\Windows\System32\config\systemprofile\AppData\Roaming\TimeSvc3\

Files:

- c:\Windows\SysWOW64\TimeControlSvc\dpinst_64.exe
- c:\Windows\SysWOW64\TimeControlSvc\vmnetdrv32.exe
- c:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe
- c:\Windows\SysWOW64\TimeControlSvc\sysprotect64.exe
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\NtControlSvc.exe
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\PCController.exe
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\ProxyConfigurator.exe
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\RegisterLSP.exe
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\RegisterLSP64.exe

- c:\Windows\SysWOW64\TimeControlSvc\Proxy\RunHiddenConsole.exe

Types of StaffCop Enterprise Agent installation

Remote installation

To start installation of StaffCop Enterprise Agent, download installation file by completing the following steps:

1) Launch StaffCop Enterprise admin panel by entering StaffCop Enterprise server address in any web browser;

2) Click admin panel icon and download installation file of StaffCop Enterprise Agent by clicking **Download agent installer**.

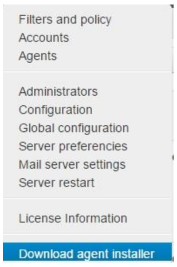
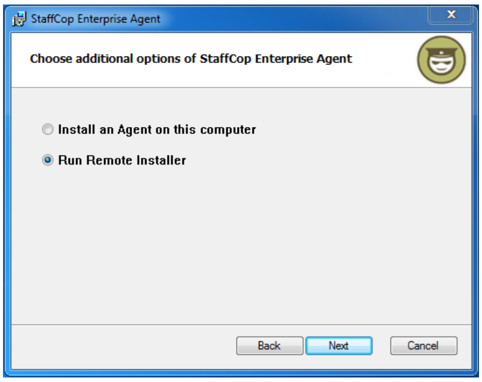


Figure 18. Download agent installer.

3) After the agent is installed continue installation process and launch the Agent installer **agent-[server_IP].msi**. Follow installer hints;

4) In additional installation options select – **Run Remote Installer**;


StaffCop Enterprise Agent

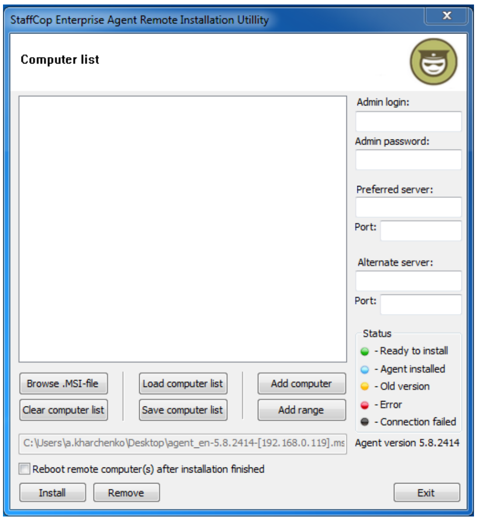
Choose additional options of StaffCop Enterprise Agent

○ Install an Agent on this computer

● Run Remote Installer

Figure 19. Run Remote Installer.

5) **Computer list** window will open;

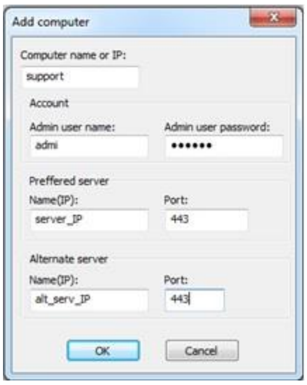


C:\Users\a.kharchenko\Desktop\agent_en-5.8.2414-[192.168.0.119].ms

□ Reboot remote computer(s) after installation finished

Figure 20. Remote installation utility.

6) There are two ways to select computers (workstations) that will be monitored:
   a) Add computer names or IP addresses: click **Add computer** and enter computer name or IP address in required fields;



Computer name or IP: support

Admin user name: admi

Admin user password: ••••••

Name(IP): server_IP

Port: 443

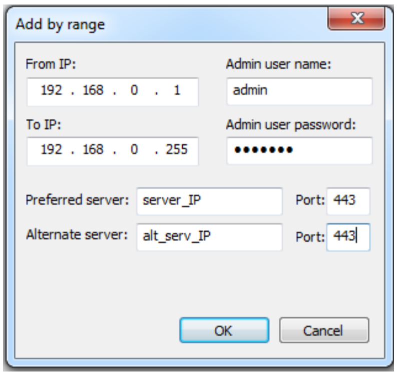
Name(IP): alt_serv_IP

Port: 443

Figure 21. Add computer.

OR

Specify IP range or workstations: click **Add range** and specify the beginning and end of IP range by filling out required fields.



From IP: 192 . 168 . 0 . 1

Admin user name: admin

To IP: 192 . 168 . 0 . 255

Admin user password: •••••••

Preferred server: server_IP

Port: 443

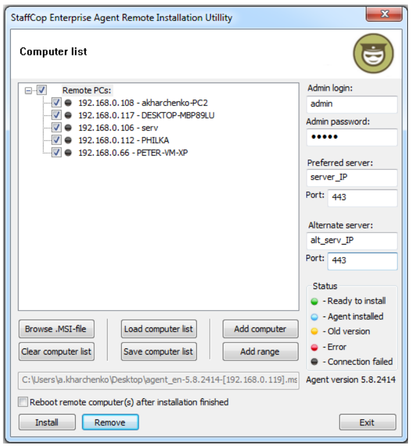
Alternate server: alt_serv_IP

Port: 443

Figure 22. Add range.

Note: Do not forget to specify correct admin data on remote workstations. If you skip this step, installation will not be completed!

7) After you click **OK**, all workstations will be displayed in the list;



StaffCop Enterprise Agent Remote Installation Utillity

Computer list

☑ Remote PCs:
- ☑ ● 192.168.0.108 - akharchenko-PC2
- ☑ ● 192.168.0.117 - DESKTOP-MBP89LU
- ☑ ● 192.168.0.106 - serv
- ☑ ● 192.168.0.112 - PHILKA
- ☑ ● 192.168.0.66 - PETER-VM-XP

Admin login: admin

Admin password: •••••

Preferred server: server_IP

Port: 443

Alternate server: alt_serv_IP

Port: 443

Status
- ● - Ready to install
- ● - Agent installed
- ● - Old version
- ● - Error
- ● - Connection failed

C:\Users\a.kharchenko\Desktop\agent_en-5.8.2414-[192.168.0.119].ms

Agent version 5.8.2414

□ Reboot remote computer(s) after installation finished

Figure 23. Remote PCs.

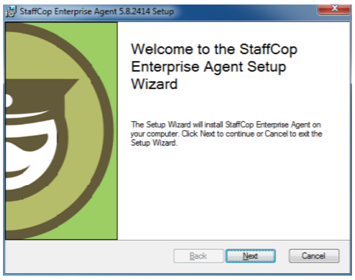
8) After you click **Install** installation of StaffCop Enterprise Agents will be initiated on specified workstations.

Corresponding dialog window is displayed at the end of installation and all StaffCop Enterprise Agents will be available in the admin panel.

Local installation

If for some reason it is impossible to launch multiple installation, you can install StaffCop Enterprise Agent manually. Installation time is directly proportional to number of workstations in your network.

1. Launch the Agent installer **agent-[server_IP].msi**. Follow installer's hints;
2. Installation Constructor of StaffCop Agent will open. Click **Next**;



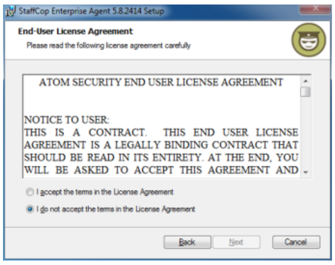
StaffCop Enterprise Agent 5.8.2414 Setup

Welcome to the StaffCop Enterprise Agent Setup Wizard

The Setup Wizard will install StaffCop Enterprise Agent on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure 24. StaffCop Enterprise Agent Setup Wizard.

3. Read the license agreement of end user. Click **Next**;


StaffCop Enterprise Agent 5.8.2414 Setup

End-User License Agreement

Please read the following license agreement carefully

ATOM SECURITY END USER LICENSE AGREEMENT

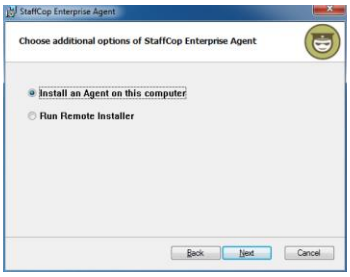
NOTICE TO USER:
THIS IS A CONTRACT. THIS END USER LICENSE AGREEMENT IS A LEGALLY BINDING CONTRACT THAT SHOULD BE READ IN ITS ENTIRETY. AT THE END, YOU WILL BE ASKED TO ACCEPT THIS AGREEMENT AND

○ I accept the terms in the License Agreement

● I do not accept the terms in the License Agreement

Figure 25. End user license agreement.

4. Select **Install an Agent on this computer** in additional installation options. Click **Next**;


StaffCop Enterprise Agent

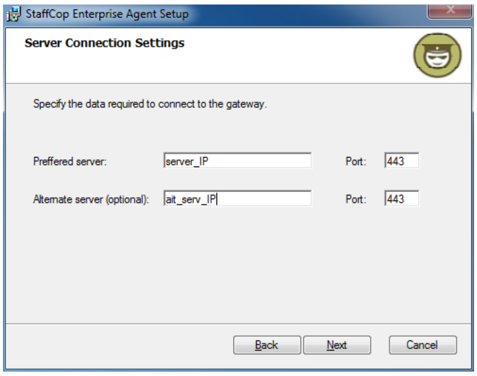
Choose additional options of StaffCop Enterprise Agent

● Install an Agent on this computer

○ Run Remote Installer

Figure 26. Additional options.

5. Specify IP address of StaffCop Enterprise Server. Click **Next**;


StaffCop Enterprise Agent Setup

Server Connection Settings

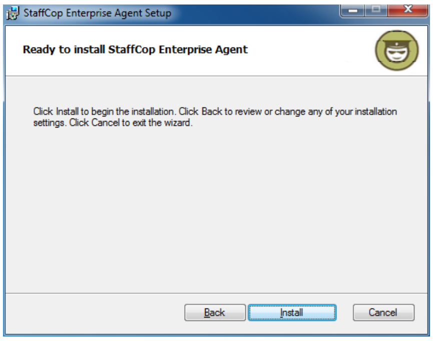
Specify the data required to connect to the gateway.

Preffered server: server_IP Port: 443

Alternate server (optional): alt_serv_IP Port: 443

Figure 27. StaffCop Enterprise Server parameters.

6. Everything is ready for installation. On the next screen, you can read configuration overview before launching installation. If you missed some steps, simply click **Back** to go back to that screen and change settings. If you finished configuring, click **Install**;



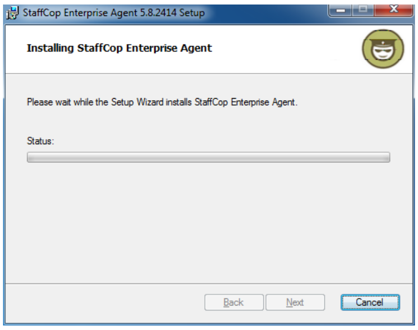
StaffCop Enterprise Agent Setup

Ready to install StaffCop Enterprise Agent

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Figure 28. Initiating StaffCop Enterprise Agent installation.

7. Installation progress bar will be displayed in Installation Constructor. Please note installation process might take several minutes to complete depending on the speed of your PC;



StaffCop Enterprise Agent 5.8.2414 Setup

Installing StaffCop Enterprise Agent

Please wait while the Setup Wizard installs StaffCop Enterprise Agent.

Status:

Figure 29. Installation progress bar.

8. After successful installation, click **Finish**. You will be prompted to restart your PC. Click **Yes** for immediate restart, or click **No** to restart your PC at more convenient time.

Installing Agent using Active Directory

Detailed installation instructions are available on the website in **FAQ section**:

- Installing StaffCop Enterprise Agent using Active Directory (Win 2000/2003);
- Installing StaffCop Enterprise Agent using Active Directory (Win 2008).

1. Copy Agent distributive **Agent.msi** on domain controller. Move it to **C:\sc** folder on your computer and share it as **\\domain_controller_name\sc$**;

2. In **Start** menu (or **Start**>>**Programs in Windows 2000**) select **Administrative Tools/Active Directory Users and Computers**;

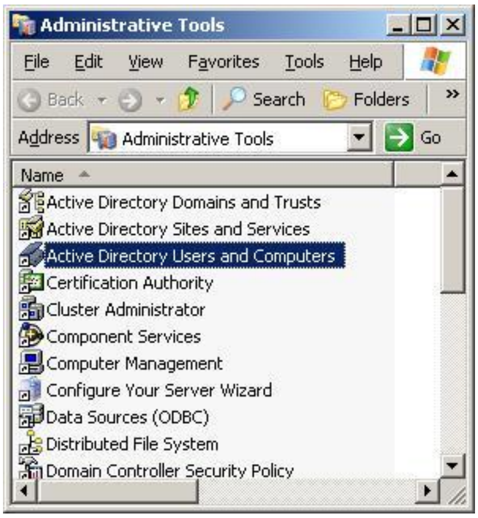

Administrative Tools
File Edit View Favorites Tools Help
Back Search Folders
Address Administrative Tools Go
Name
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers
Certification Authority
Cluster Administrator
Component Services
Computer Management
Configure Your Server Wizard
Data Sources (ODBC)
Distributed File System
Domain Controller Security Policy

Figure 30. Administrative Tools.

3. Create new **Subsection** in domain, which include workstations on which the Agents will be installed, and call it, for example, StaffCop.

   To do this:
   — Select **Create**/**Organization Unit** in the domain menu. In the new window enter the name of new subsection and click **OK**. Include all workstations, on which you will install the Agents, in newly created subsection.

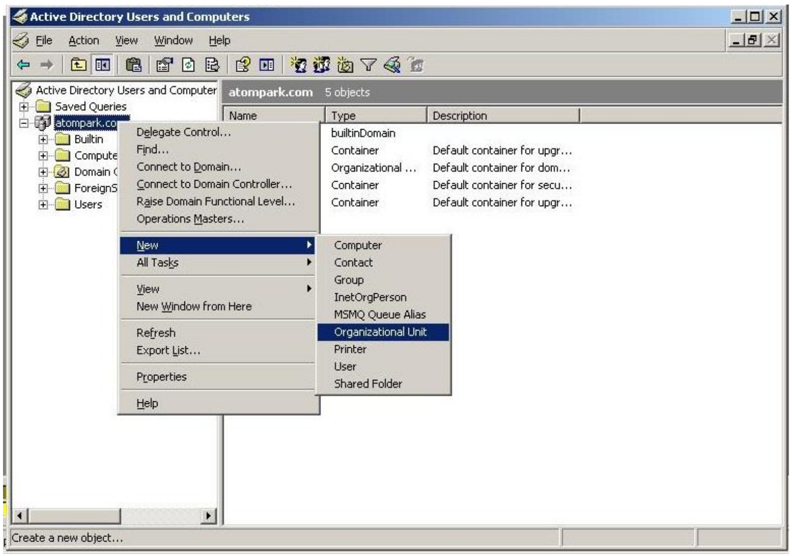
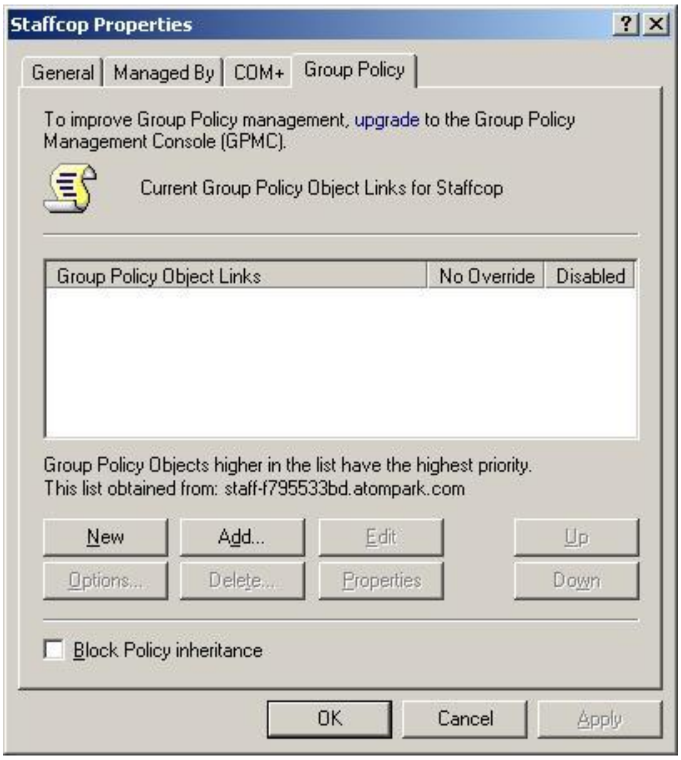


Figure 31. Domain menu New.

4. Open **Group policy management** editor window;

   Do the following:
   — In **Windows 2000/2003:** Select **Properties** in the context menu of new **StaffCop** subdivision. From **Properties** window go to **Group policy** tab;



To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

Current Group Policy Object Links for Staffcop

Group Policy Object Links	No Override	Disabled

Group Policy Objects higher in the list have the highest priority.
This list obtained from: staff-f795533bd.atompark.com

□ Block Policy inheritance

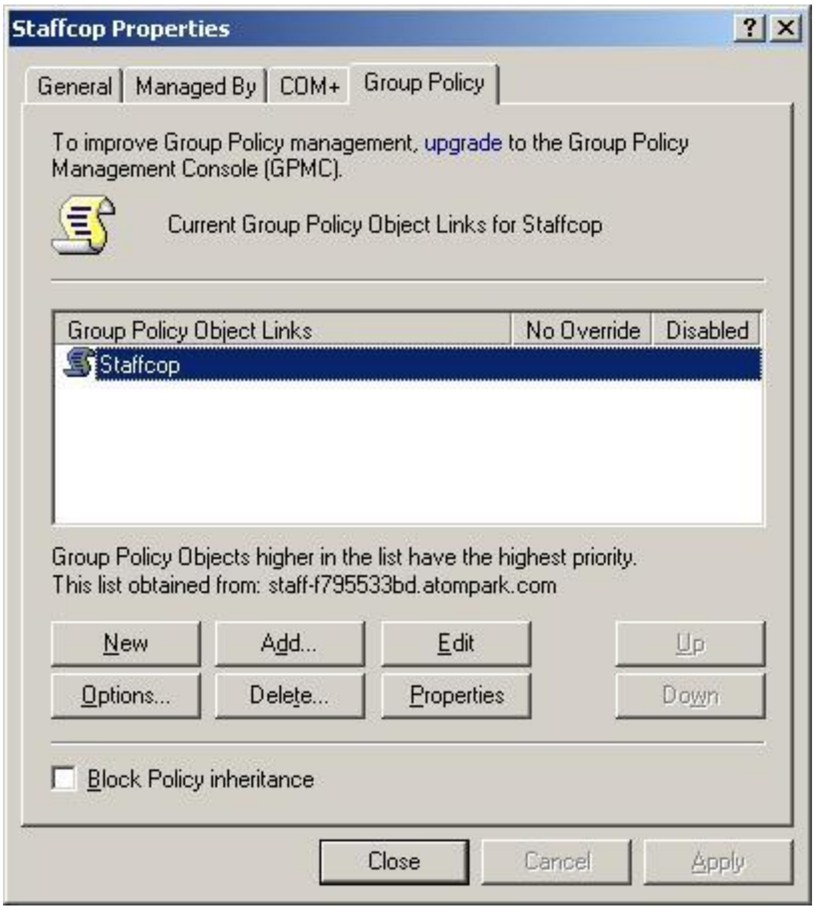
Figure 32. Group policy window.

— In **Windows 2008 Server:** Click **Start - Administrating - Group policy** management.

5. Specify group policy for new **StaffCop** subdivision.

   Do the following:
   — In **Windows 2000/2003:** Click **Add** and create **StaffCop** element. Double click its name;

   — In **Windows 2008:** In the context menu of new *StaffCop* subdivision select **Create GPO object in current domain and assign it to...** In the next window specify the name of a new group policy object and click **OK**. Click **Change...** in the context menu of new group policy;



To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

Current Group Policy Object Links for Staffcop

Group Policy Object Links	No Override	Disabled
Staffcop		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: staff-f795533bd.atompark.com

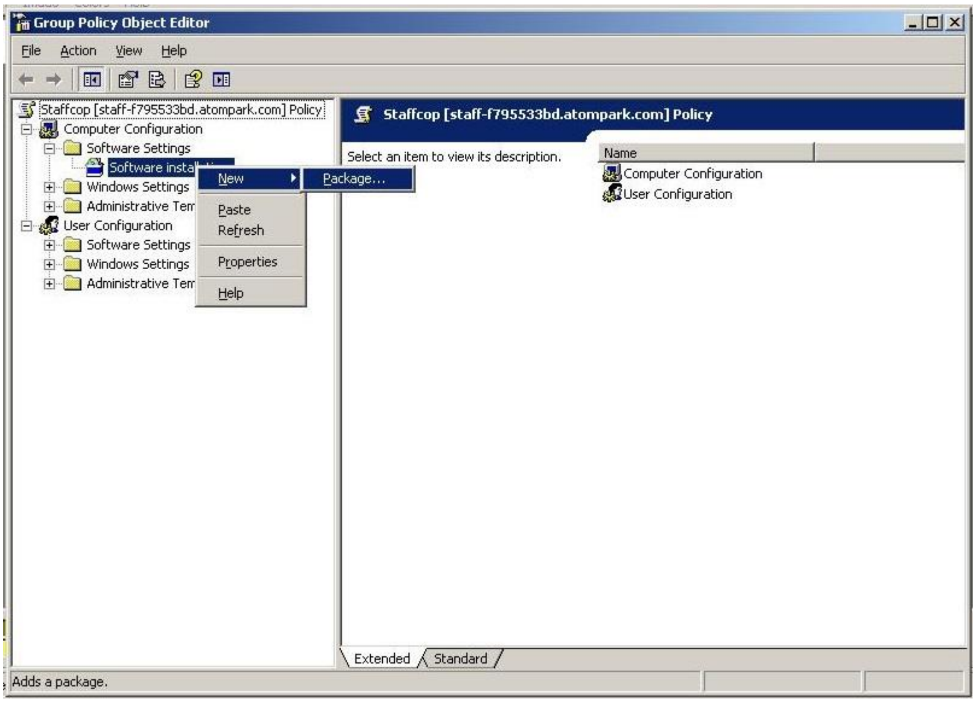
□ Block Policy inheritance

Figure 33. StaffCop Group policy.

6. In Editor of group policy management window configure settings for previously created group policy:

   Do the following:
   — In **Windows 2000/2003:** select **PC configuration - Program configuration - Programs installation;**

   — In **Windows 2008:** Select **PC configuration - Policies - Program configuration - Programs installation**;



Select an item to view its description.

Adds a package.

Figure 34. Group policy management editor.

7. Select **New>> Package** in **Programs installation** context menu;

8. Specify the Agent installation pack:

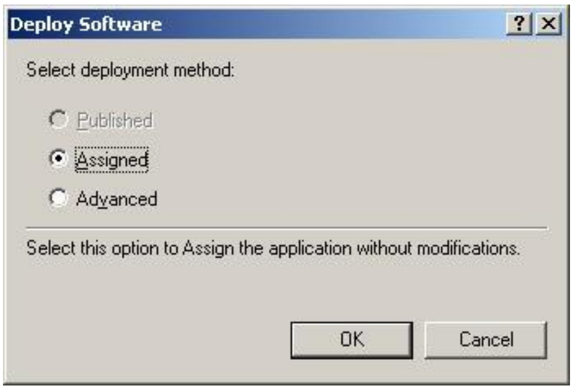
   Do the following:

   — specify address of network shared resource. Specify a path to catalog containing the pack as network address even if the catalog is accessible locally: **«\\domain_controller_name\sc\Agent.msi»**.

   Important! .msi file name should contain server IP or server name in square brackets.

   Example: **agent-5.8.2396-[192.168.1.101].msi** or **agent-5.8.2396-[staffcop-sky.ru].msi**

9. **Deploy Software** window will open. Select **Assigned**. Click **OK**;


Deploy Software

Select deployment method:

○ Published

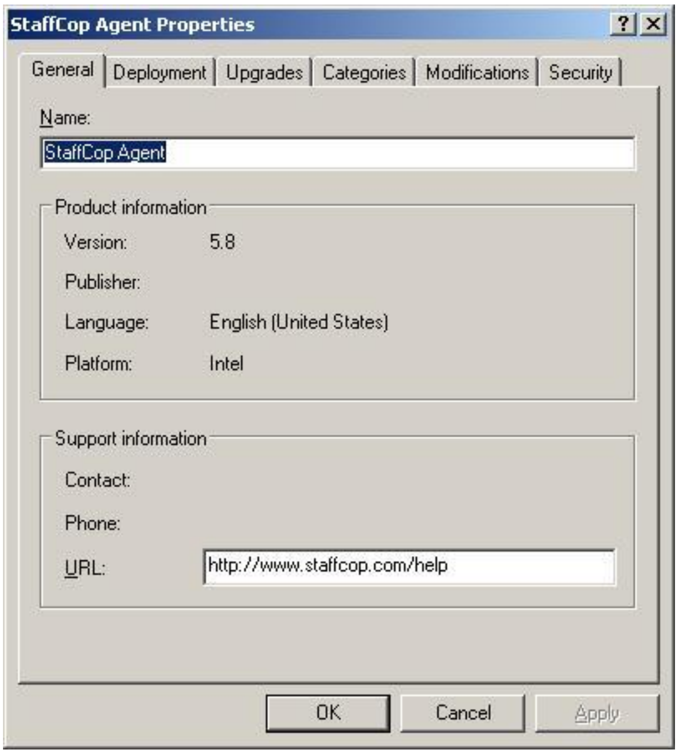
● Assigned

○ Advanced

Select this option to Assign the application without modifications.

Figure 35. Select deployment method.

10. New item, called **StaffCop Agent**, will appear in group policy management editor window. Select it and click **Properties** in the context menu.


StaffCop Agent Properties

Name: StaffCop Agent

Product information

Version: 5.8

Publisher:

Language: English (United States)

Platform: Intel

Support information

Contact:

Phone:

URL: http://www.staffcop.com/help

Figure 36. StaffCop Agent properties.

11. Review all tabs of the opened window of package properties and click **OK**. Close all windows while saving all changes you have made.

Attention! Make sure that you checked **Install current application** when accessing the system in **Deployment Software**.

12. The Agent will be installed on selected workstations as soon as they will be registered in domain.

Adding exceptions for antivirus software

In order for your antivirus not to consider StaffCop Enterprise Agent as a threat, add the following file paths to the list of exceptions in your antivirus software:

For 32-bit systems:

Folders:

- c:\Windows\System32\TimeControlSvc\
- c:\Windows\System32\TimeControlSvc\Proxy\
- c:\Windows\System32\config\systemprofile\AppData\Roaming\TimeSvc3\

Files:

- c:\Windows\System32\TimeControlSvc\dpinst_32.exe
- c:\Windows\System32\TimeControlSvc\vmnetdrv32.exe
- c:\Windows\System32\TimeControlSvc\vmnetdrv64.exe
- c:\Windows\System32\TimeControlSvc\sysprotect.exe
- c:\Windows\System32\TimeControlSvc\Proxy\NtControlSvc.exe
- c:\Windows\System32\TimeControlSvc\Proxy\PCController.exe
- c:\Windows\System32\TimeControlSvc\Proxy\ProxyConfigurator.exe
- c:\Windows\System32\TimeControlSvc\Proxy\RegisterLSP.exe
- c:\Windows\System32\TimeControlSvc\Proxy\RegisterLSP64.exe
- c:\Windows\System32\TimeControlSvc\Proxy\RunHiddenConsole.exe

For 64-bit systems:

Folders:

- c:\Windows\SysWOW64\TimeControlSvc\
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\
- c:\Windows\System32\config\systemprofile\AppData\Roaming\TimeSvc3\

Files:

- c:\Windows\SysWOW64\TimeControlSvc\dpinst_64.exe
- c:\Windows\SysWOW64\TimeControlSvc\vmnetdrv32.exe
- c:\Windows\SysWOW64\TimeControlSvc\vmnetdrv64.exe
- c:\Windows\SysWOW64\TimeControlSvc\sysprotect64.exe
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\NtControlSvc.exe
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\PCController.exe
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\ProxyConfigurator.exe
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\RegisterLSP.exe
- c:\Windows\SysWOW64\TimeControlSvc\Proxy\RegisterLSP64.exe

- c:\Windows\SysWOW64\TimeControlSvc\Proxy\RunHiddenConsole.exe

StaffCop Enterprise Interface

StaffCop Enterprise interface consists of the following elements:

1. Upper navigation panel:

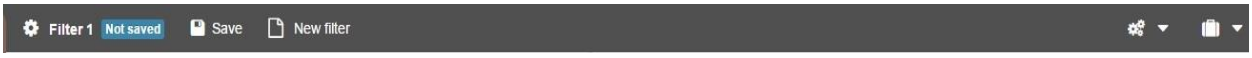


Figure 37. Upper navigation panel.

Where:

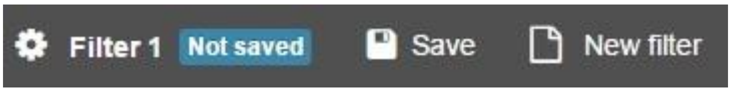


Figure 38. Filters menu.

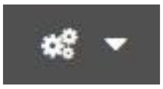


Figure 39. Admin menu icon.

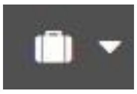


Figure 40. Main menu icon.

2. Left navigation panel:

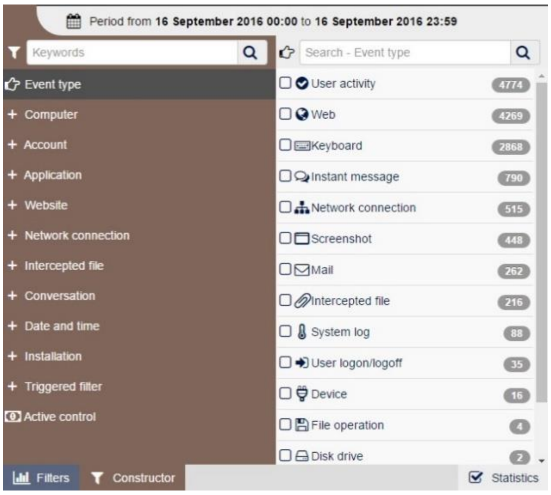
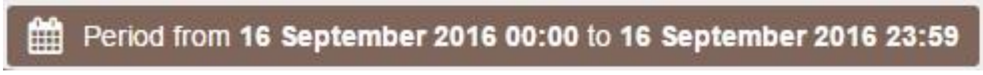


Figure 41. Left navigation panel.

2.1 Widget to select data and time interval;



Period from **16 September 2016 00:00** to **16 September 2016 23:59**

Figure 42. Widget to select data and time interval.

2.2 Find event type: enter event type in the search field;

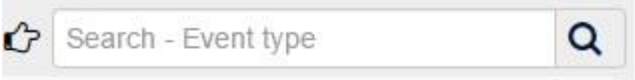


Figure 43. Search event type field.

2.3 Sidebar to select required monitoring dimension;

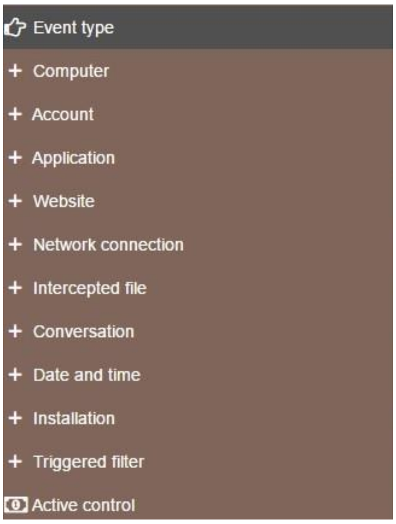


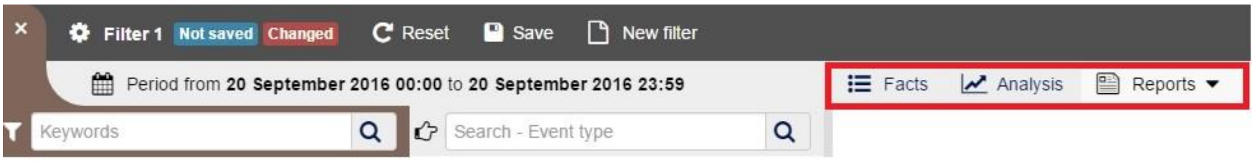
Figure 44. Monitoring dimensions.

2.4 Aggregate bar where data aggregated by various events is displayed;

2.5 Button to turn on counter of events in aggregate bar;

2.6 Switch buttons **Filters/Constructor**.

3. Data display panel:



Period from **20 September 2016 00:00** to **20 September 2016 23:59**

Figure 45. Data Display Panel.

3.1 **Facts**;
3.2 **Analysis**;
3.3 **Reports**.

4. Lower panel:

– forced data refresh in admin part.

Mode of operation

The main mode of StaffCop Enterprise v. 3.1 operation is the following:

1. Find required information using consequent overlapping of various filters and/or using full-text search in the Constructor (Navigation panel)

2. Select required mode of data visualization in **Data Visualization Panel**. The system contains large range of events views (Table, List, etc.), for statistics analysis (Graphs, Line charts, Pie charts, etc.), and for viewing efficiency reports.

3. Save new filter set under any name (the report will be stored in root folder of **Filters** section, relieving you from necessity to overlap same filters over and over again in the next StaffCop Enterprise sessions).

4. If required, set **Productive** to Filter, enable **Notifications of new facts, scheduled reports e-mailing** and configure other **Properties**.

5. For more convenience, move the report inside the section’s hierarchy tree. To do this, go to **Admin** - **Filters and Policy**. While pressing mouse cursor on “plus”, DRAG created **Filter** to required folder.

Features

StaffCop Enterprise is a multifunctional software applied to a wide range of tasks, such as information security, employee work time tracking, and improvement of employee efficiency. Fine-tuning of the system access rights enables managers of different departments to use it in accordance with their business profiles.

Main menu

Upper panel

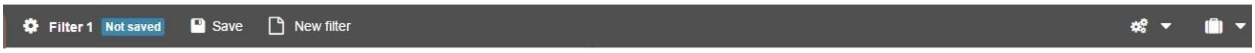


Figure 46. Upper panel.

Filters menu

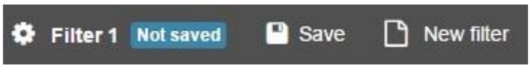


Figure 47. Filters menu.

Use **Filters** menu to work with filters. In this menu you can create new filter by clicking **New filter,** save filter under any name **Save**, reset filter settings, and go to fine-tuning mode of filter settings.

To go back from filter **Properties** menu, click **Constructor**.

Use **Admin menu** to configure StaffCop Enterprise. The set of menu items depends on admin role and set of rights:

- Filters and policy;
- Accounts;
- Agents;
- Administrators;
- Configuration;
- Global configuration;
- Server preferencies;
- Mail server settings;
- Server restart;
- License information;
- Download agent installer.

Main menu

Main menu of StaffCop Enterprise admin (user) contains the following:

- **About**: info about the Server and Agent versions;
- **Help**: current StaffCop Enterprise User Guide;
- **Support**: technical support request form;
- **Change password**: to change password for accessing the system's web interface;
- **Logout**: please note that the session is not terminated automatically in web browser.

Admin menu

Use **Admin** menu to configure StaffCop Enterprise. Admin menu items may change according to admin roles and rights.

Filters and policy

In **Filters and policy** create, edit, remove filters and policies, and configure Filters tree structure.

Filters consist of two categories:

1. Use **Filters** to view data.

2. Use **Policies** (or **Active filters**) to configure the system settings, execute various service operations, and special processing and analysis of filtered data.

Filters

To create regular Filter, do the following:

1) On navigation panel click **Constructor** and find required data using consequent overlapping of various filters and/or using full-text;

2) On data visualization panel select type of view. The system contains a variety of modes to view events (**Table**, **List**, etc.), for statistics analysis (click **Analysis** and select **Linear diagram**, **Pie chart**, **Graph**) and for viewing efficiency reports;

3) Click **Save** in the upper menu to save the set of filters you have created under any name.

To edit filter properties, do the following:

In upper left corner of the main window click filter name.

OR

Click **Filters and policy** in **Admin** menu, and click filter name in filters and policies table.

Regular Filter should have Report type and you can set any productivity category to it.

Productivity category – there are five categories:

1. Premium;
2. Productive;
3. Neutral;
4. Unproductive;
5. Incident.

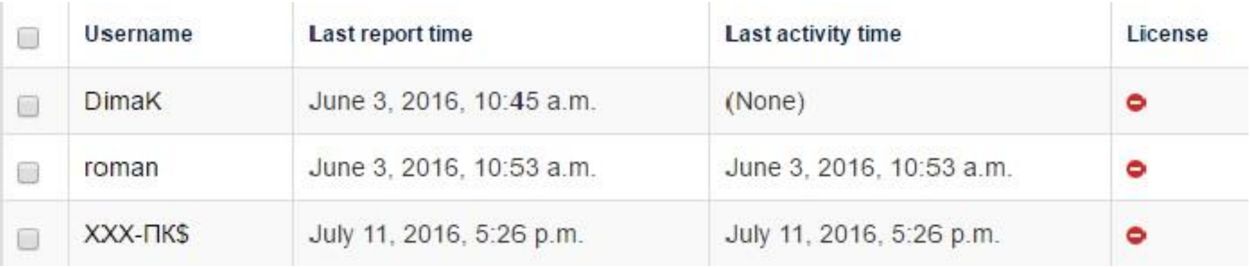
As a result, all events suitable for these filters will be aggregated according to their productivity.

Click **Category** and select required category in **Constructor** for corresponding report.

IMPORTANT! Do not checkmark **Activate filter processing** when creating regular Filters. This item exists for turning on/off **Active filters (Policies)**.

Profile

To access profiles of monitored workstations, go to **Accounts** in **Admin** menu. In profile summary of users of monitored workstations you see the following information: user name (1), time of the latest received report (2), time of the latest user activity (3).



□	Username	Last report time	Last activity time	License
□	DimaK	June 3, 2016, 10:45 a.m.	(None)	⛔
□	roman	June 3, 2016, 10:53 a.m.	June 3, 2016, 10:53 a.m.	⛔
□	XXX-ПК$	July 11, 2016, 5:26 p.m.	July 11, 2016, 5:26 p.m.	⛔

Figure 48. User profiles.

When you click profile name, User card containing all user information is displayed.

1. User name: displayed user name, initially retrieved from GUID (in case of domain users from Displayed name Active Directory). For convenient work, you can edit displayed user.

   StaffCop Enterprise supports synchronization with Active Directory, corresponding information from Active Directory is displayed in User card:

   - User name:
   - Full name:
   - Description:
   - Company:
   - Position:
   - Department/office:
   - Executive:
   - Phone number:
   - Skype:
   - E-mail:
   - Web page (If the Agent could not retrieve information from AD – the fields stay empty).

   If Active Directory is not used, you can enter all information into Profiles manually.

Additional information:

1) GUID: SID is used for the Agents registration and identification.
2) Last report time
3) Last activity time

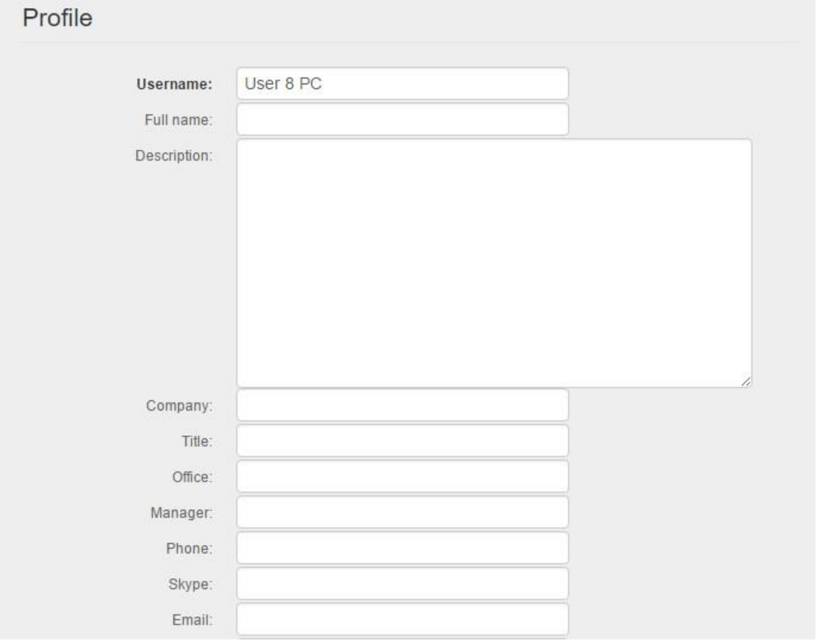
2. Last report time: time of receiving last report from selected user.
3. Last activity time: time of user latest activity.

In the next versions of StaffCop Enterprise User card functionality will be expanded significantly. We are planning to display the following user information in these versions:

1) History of information policy breaches;
2) Information received on the basis of intercepted data analytics (IM user accounts and alternative e-mail addresses, user pages in social networks, etc.);

Adding new user: new users are added automatically to the system when the Agent is registered on the server. There is no need to add users manually.

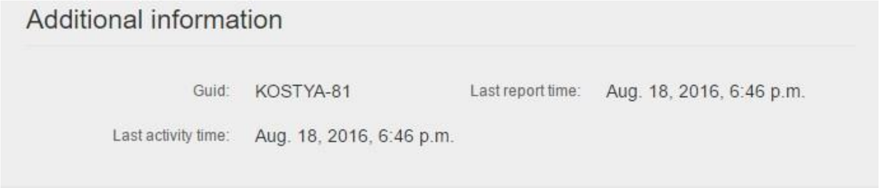
Editing user information: click user name to edit displayed name and other user info. User name editing window will open. You can change user name and add new info about the user in corresponding fields of displayed **Username** window.



Profile

Username: User 8 PC

Figure 49. Editing user profile. Main parameters.



Additional information

Guid: KOSTYA-81

Last report time: Aug. 18, 2016, 6:46 p.m.

Last activity time: Aug. 18, 2016, 6:46 p.m.

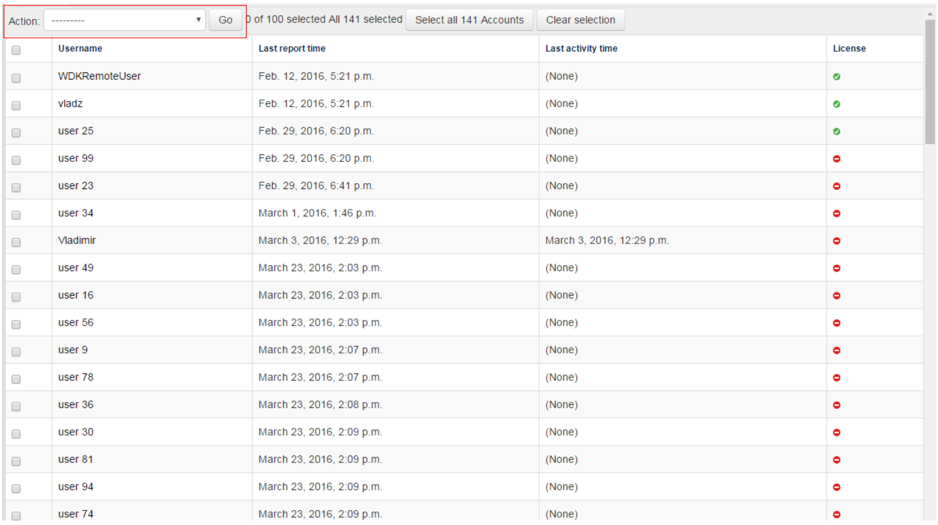
Figure 50. Additional information.

- System information. In this section, Guid and Username (displayed name) are displayed as well as last time the report from user workstation was sent and last activity time of the user;

- To change displayed name, in **Username** field change user name according to requirements:
- Profile. Specify different user data in corresponding fields:
  - **Description**: enter additional information about the user in this field.
  - **Company**: name of company, organization, or filial;
  - **Title**: specify user position in the company;
  - **Office**: specify user department in the company;
  - **Manager**: specify full name of user director, or head of user department;
  - **Phone**: business phone number;
  - **Skype**: specify user Skype ID;
  - **E-mail**: displayed business e-mail address
  - **WWW**: link to profile service page;

Click **Save** to save changes and return to **User profiles** screen.

On **User profiles** screen you can check several user accounts and select action from **Action** drop-down list (**Delete selected users**), and click **Execute**.



□	Username	Last report time	Last activity time	License
□	WDKRemoteUser	Feb. 12, 2016, 5:21 p.m.	(None)	✓
□	vladz	Feb. 12, 2016, 5:21 p.m.	(None)	✓
□	user 25	Feb. 29, 2016, 6:20 p.m.	(None)	✓
□	user 99	Feb. 29, 2016, 6:20 p.m.	(None)	⊖
□	user 23	Feb. 29, 2016, 6:41 p.m.	(None)	⊖
□	user 34	March 1, 2016, 1:46 p.m.	(None)	⊖
□	Vladimir	March 3, 2016, 12:29 p.m.	March 3, 2016, 12:29 p.m.	⊖
□	user 49	March 23, 2016, 2:03 p.m.	(None)	⊖
□	user 16	March 23, 2016, 2:03 p.m.	(None)	⊖
□	user 56	March 23, 2016, 2:03 p.m.	(None)	⊖
□	user 9	March 23, 2016, 2:07 p.m.	(None)	⊖
□	user 78	March 23, 2016, 2:07 p.m.	(None)	⊖
□	user 36	March 23, 2016, 2:08 p.m.	(None)	⊖
□	user 30	March 23, 2016, 2:09 p.m.	(None)	⊖
□	user 81	March 23, 2016, 2:09 p.m.	(None)	⊖
□	user 94	March 23, 2016, 2:09 p.m.	(None)	⊖
□	user 74	March 23, 2016, 2:09 p.m.	(None)	⊖

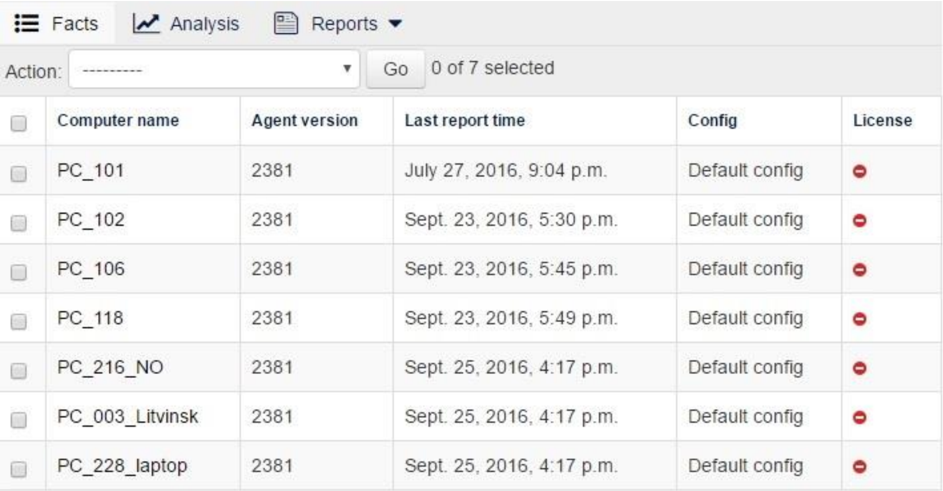
Figure 51. User profiles.

Agents

Summary information about workstations registered on StaffCop server is displayed on **Agents** screen:

3) **Computer name**: name of monitored computer;
4) **Agent version**: version of deployed Agent;
5) **Last report time**: time of sending last report to the server;
6) **Config**: configuration applied to corresponding computer;
7) **License** (in case of "floating" license).

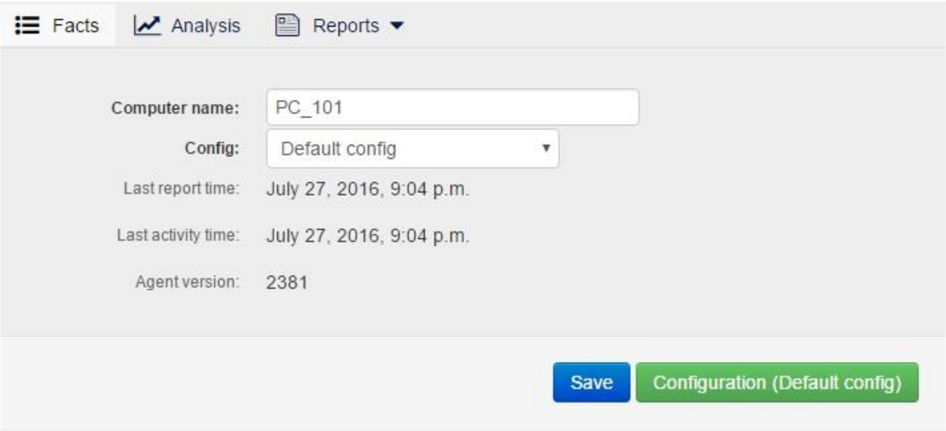
Computers (workstations) are added AUTOMATICALLY on the server! To add new workstation simply install the Agent on it. The Agents are automatically registered after installation on workstations, and aggregated information is transferred to the server and displayed on web interface as soon as the Agent is installed.



□	Computer name	Agent version	Last report time	Config	License
□	PC_101	2381	July 27, 2016, 9:04 p.m.	Default config	⛔
□	PC_102	2381	Sept. 23, 2016, 5:30 p.m.	Default config	⛔
□	PC_106	2381	Sept. 23, 2016, 5:45 p.m.	Default config	⛔
□	PC_118	2381	Sept. 23, 2016, 5:49 p.m.	Default config	⛔
□	PC_216_NO	2381	Sept. 25, 2016, 4:17 p.m.	Default config	⛔
□	PC_003_Litvinsk	2381	Sept. 25, 2016, 4:17 p.m.	Default config	⛔
□	PC_228_laptop	2381	Sept. 25, 2016, 4:17 p.m.	Default config	⛔

Figure 52. List of installed Agents.

In a lot of cases, computer (workstation) names in large enterprises have names that are difficult to remember, consisting of letters and numbers making it inconvenient to find specific workstation name. Computers with similar names can be found in dispersed networks. To resolve such situation you should click computer name in the list and edit it. After editing, click **Save** to save changes. To return to default configuration, click **Configuration (Default config)**.



Computer name: PC_101

Config: Default config

Last report time: July 27, 2016, 9:04 p.m.

Last activity time: July 27, 2016, 9:04 p.m.

Agent version: 2381

Figure 53. Editing Agent parameters.

Required configuration is applied to the Agent, when you select it from drop-down list.

Notifications of new facts, scheduled reports e-mailing

You can turn on notification about new events (alerts) and configure sending out reports according to schedule in **Notifications of new facts, scheduled reports e-mailing**.

To turn on notification do the following:

1. Checkmark **Display notifications about new facts** against **Notifications**;
2. Specify e-mail address to where alerts should be send in **E-mails to send notifications**;

Note: You can specify several e-mail addresses. Specify each e-mail in a new line.

To enable sending of reports according to schedule do the following:

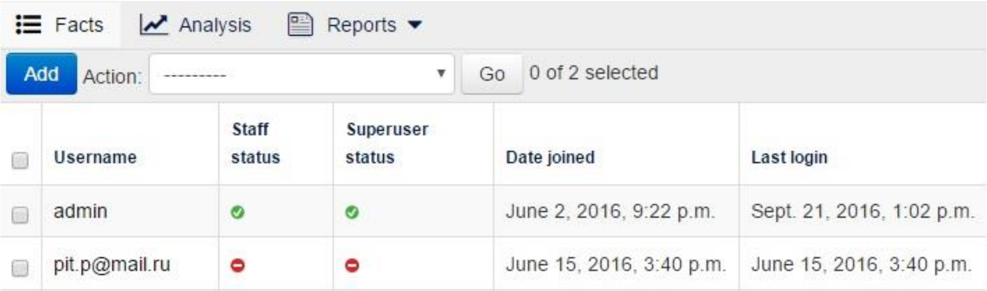
1. Select interval between sending out reports in **Schedule of report sending**:
   - **Do not send**: report won't be generated nor send;
   - **Daily**: the report about previous day's events is generated and send out each morning;
   - **Weekly**: the report about last week's events (from Monday 0:00 pm. to Sunday 11:59 pm.) is generated and send out each Monday;
   - **Monthly**: the report about last month's events is generated and send out each first day of a month.

2. Specify e-mail address to which the report should be send in **E-mails to send notifications**;

IMPORTANT! You cannot activate both: **Display notifications about new facts** and **Schedule of report sending** for the same Filter!

Administrators

Administrators: accounts of StaffCop users. You can assign specific role and corresponding access rights to each account. There are several predefined roles in the system, but you can create your own role with any rights. You can assign rights to review specific reports to any role. If no limiting report is selected, this account has access to all existing reports.



□	Username	Staff status	Superuser status	Date joined	Last login
□	admin	✓	✓	June 2, 2016, 9:22 p.m.	Sept. 21, 2016, 1:02 p.m.
□	pit.p@mail.ru	⊖	⊖	June 15, 2016, 3:40 p.m.	June 15, 2016, 3:40 p.m.

Figure 54. List of administrators.

User name

By selecting name in *User name* column you can go to editing user information and account settings, containing the following:

- **Username**: displays login name for accessing user account;
- **E-mail (POP/IMAP/SMTP)**: edit e-mail address in this field;
- **Password**: displays encrypted password. If there is no password specified it states “**Password is not specified”**. Also contains a link to change password for this account;
- **Last login**: displays information about admins last login to the system;
- **Date joined**: displays date of current admin account registration.

Access rights

Access rights: enables to configure access rights of admin account according to the following criteria:

- **Active**: check this item if admin should be specified as active. Uncheck this item instead of deleting this account;
- **Staff status**: check this item if user can access admin part of the web site.

- **Superuser status**: indicates that user has all rights without obvious specification.
- **Groups**: groups to which a user account is assigned. User has all rights specified in each group. Hold **Control** (or **Command** on Mac) to select several values. Click **plus** sign to add a new group and enter form adding required rights from **Available rights** list;
- **Access to reports**: select reports to be accessed by future admin account.
- **Access to events:** select events to be accessed by future admin account.
- **Access to constructor:** select constructor to be accessed by future admin account.

Note: If system admin rights should be assigned to a user, both items should be checked: **Staff status** and **Superuser status**.

Click **Delete** to delete an administrator account. To save changes and exit to main screen, click **Save**. Click **Save and continue editing** to save changes and remain on Administrator editing screen.

Account roles:

Super admin

Super admin has all rights.
For correct work, specify the following access rights for this account:

- Active;
- Personnel status;
- Superuser status.

Administrator

Administrator has all rights to be able to administrate the system, except rights to manage user accounts. Does not have access to events and reports.
For correct work, specify the following access rights:

- Active;
- Personnel status.

You can allow administrator access to events by adding **Access to** role.

Executive

Executive has access to all events and reports. Does not have access to Report Constructor. Access to admin part is denied. For correct work, specify the following access right: Active.

You can allow **Executive** access to the Constructor by adding additional role **Access to the Constructor.**

Please note that for correct work, **Executive** role with access to the Constructor should have the following access rights assigned:

- Active;
- Personnel status.

Human resources (HR)

HR has access to reports and statistics data. Does not have access to events. Access to admin part is denied. For correct work, specify the following access right to **HR** role: Active.

Security service

Security service has access to all events and reports. Also has access to Report Constructor. Access to admin part is denied. For correct work, specify the following access rights to HR role:

- Active;
- Personnel status.

Staff status

Displays status of activity of **Staff (system admin) status** specified in account editing form. See in description of **User name: Rights.**

✅ - **Staff status** enabled;

⛔ - **Staff status** disabled.

Super user status

Displays activity status of **Super user (system admin) status** specified in account editing form. See in description of **User name: Users**.

✅- **Super user status** enabled;

⛔- **Super user status** disabled.

Adding new account

Click **Add** to add new account, fill out form for entering data about new account should open. It will contain the following buttons:

- **Delete**: delete account;
- **Save**: create new account.

Fill out just one field **E-mail** in creating new account form. Accounts are identified by e-mail, and account names are the same as e-mail addresses specified during their creation.

Deleting administrator account

To delete specific administrator account, do the following:

1) Checkmark accounts you want to delete;
2) Click **Action** window;
3) In Action drop-down list click **Remove selected administrators**;
4) Click **Go**.

StaffCop Enterprise Configuration

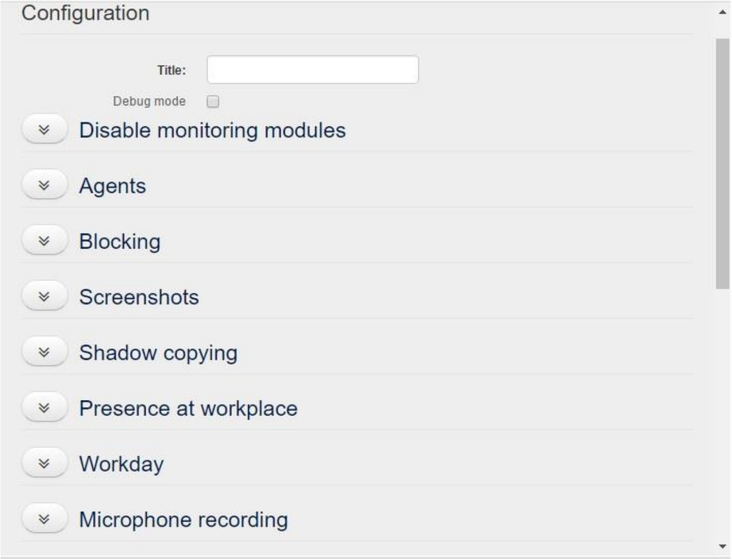
Configuration enables admin to enable/disable different monitoring modules, the Agent configuring, and adding various interception and blocking rules resulting in fine-tuning of the Agents to accomplish different tasks efficiently.

You can make uniquely configure any monitored Agent.

By default all initially deployed Agents are assigned **Default config** configuration.

Click corresponding name of configuration to edit it.

Editing configuration


Configuration

Title:

Debug mode □

Figure 55. StaffCop Enterprise Configuration screen, part 1.

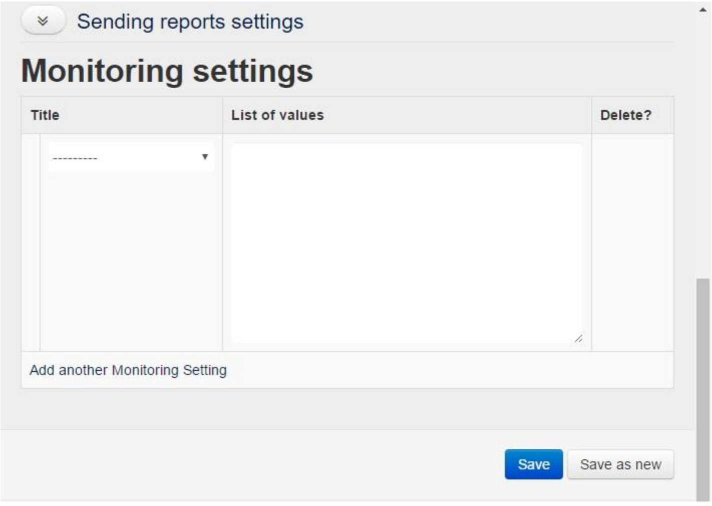


Figure 55. StaffCop Enterprise Configuration screen, part 2.

1. **Name**: specify name of new configuration or name of existing configuration will be displayed here;

2. **Debug mode**: when this mode is enabled, the Agent creates detailed debugging log, required for determining reasons for issues occurring during the Agent work. If you see that in your opinion the Agent works incorrectly, enable this mode and send the log it generates to support@staffcop.com together with the description of occurred issue. The logs are contained in the following folders:

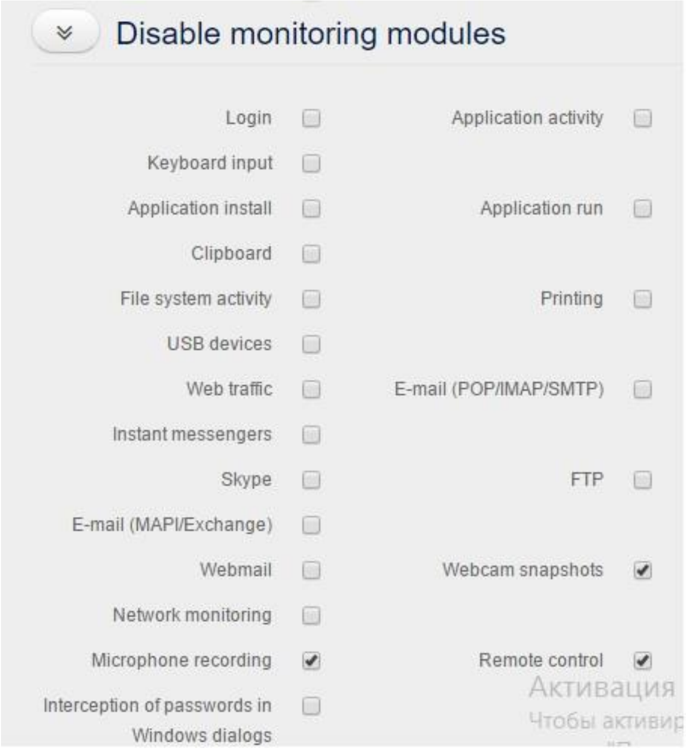
   c:\windows\system32\timecontrolsvc\Debug_Agent.log (for OS Windows 32-bit)

   c:\windows\sysWOW64\timecontrolsvc\Debug_Agent.log (for OS Windows 64-bit)

3. **Agents**: form for assigning current configuration to users. Select users from **Available Agents** list who should apply current configuration.

Disable monitoring modules

Disabling unused monitoring modules lowers workstation workload and do not overload database with excessive/irrelevant information:



Disable monitoring modules

Login	□	Application activity	□
Keyboard input	□		
Application install	□	Application run	□
Clipboard	□		
File system activity	□	Printing	□
USB devices	□		
Web traffic	□	E-mail (POP/IMAP/SMTP)	□
Instant messengers	□		
Skype	□	FTP	□
E-mail (MAPI/Exchange)	□		
Webmail	□	Webcam snapshots	☑
Network monitoring	□		
Microphone recording	☑	Remote control	☑
Interception of passwords in Windows dialogs	□		

Figure 56. Disable monitoring modules.

1. **Login:** monitors users accessing/exiting MS Windows;

2. **Keyboard input:** intercepts key strokes made on monitored workstation keyboard;

3. **Application install**: monitors installation/uninstallation of applications;

4. **Clipboard** module intercepts MS Windows clipboard;

   Please note that in rare cases, this module might conflict with MS Office applications (often with MS Excel).

   If delays occur in workstations productivity and while monitored employees work in MS Excel (or with other MS Office applications) try to disable this module;

5. **File system activity:** monitors all file activity on workstation. Please note if this module is configured incorrectly delays might occur in workstations operations.

   If you do not have a task to monitor file activity on user workstation, disable this module to lower workload.

6. **USB devices:** monitors all connections/disconnections of USB devices, file activities, and shadow copies all files copied from monitored workstations to USB data storages. If you do not require USB monitoring, disable this module:

File activity module and **Shadow copying** function should be enabled for this module to fully function;

7. **Web traffic:** intercepts HTTP/HTTPS traffic. The Agent intercepts and logs all network activity of applications, including data transferred via encrypted channels (SSL/TLS). This module is required for interception of web page visits history and for generating reports on work time tracking;

8. **Instant messengers**: intercepts messages and files sent/received via instant messengers;

9. **Skype**: intercepts messages and files sent/received via Skype;

10. **E-mail (MAPI/Exchange):** intercepts e-mail exchange with MS Exchange mail server.

    Due to connection with special mechanism of module's functionality, MS Outlook might display error message about failure to establish connection with Exchange server once in a several minutes and while this error message is displayed MS Outlook interface works with delays. The reason for this error message is that while it is displayed, the Agent connects with the server to download all necessary information. If you do not require such monitoring, you should disable this module to avoid such effects;

11. **Webmail:** intercepts incoming/outgoing web mail in main web browsers (Google Chrome, Mozilla Firefox, Yandex Browser, 360 Browser, Internet Explorer, Opera, and etc.) and all main public e-mail services (Gmail, Yandex, Mail.ru, Rambler.ru, Outlook.com, and etc.) Intercepts all outgoing mail including attachments;

12. **Network monitoring:** intercepts events occurring via IP and ports connection;

13. **Microphone recording:** enables to record all audio around monitored workstation's microphone. You can record Skype calls, and etc. as well as external sounds within a room where monitored workstation is located. You just have to find event related to microphone recording and download recorded audio file;

14. **Interception of passwords in Windows dialogues**: password interception in OS Windows dialog windows.

15. **Application activity**: determines the total time applications on monitored workstation are running, application user time spent working in applications, and user idle time in applications. This module is useful when work time tracking reports, time sheets and etc. are generated;

16. **Application run:** monitors applications launch;

17. **Printing** : interception of documents sent to print is released in two ways:
    - Intercepting print tasks sent to print (spooler);
    - Shadow copying of original (printed) document;

    In combination, these two methods enable to intercept documents sent to print more efficiently. Enable **File system activity** module and **Shadow copying** function should be enabled for this module to fully function;

18. **E-mail (POP/IMAP/SMTP):** intercepts e-mail messages transferred via e-mail clients (Outlook, Thunderbird, The Bat) using POP, IMAP, and SMTP protocols;

19. **FTP**: monitors FTP connections with employee workstations;

20. **Webcam snapshots**: enables administrator to switch on webcam on monitored workstation and make snapshots of surroundings. It helps to identify workstation user by his or her photo, as well as to identify office surroundings;

21. **Remote control:** viewing monitored employee desktop from remote location. We are planning to implement complete remote control over monitored workstations in the future versions of StaffCop Enterprise.

Agents

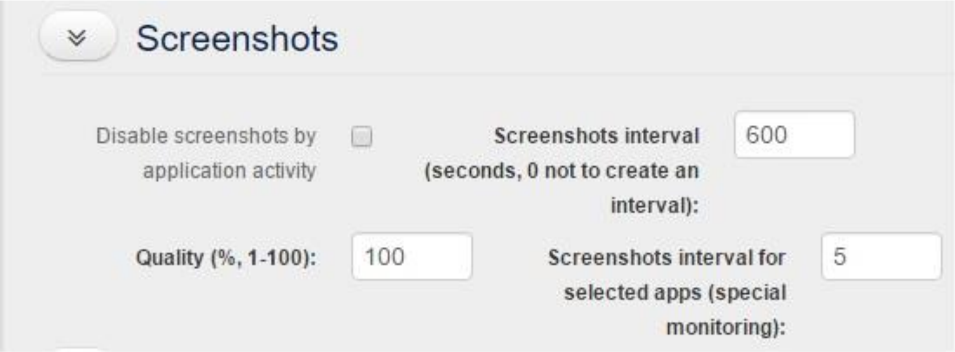
Option to apply configuration to selected agents and/or groups of agents.

Blocking

USB devices: blocks all USB data storages connected to monitored workstation. When the module is enabled employees cannot copy anything to and from USB data storages on their workstations.

Screenshots

The Agent can capture screenshots from workstation monitor and web camera according to the following parameters:


Screenshots

Disable screenshots by application activity ☐

Screenshots interval (seconds, 0 not to create an interval): 600

Quality (%, 1-100): 100

Screenshots interval for selected apps (special monitoring): 5

Figure 57. Screenshots settings.

1. **Disable screenshots capture by application activity**. Check this item if you **DO NOT** require screenshots capture every time when employee switches active window (for example, using Alt-Tab combination);

2. **Quality (%, 1-100)**: specify quality of captured screenshots in percentage ratio depending on monitor resolution of StaffCop Enterprise user.

3. **Screenshot interval (seconds, 0 – not to create an interval)**: specify interval between screenshots capture in seconds. To disable the module, set it to 0.

Modes:

- **By application activity**: screenshots are captured each time active window is switched.

  Note: In this mode, screenshots are captured with unpredictable intervals, so you might have trouble in calculating disk space required for their storage!

- **With specified interval**: screenshots are captured with specified interval only during activities of employee on monitored workstation. If employee is not active on workstation, the screenshots are not captured.

  Both these modes can be enabled simultaneously. The screenshots will be captured in both cases.

  Note: In this mode, screenshots are captured with unpredictable intervals, so you might have trouble in calculating disk space required for their storage!

- **Screenshots interval for selected apps (special monitoring)**: specify interval between screenshots capture for applications that were specified in **Monitoring settings: Applications – Special monitoring** in the current configuration;

Shadow copying

The Agent's file drive can intercept and create shadow copies of files sent outside of monitored workstation:

- Sent via e-mail (including files sent via web mail);
- Sent to Flash data storage devices;
- Downloaded from Internet via Internet browsers (to file exchange services, cloud services, etc.);
- Sent via Internet messengers such as QIP, Skype, ICQ, Mail.ru Agent, and etc.;
- Sent to print;

4. **Disable shadow copying**: check this item to disable shadow copying option.

5. **Max. size of file**: intercepted file will be shadow copied only if its size is less than the size specified in this item. This item enables to protect the system from overloading in cases when there is a mass transfer of large files to Flash storage devices.

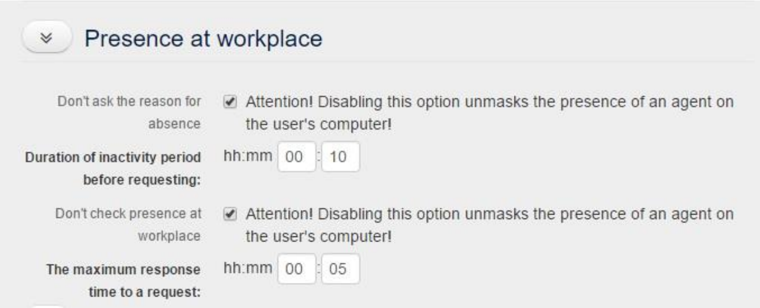
   Three conditions, described below, should be fulfilled in order to enable creation of shadow copies:

   - **Shadow copying** setting should be enabled (it is not related to interception of files from e-mail clients and browsers);
   - Maximum file size should not be greater specified value;
   - File monitoring rules should be applied to the file;

   Shadow copying settings are very flexible and described in detail further in this document, in **Monitoring settings** section.

Presence at workplace

Current functional was implemented for checking employee presence at his or her workplace.



Presence at workplace

Don't ask the reason for absence ☑ Attention! Disabling this option unmasks the presence of an agent on the user's computer!

Duration of inactivity period before requesting: hh:mm 00 : 10

Don't check presence at workplace ☑ Attention! Disabling this option unmasks the presence of an agent on the user's computer!

The maximum response time to a request: hh:mm 00 : 05

Figure 58. Presence at workplace.

1. **Don't ask the reason for absence**: If you do not wish to request the reason for absence from your employees uncheck this item;

2. **Duration of inactivity period before requesting:** specify time interval before StaffCop Agent sends request to StaffCop server;

   Specify interval in minutes in **Duration of inactivity period before request** field. If there is no user activity during specified time interval on employee workstation, the following window pops up on employee desktop:

   "No activity is detected on workstation from HH-MM. Please state the reason for your absence", where HH-MM is the time of last user activity detected by the Agent.

   In this window employee can explain the reason for his or her absence at workplace. When employee clicks **OK**, this event is transferred to the server, where it can be seen in **Event type: User activity**. If employee won't write anything in this window, but will click **OK** anyway or close this window, this event will be transferred to the server nonetheless and it will inform admin how long was employee idle time at workstation.

   Keystrokes and mouse movements he or she makes on workstation register employee activity at workstation.

3. **Don't check presence at work place**: Uncheck this item to enable it;

4. **The maximum response time to a request**: specify interval in minutes.

   Similar to the previous functional, when there is no employee activity detected during time interval specified in "**Duration of inactivity period before requesting**", a window containing simple mathematical task pops-up on employee desktop for employee to solve it. When employee enters correct answer, the window closes, and event of "**YES**" type is send to the server. In case of incorrect answer, the window closes and event of "**ERROR**" type is send to the server.

If employee did not specify any answer in the window, at the end of the time interval, specified in **The maximum response time to a request** field, the window will disappear and event of “**NO**” type is send to the server. Later this data can be used for analysis of employee efficiency at workplace.

Workday

In *Workday* settings specify beginning and end of employee workday. This data is used during generation of work time tracking reports to calculate employee lateness and overtime, active and work time.

1. **Workday start**: specify beginning of a workday;

2. **Workday end**: specify end of a workday.

3. **Delay of inactive time counting, sec.:** enables to specify time interval of user inactive time, after this time interval, employee must show activity at his or her computer (workstation). For example, it can be a time interval when employee should read one page of text on the screen of monitored computer**.**

Microphone *recording*

Configuring audio recording via microphone of monitored employee.

Audio clip recording interval (sec.): length of recorded audio files.

Cutoff interval – (stops microphone record if silent period is longer than cutoff interval): the time period after which audio recording should stop if monitored employee stopped using his or her microphone.

Noise gate level (disable microphone record if noise volume is lower than specified, -100..100): configuring noise threshold to trigger microphone recording. For example, sounds of environment.

Microphone record level (%, 0 - standard): influences audio recording volume.

Quality: when set as <0 – the size is smaller, when >0 – the quality is better.

Sending reports settings

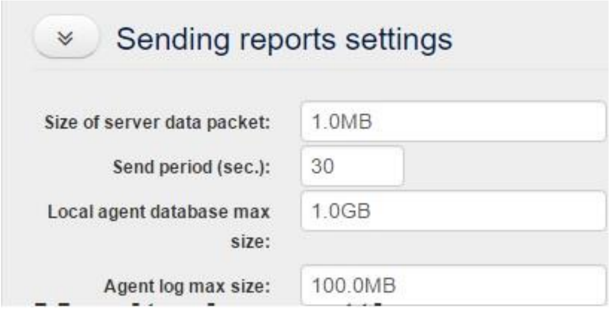
Configuring StaffCop Enterprise Agents reports send out to StaffCop server:

StaffCop Agent sends out data in small encrypted packages, distributed in time, to StaffCop server allowing to avoid network overload. You can specify the maximum size of data packetand time interval between sending packages, thus regulating your network and StaffCop server load.

When StaffCop Enterprise works correctly, the Agents aggregate data on events, send it to the server, and when they receive response from the server that the data was received, cleanup local database. So, employee is not capable of replacing, deleting, or editing the data intercepted at his or her workstation due to the fact that all data is stored on StaffCop server.

In some cases, when server connection is unavailable for some reason, the Agents start aggregating data in local database on the system disk of their workstations. For these cases, you can specify maximum size of local database in **Local agent database max size** field. When this maximum size is reached, the Agent starts to overwrite new aggregated data over the oldest one, thus maintaining relevance of aggregated data.

When “debugging mode” is enabled, the Agent creates service log and sends it to the server each time monitored workstation/StaffCop Agent is restarted or when the Agent receives new data. You can limit the size of this log by specifying maximum size in **Agent log max size**.



Sending reports settings

Size of server data packet: 1.0MB

Send period (sec.): 30

Local agent database max size: 1.0GB

Agent log max size: 100.0MB

Figure 59. Sending reports settings.

4. **Size of server data packet**: specify maximum size of data packet send from the Agent to the server;

5. **Send period (sec.)**: specify time interval between data packets sending from the Agent to the server;

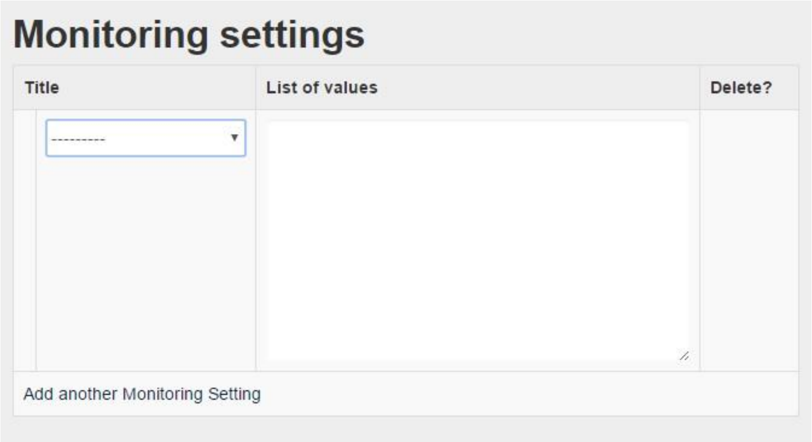
6. **Local agent database max size**: specify maximum size of local database on employee workstation that contains data aggregated by StaffCop Agent but not sent to StaffCop server due to issues with server connection.

   Attention! Maximum size of local database containing data aggregated by the Agent should not exceed 9 Gb!

7. **Agent log max size**: specify maximum size of StaffCop Agent log.

Monitoring settings

Monitoring settings enable admin to specify monitoring and lock-up settings very flexibly using white/blacklists.



Monitoring settings

Title	List of values	Delete?

Add another Monitoring Setting

Figure 60. Monitoring settings.

1. **Title**: rule’s title, specified automatically after settings are saved. There are two main types of monitoring: **File monitoring** and **Network monitoring**;

2. In **List of values** field each value should be listed and specified separately;

   Attention! Do not apply whitelist and blacklist of one type of settings simultaneously, this can lead to incorrect work of your StaffCop Agents!

   Specify values to which, depending on **Title**, monitoring rule will be applied. The list supports “*” mask, divider – hardline break.

3. **Delete?**: if you selected this item, current setting will be deleted.

Monitoring rules

Example

Title: "File monitoring - Paths and masks - Allow";

Condition: "File monitoring - Paths and masks - Prohibit";

List of values: Masks of monitored files;

Current rule enables to monitor only specific files and folders specified in **List of values**.

- **File monitoring - Applications - Enable/ File monitoring - Applications - Disable**: list of applications which file activity should be or should not be intercepted;

  Examples:

1. *File monitoring - Applications - Enable: explorer.exe:* file activity of just explorer.exe is intercepted;

2. *File monitoring - Applications - Disable*: chrome.exe: file activity of all applications except chrome.exe is intercepted;

   Note: this setting does not affect interception of files send via e-mail or downloaded to any Internet resource because separate module is used for intercepting web traffic.

- **File monitoring - Paths and masks - Enable/ File monitoring - Paths and masks - Disable**: one of the main settings of file monitoring. It very much affects performance of monitored workstation. There are two ways to configure this rule:

  - **To whitelist**: **File monitoring - Paths and masks - Enable**: In **List of values** specify list of folders, in which file activity should be monitored. You can specify different masks (for example, by file extension) in **List of values**. When file name will coincide with current mask, file activity with this file will be intercepted, otherwise this won't happen.

    Example:

    *.doc
    *.xls

  - **To blacklist: File monitoring - Paths and masks - Disable**: in list of values list folders in which file activity should not be monitored.

    In list of values specify masks of files that do not require their file activity to be monitored

    Example:

    *.doc
    *.xls

- **Network monitoring - Applications – Enable** / **Network monitoring - Applications - Disable**: When you add application to whitelist or blacklist, StaffCop Agent either will or will not intercept network traffic. Some applications might conflict with network module of StaffCop Agent. In this case, you should add such application to blacklist of applications in **Network monitoring**. In order to intercept traffic of nonstandard applications (some rare messengers, and etc.) you should add this application to whitelist of applications in **Network monitoring**.

Example:
mAgent
1C

- **Network monitoring - IP - Enable/ Network monitoring - IP - Disable**: Whitelists/blacklists of monitored IP addresses. StaffCop Agent replaces root certificate in browsers and other web applications to intercept encrypted traffic. But many resources for which you have to choose user certificate (state procurement web sites, tender platforms, bank-client services, tax services web sites, etc.) react very painfully to certificate replacements and do not work when StaffCop Agent operates (no selection window with list of user certificates is displayed).

  There is a following solution for such cases:

  Network monitoring – IP – Disable: XXX.XXX.XXX.XXX

  YYY.YYY.YYY.YYY

  (where XXX.XXX.XXX.XXX и YYY.YYY.YYY.YYY) pool of IP addresses used by the web resource).

  In this case, web traffic at this IP address will be allowed to go past network component of StaffCop Agent without influencing its processes.

In general case, when you suspect that the Agent disrupts operations of any web service that uses some IP address, add this IP to backlist.

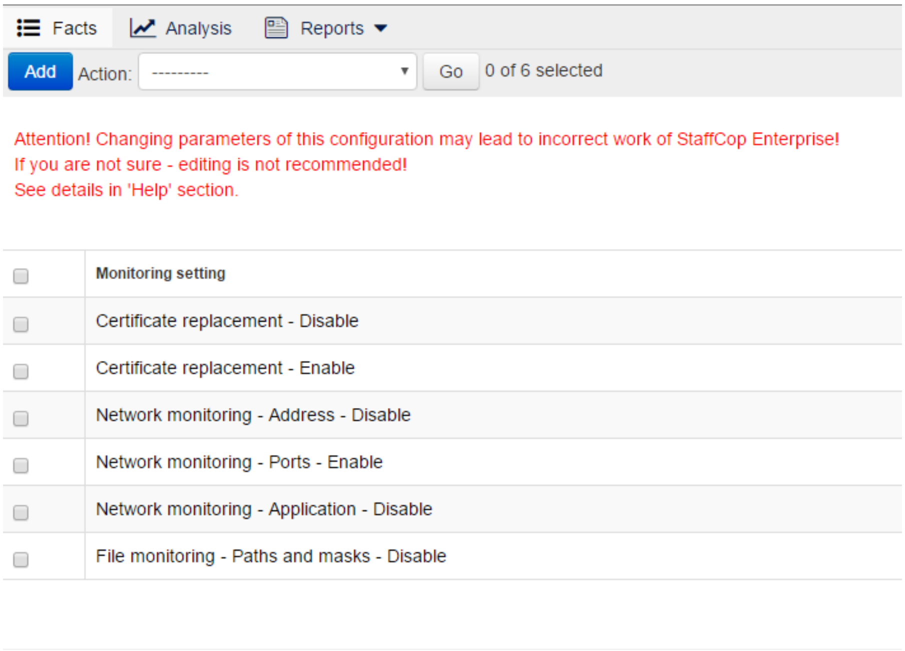
One configuration may contain unlimited number of rules. You can add new rules by clicking **Add another Monitoring Setting**.

1. **Add another Monitoring Setting**: adds another monitoring setting;

2. **Save**: saves current changes in configuration;
3. **Save as new**: enables to save it as new configuration.

Global configuration of StaffCop Enterprise

Global configuration enables admin to fine-tune monitoring modules for all admins independently from configuration assigned to them. You can add new configuration rules. It is not recommended to delete configuration rules, StaffCop Agents might stop responding. **Global configuration** settings are summarized with monitoring rules of the Agent configuration.



Attention! Changing parameters of this configuration may lead to incorrect work of StaffCop Enterprise!
If you are not sure - editing is not recommended!
See details in 'Help' section.

□	Monitoring setting
□	Certificate replacement - Disable
□	Certificate replacement - Enable
□	Network monitoring - Address - Disable
□	Network monitoring - Ports - Enable
□	Network monitoring - Application - Disable
□	File monitoring - Paths and masks - Disable

Figure 61. Global configuration.

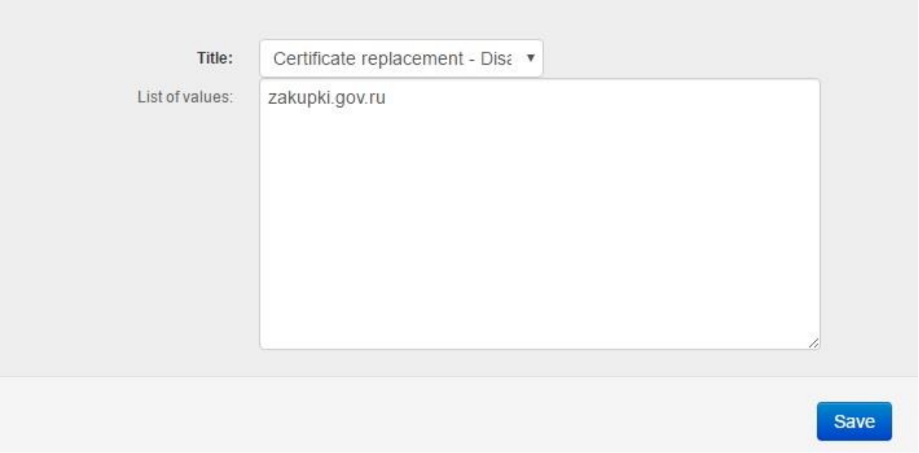
Click corresponding name of global configuration parameter to edit this configuration.

Editing global configurations

Editing global configurations form is similar to **Monitoring settings.** You can add new types of rules and their values there.

Title: enables admin to select a type of applied global configuration rule;

List of values: enter values for selected configuration. To select several values, specify them in a list, one under another, without specifying separator characters. Click **Save** to save monitoring rules of **Global configuration**.



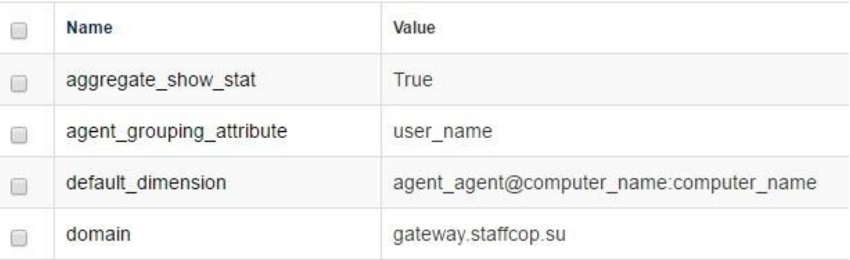
Title: Certificate replacement - Disa

List of values: zakupki.gov.ru

Figure 65. Configuring global configuration.

StaffCop Enterprise Server preferences

List of server preferences enables to edit the following values of fixed set of StaffCop Enterprise preferences:



☐	Name	Value
☐	aggregate_show_stat	True
☐	agent_grouping_attribute	user_name
☐	default_dimension	agent_agent@computer_name:computer_name
☐	domain	gateway.staffcop.su

Figure 66.Server preferences.

- **aggregate_show_stat**: False or True; to display/hide aggregator bar;
- **agent_grouping_attribute**: user_domain, comment, post, office, company, user_name; specify attribute that will be used for agents grouping.
- **default_dimension**: change default settings. Value parameter has value **Computers** which can be changed to **Accounts** or **Users** , then **the Constructor** will open automatically on users, and users will be displayed in **Work time tracking** report (note: it is convenient to create the report when StaffCop Agent works on terminal server);
- **domain**: name of domain where admin part web interface will be accessible. When you change StaffCop Enterprise server IP or domain address this value should be changed accordingly.

Mail server settings

Select required configuration from drop-down list and it will be applied to StaffCop Agent.

Server restart

Server restart is used for forced restart of the services. If web interface of StaffCop Enterprise stops responding or responds with delay, try to restart StaffCop Enterprise server to resolve this issue. Also you can force the launch recount of all events, operating same way as “staffcop sessions_reset” command, according to the new settings.

License Information

License Information: contains information about your license life span and information about quantity of StaffCop Agents.

Download agent installer

Download agent installer: link to download StaffCop Agent from specified server IP address.

Navigation panel

You can hide and show Navigation panel by clicking cross sign:

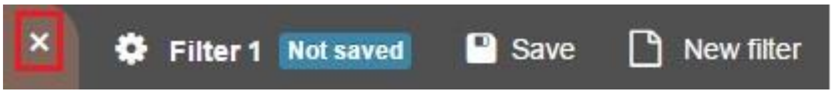


Figure 67. Closing Navigation panel button.

Please note that some reports look better when navigation panel is closed. To show the panel, click the same button again.

Widget for selecting date and time interval

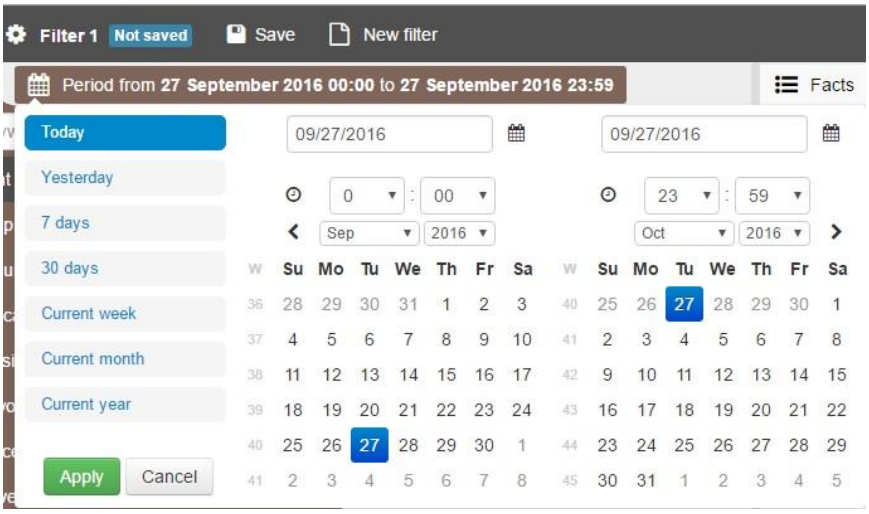


Figure 68. Widget for selecting date and time interval

When you click it, the form for selecting required time interval is opened. You can choose standard time interval (day, week, month, etc.) in the left side. To select any period click start date of this period in calendar, and then click end date of the period. When time interval is selected, click **Apply**.

Search by events form

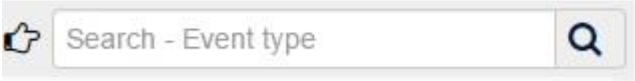


Figure 69. Search – Event type.

Enter key word or regular expression, and press **Enter**. The system will display all related events by type. Use quotations to search exact matches (expressions).

Sidebar for selecting required filter

It has two main modes: **Filters** and **Constructor**

Filters: enables you to view and edit Filters and Policies divided into three groups:

1. **Efficiency**: here you can find reports for work time tracking reports and analysis of employee efficiency;
2. **Security**: here you can find reports about security, threats, actors and incidents;
3. **Policies**: here you can find various Policies on security, productivity, intercept, and etc.

> NOTE: **Policy** section used for **CONFIGURING** the system and not for viewing events. In the interface, **Policies** displayed as wrench icon. Edit, create, and delete **Policies** only when you are sure in your actions. In case of incorrect configuring of **Policies** the system might work incorrectly or will become less responsive. Detailed information about configuring and editing of **Policies** can be found in **Admin menu/ Filters and Policies** section of the current guide.

Constructor: enables admin to search and analyze data, and to create new Filters. To create new Filter you have to overlap different limiting filters in sequence. Each overlapping of next filter in real-time mode cuts out “irrelevant” data enabling to find necessary data in 2-3 clicks.

Aggregator bar

In this form events are aggregated (grouped) by different dimensions and attributes. It makes it significantly easier to navigate by events and to create new filters.

Button for switching on events counter in aggregator bar

Quantity of events aggregated in the aggregator bar is automatically calculated and displayed to the right from corresponding record.

When events quantity is big, their calculation might take considerable time. To increase response time you can switch off forced count of aggregated events, and switch it back on after specifying filter conditions.

When aggregated events counter is switched off, the aggregate bar displays all events occurred at all times.

After you specify filter conditions and switch on aggregated event counter, all “irrelevant” data, outside of set time interval and other filter conditions disappear.

Data Visualization panel

This panel displays data in visual and convenient view for admins. Various graphic modules for visualizing events, statistics, interconnections, and graphic reports are divided into categories.

In the upper part of the panel is selection of main sections. In the lower part – selection of subsections (modes).

1. **Events**: current section contains widgets for visualizing events in different views:
    - **Table**: Events are displayed in convenient table view. The table changes dynamically according to the types of events selected for viewing. Preview area is located in the lower part of the table. For example, when viewing e-mailing events (**E-mail** type of event), contents of an e-mail selected in the table, and two additional columns “Sender”, “Recipient” will be added to the table;

    - **List**: events are displayed as a list. When you click on an event, event details will be displayed;

    - **Thumbnails**: screenshots will be displayed as thumbnails;
    - **Activity**: heat diagram, it enables to visualize registered event by time and date via calendar.

For user convenience, the grid is divided into following:

a) squares with gradation in days and hours (when selected time period is longer than 24 hours);

b) squares with gradation in hours and minutes (when selected time period is 24 hours or less);

Empty (white) cells mean that no events were registered during selected time period (hours). Colored cells mean there were registered events during selected time period. Color intensity indicates quantity of events. The more intensive is a color, the more events were registered in this time interval. When you hove cursor over such cell, a window pops-up containing information about date, time and number of events in this time period.

When you click any cell, detailed table view of events occurred in this time (hour or minute) is opened;

2. **Analysis**: current section contains widgets to view and analyze statistics:

    - **Table**: to display statistics info in table view. You can add unlimited number of columns (dimensions). There is an option to convert this table into Excel document;

    - **Linear graph**: X-axis is a time scale. Select time interval in the upper part of the window (by days/hours/minutes). Y-axis is a number of events according to selected filter. It helps to determine statistics anomalies by specified events and evaluate employee efficiency;

    - **Pie chart**: classic pie chart. Select dimension for analysis. If specified dimension allows it, select corresponding measurement. For example, active time for applications or duration in minutes for voice conversations;

    - **Graph:** constructs visual graphs of employee interconnections according to selected dimensions. Using this graph you can easily determine touch points and interconnections of specific employees. Also it provides visual representation of data distribution and existing information channels.

3. **Reports**: current section contains work time tracking and efficiency reports, timesheets, statistics represented as interactive table:

    - Time tracking;
    - Summary report;

- Lateness report;
- Summary statistics;
- Statistics by day;
- Work timesheet;
- Activity timesheet;
- Absence timesheet;
- Printer usage timesheet;
- Facts feed.

Lower panel

Lower panel: contains button of forced refresh of selected report (with repeated request to database). This button is used for updating operational information via web interface.

Search

Search: field to co conduct search by content.

Administrating StaffCop Enterprise Server

Disk auto cleanup

In most cases, preventing issue from occurring is much simpler than resolving it. In order to prevent disk overload evaluate the future volume of aggregated data you will have to store and configure disk auto cleanup accordingly.

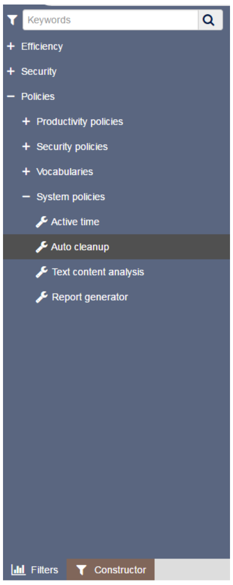
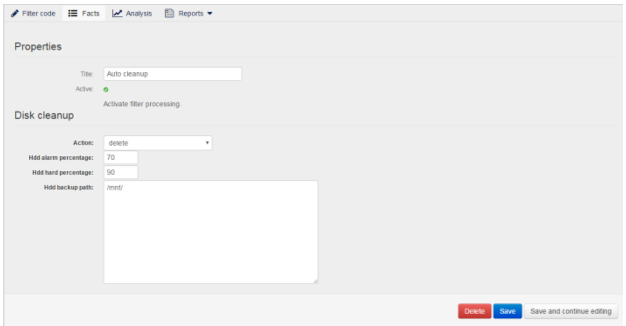


Figure 70. Disk auto cleanup.

In order to configure auto cleanup, got to **Filters** tab, open tree of reports called **Policies**, open **System polices**, open **Properties** window of **Auto cleanup** police.



Properties

Title: Auto cleanup

Active: ●

Activate filter processing.

Disk cleanup

Action: delete

Hdd alarm percentage: 70

Hdd hard percentage: 90

Hdd backup path: /mnt/

Figure 71. Properties window of Auto cleanup policy.

Auto cleanup settings:

1. Action: select action to be initiated when threshold of hard disk space is reached. Specify this threshold in **Hdd hard percentage**. The following actions are available:

   - **Nothing**: do nothing;

   - **Delete**: delete old data when disk space threshold is reached;

   - **Move**: move data to backup file. Specify file path to this backup file in **Hdd backup path**.

2. **Hdd alarm percentage**: specify disk space threshold (in percents), when it is reached, you will be alerted;

3. **Hdd hard percentage**: specify disk space threshold (in percents), when it is reached, actions specified in **Actions** will be executed;

4. **Hdd backup path**: specify paths to data storage when data is moved. Any report can be created for auto cleanup. To do this, specify **Backup** value for **Type** parameter.

Database backup

In order to back up your database, complete the following steps:

1. **Preparations:**

Make sure that

- there is enough free space on your hard disk:

```
df -h
```

- there is installed operational version of postgresql, and that it is launched;

```
 sudo service postgresql status
```

2. **Initiating backup:**

Execute the following command:

```
 sudo staffcop info
```

If your version of StaffCop Enterprise is higher than 3.1.233, execute the following command:

```
sudo staffcop backup_db
```

Your backup will be stored in the following folder: **/var/lib/staffcop/staffcop_backup**

To move this folder to another computer, copy this folder via network, or use mobile data storage to move it.

In case you are using StaffCop v. 2.x or earlier than 3.1.233 – execute the following command:

```
 wget -P /tmp/ -N http://dist.staffcop.ru/utils/script/backup/bp_install.sh
&& sudo bash /tmp/bp_install.sh
```

It will download and install required components. After the command will be successfully executed, repeat the following command:

```
 sudo staffcop backup_db
```

3. **Restoring backup**:

To restore backup execute the following command:

```
 sudo staffcop restore_db
```

In case your backup file is located in folder other than /var/lib/staffcop/staffcop_backup , you should indicate full file path to it, for example:

```
 sudo staffcop restore_db /home/support/backup
```

Scripts source codes

Installer script:

bp_install.sh

```
#!/bin/bash -e
cd ~
wget -O ~/backup_db
http://dist.staffcop.ru/utils/script/backup/backup_db
cp ~/backup_db /usr/share/staffcop/bin/
chmod +x /usr/share/staffcop/bin/backup_db

wget -O ~/restore_db
http://dist.staffcop.ru/utils/script/backup/restore_db \
cp ~/restore_db /usr/share/staffcop/bin/restore_db \
chmod +x /usr/share/staffcop/bin/restore_db
```

Creating backup script:

backup_db.sh

```
#!/bin/bash -e
echo "Backup StaffCop"

if ! [ -f /bin/tar ]; then
echo "No app tar. Please install 'sudo apt-get install tar'"
exit 3
fi

if ! [ -f /usr/bin/pg_dump ]; then
echo "No app pg_dump. Exit"
exit 3
fi
#---------------------------
bname=${DBNAME}-db.dump
sname=${DBNAME}-setting.tar
cname=${DBNAME}-sert.tar
def_folder="staffcop_backup"
def_patch="/var/lib/staffcop"
#--------------------------

if [ $1 ] ;  then
patch=$1
else
patch=${def_patch}
fi

if ! [ -f /usr/bin/realpath ]; then
echo "Warning. No app realpatch. Please install 'sudo apt-get install
realpath'
else
patch=$(realpath $patch)
fi

patch=${patch}/${def_folder} \
echo "Backup patch $patch"

#Create backup patch \
echo "Create backup patch" \
mkdir -p $patch \
chmod 777 -R $patch

if ! [ -d  "$patch" ] ; then \
echo "directory does not exist. exit" \
exit 1 \
fi \
echo "Remove old backup files" \
rm $patch/* || true

#File name \
full_patch=${patch}/${bname} \
sfull_patch=${patch}/${sname} \
cfull_patch=${patch}/${cname}

echo "Backup patch $full_patch" \
echo "Setting patch $sfull_patch" \
echo "CA patch $cfull_patch" \
echo "------------------------------------------" \
echo "Backup config" \
tar --absolute-names --create --verbose --file $sfull_patch
/etc/staffcop

echo "Backup CA" \
tar --absolute-names --create --verbose --file $cfull_patch
/var/lib/staffcop/CA

echo "Backup DB" \
sudo -u postgres pg_dump --host=$DBHOST_OPTION --port=$DBPORT_OPTION  -
-verbose
--compress=7 --clean --create --blobs --format=c --file=$full_patch --
dbname=$DB
NAME

echo "------------------------------------------" \
echo "Backup patch"

if ! [ -f $full_patch ]; then \
echo 'No file db. Error' \
exit 1 \
else \
echo "File DB: $(du -h $full_patch)" \
fi

if ! [ -f $sfull_patch ]; then \
echo 'No file setting. Error' \
exit 1 \
else \
echo "File seting: $(du -h $sfull_patch)" \
fi

if ! [ -f $sfull_patch ]; then \
echo 'No file CA. Error' \
exit 1 \
else \
echo "File CA: $(du -h $sfull_patch)" \
fi
```

Restoring database script:

restore_db.sh

```
#!/bin/bash
#----------------------------
```

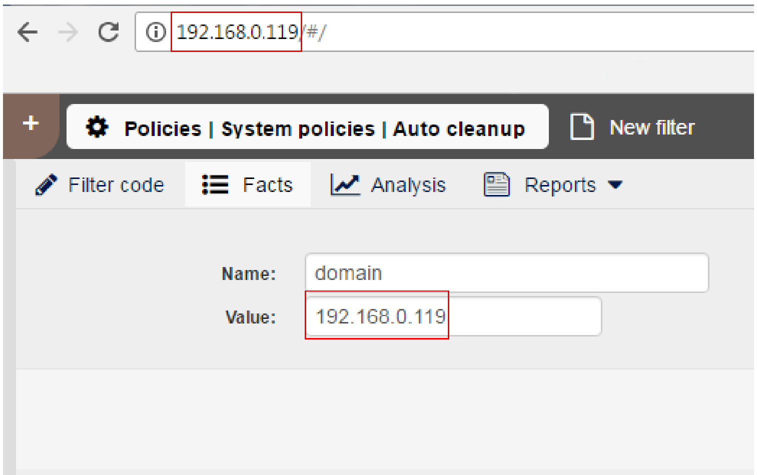
```
bname=${DBNAME}-db.dump
sname=${DBNAME}-setting.tar
cname=${DBNAME}-sert.tar
def_folder="staffcop_backup"
def_patch="/var/lib/staffcop/${def_folder}"
#--------------------------

if [ $1 ] ;  then
        patch=$1
else
        patch=${def_patch}
fi

if ! [ -f /usr/bin/realpath ] ; then
 echo "Warning. No app realpatch. Please install 'sudo apt-get install
realpath'"
else
 patch=$(realpath $patch)
fi

if ! [ -d  "$patch" ] ; then
        echo "directory does not exist. exit"
        exit 1
fi

echo "Restore patch $patch"

full_patch=${patch}/${bname}
cfull_patch=${patch}/${cname}

if ! [ -f $full_patch ]; then
        echo "No backup db"
else
        echo "Restore backup staffcop DB ${DBNAME}"
        echo "Stop service staffcop"
        service staffcop stop
        echo "Restart PG"
        service postgresql restart
        echo "Start restore ${DBNAME}"

        sudo -u postgres pg_restore  --host=$DBHOST_OPTION --
port=$DBPORT_OPTION  --verbose --clean --create  --format=c $full_patch
-d postgres
        echo "Analyse ${DBNAME}"
        echo "analyze;" | sudo -u postgres psql ${DBNAME}
        echo "Vacuum"
        echo "vacuum full analyze;" | sudo -u postgres psql ${DBNAME}
        echo "Reindex"
        echo "reindex database ${DBNAME};" | sudo -u postgres psql
${DBNAME}
        staffcop init
        echo "Sessions reset"
        staffcop sessions_reset full
        echo "Finish restore  ${DBNAME}"
        staffcop info
fi

echo "Certificate"
if ! [ -f $cfull_patch ]; then
        echo "No backup sert"
else
        service staffcop stop
        service nginx stop
        rm /var/lib/staffcop/CA/*
```

```
            tar --absolute-names --extract --verbose --file $cfull_patch
            chown -R staffcop:staffcop /var/lib/staffcop/CA/
            chmod 775 -R /var/lib/staffcop/CA/
            service staffcop start
            service nginx start
    fi
    service staffcop start
```

No screenshots

If you checked screenshots capture from monitored computers in the program settings but you see thumbnails instead of screenshots, check the following:

1. Whether IP or sever domain name in config corresponds with address string (admin-server preferences-domain);



192.168.0.119/#/

Name: domain

Value: 192.168.0.119

Figure 72. Comparing IPs.

2. In case when all server parameters are specified correctly, but instead of pictures you see white icons, check access rights to folder containing screenshots:

   ```
   sudo ls -lR /var/lib/staffcop/upload/filedta
   ```

   User should be a folder owner.

StaffCop Command line

A lot of operations related to administrating StaffCop has compact and concise system of commands executed in command line.

Change password for admin web interface user.

```
sudo staffcop passwd NEW_PASSWORD
```

Remove all files and events from database that are older than X days (where X = number of days)

```
sudo staffcop cleanup X
```

Upgrade to the latest stable version

```
sudo staffcop upgrade
```

Reset the system with known operable parameters

```
sudo staffcop init
```

Restart staffcop service

```
sudo service staffcop restart
```

Receive information about working version of StaffCop: size of database, size of aggregated file storage, etc.

```
sudo staffcop info
```

Remove information about specific workstation

```
sudo staffcop delete COMPUTER_NAME
```

StaffCop commands

staffcop sessions_reset

Resets all events and reports. For example, when one web site was productive, and you change its classification to become unproductive.

StaffCop Server main commands

sudo staffcop passwd NEW_PASSWORD: change password for admin user of web interface;

sudo staffcop upgrade: upgrade to the latest stable version;

sudo reboot: reboot server;

sudo staffcop delete COMPUTER_NAME: delete information about computer;

sudo staffcop init: resets system with known working parameters;

ifconfig: view information about network subsystem;

sudo service staffcop restart: restart staffcop service;

sudo service nginx restart: restart nginx (web server) service;

sudo dpkg -i package_name.deb: installation of downloaded packages;

sudo staffcop cleanup X: deletes all files and events older than X days (where X – number of days);

sudo apt-get update && sudo apt-get upgrade: refresh OS;

df –h: view used disk space;

sudo apt-get install tzdata: install tzdata to setup time zone;

sudo dpkg-reconfigure tzdata: select time zone;

date: view current time and time zone;

Remote copy

File transfer between/from/to remote server can be done as following:

```
 sudo scp -rpC -c blowfish source/. user@server:/folder
```

where -r - recursive copy (for folders), p – saving time of file creation, C – file compression (not actual during transfer of files compressed by archive program), c – fastest encryption protocol.

In case of special requirements for copying use help info using scp command.

```
man scp
```

Also, you can launch remote copy from the third server situated between two others.

In case of remote copy, you have to know the password of remote user or have his key (depending on authorization scheme) and this remote user should have rights to copy to destination folder.

If you are copying under root, then do the following:

After file transfer, do not forget to check whether target user (including system user) has a right to access to folders and right to copy. You can check this using the following command, for example:

```
ls -l /folder/subfolder
```

If required – change owner using the following command:

```
sudo chmod -R user:user /folder/subfolder
```

Or by using rsync:

```
sudo sshpasswd
```

System partition: copy

Sometimes it is necessary to recursive copy not just data, but operation system itself.

Copying operation system is required when you install some additional programs, have a lot of special settings, and etc. It can be done in several ways, the most simple one is copying whole partition.

For example, using command **dd**.

```
sudo dd if=/dev/sdXY bs=1M conv=noerror | gzip -c>
/folder/subfolder/partition.dd.gz
```

The resulting file is byte-by-byte copy of your partition that includes not just files but type of file system.

This shows that if the system and data, for example, StaffCop database and screenshots, are contained in one partition, then this method is **not** suitable for you.

Of course, like any copy, it should be stored on different device.

Changing IP server

Sometimes it is necessary to change IP address. The standard method for this: edit configuration file, and RESET service.

- Interface name eth1 (it can be different, use ifconfig);

- Sub-network mask;

- Your network;

- Broadband query;

- Default gateway

```
sudo nano /etc/network/interfaces
auto eth1
iface eth1 inet static
address 192.168.201.252
netmask 255.255.255.0
network 192.168.201.0
broadcast 192.168.201.255
gateway 192.168.201.254
```

After creating interface you should specify server DNS. To do this, in OS Linux usually used resolv.conf file.

Here we specified two DNS servers, on of them is deployed on this station, and another is at 192.168.201.254.

```
sudo nano /etc/resolv.conf
nameserver 127.0.0.1
nameserver 192.168.201.254
```

Reset interface to apply these changes.

```
sudo /etc/init.d/network restart
```

Mounting disks

We added this article in the current guide for those of you who, either by necessity or simple curiosity want to understand how command 'mount' works in more detail.

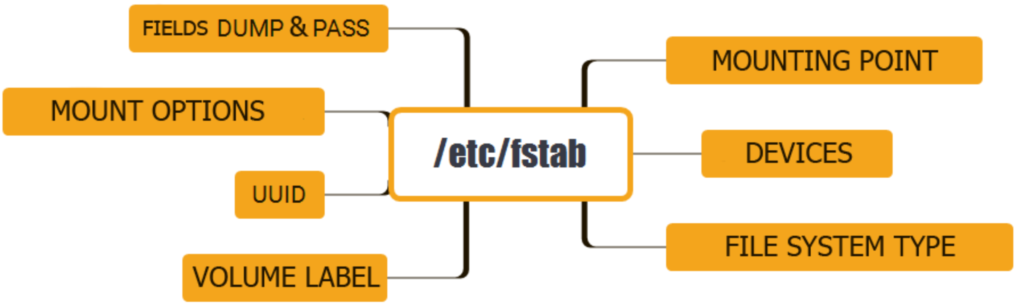


Figure 73.

filesystem	**dir**	**type**	**options**	**dump**	**pass**
Your device	Mounting point	Type of your file system	options	Should we create backup?	Should we run consistency check on the file system?
/dev/sda3	**/home**	**xfs**	**rw,auto**	**0**	**2**

The above table means that device /dev/sda3 will be mounted in folder /home, and it will be mounted automatically for reading and saving. –XSF file system, no backup will be created, and running consistency check on the file system during each disk mounting.

You can archive the same result when you manually enter the following line:

```
mount -t xfs /dev/sda3 /home
```

<note> So, fstab can be considered as automation of required mounting.</note> Additionally, you do not have to specify type of the file system, if it is not some

exotic file system.

Catalogues in Linux are represented as a tree, where its root is in /
To be connected each new data storage (hard disk, DVD disk, USB flash, or network resource) is mounted and its file structure is displayed in specific folder.
You can manually enter the following command to mount it:

```
mount
```

Or it can be mounted automatically. To do this specify required disk/device in **/etc/fstab** configuration file.

/etc/fstab consists of columns, divided by tabulation symbols (TAB button).
There are 6 fields in the file.
1. Device, at /dev/sda /dev/hda /dev/sr0 /dev/sdb1 and etc. Or by unique identifier - **UUID**.
UUID is generated by mkfs.* utilities during file system creation. blkid shows UUIDs of devices and HDD partitions:

In this case the field contains UUID=”550e8400-e29b-41d4-a716-446655440000”

2. Mounting point: is a folder, showing file system of device, which is being connected.

3. Type of file system: Most often, you will encounter **ext4 file system** since this is default file system for most Linux distributives, as well as **ntfs** and **vfat**, both file systems are developed by Microsoft.

4. Options: Includes additional options, such as: rw – read-write, ro – just read. More details are available here and here.

5. Dump is used by dump utility to determine whether data back copy should be created in a file system. Possible values: 0 or 1. If you specify “1”, dump will create backup copy. Most users do not have dump utility installed, so they should specify “0” in this field.

6. Check disk: Is used by fsck to determine if file system integrity should be checked. Possible values: 0,1 or 2. Value 1 is specified only for root file system (from / mounting point of view). Use value 2 for other file systems that you want to check. This value has less priority. Please note that in case of btrfs, you should always specify 0 even if this file system is used as root. Fsck will not check file systems containing 0 in this field.

System upgrade

Ubuntu developers regularly release upgrades of individual programs that improve security and fix small errors.

We recommend you to upgrade your system regularly. This is done by using two consequent commands, for convenience they are combin ed into one:

```
sudo apt-get update && sudo apt-get upgrade -y
```

To execute it, you should have user role with access to root privileges, and to know its password.

In case of importing from ova, this is *support* user.

Upgrade may take some time, proportional to the time interval since ova image was created, or since the last upgrade. In average in takes several minutes.
Also, upgrades require Internet access.

After upgrade is complete, you can execute the following commands:

```
sudo apt-get autoclean && sudo apt-get autoremove
```

These commands help you to delete unused packages, if they exist, and to cleanup package archive.

StaffCop upgrade

Upgrade whole system by executing the following command:

```
sudo apt-get update && sudo apt-get upgrade
```

StaffCop will be upgraded also.

To upgrade StaffCop execute the following command:

```
sudo staffcop upgrade
```

In order to execute it you should know user password and Internet connection.

Manual disk cleanup

No matter how large your hard disk is, it disk space is finite, and if you would not take any measure beforehand, sooner or later it will ran out of free space.

To prevent this situation from occurring, plan the necessary volume of your hard disk beforehand, taking into account quantity of monitored workstations, what type of data is aggregated from them, and duration of this data storage.

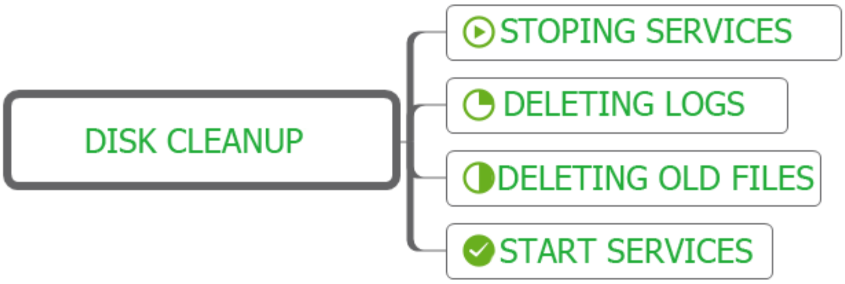


Figure 74. Disc cleanup structure.

You can specify auto cleanup settings in admin panel. If this was not done, or did not work for some reason, you can conduct disk cleanup manually:

1) Stop StaffCop by executing the following command:

```
sudo service staffcop stop
```

2) If there is enough free space on disk (**df –h** command to view it), it is enough to delete the following elements:

a) logs, by executing the following command:

```
sudo rm /var/log/*gz
```

b) old staffcop databases, by executing the following command:

```
sudo staffcop cleanup X
```

where X is time period (in days) during which backup data is aggregated.

In case hard disk is completely full, issues with data deletion might occur.

In this case, execute the following line, enabling you to delete above listed data:

```
sudo tune2fs -m 0 /dev/sdX
```

This command allows you to free up disk space, reserved for system needs.

After executing this command, execute previously mentioned manual hard disk cleanup.

Then you should return disk space, reserved for system needs, to superuser. To do this, execute the following command:

```
sudo tune2fs -m 5 /dev/sdX
```

If this command is not executed there is a possibility that due to incorrect settings whole hard disk space will be allocated including 5% of superuser space.

Make sure to return 5% of disk space as reserve. To leave 5% of hard disk space as reserved space is a standard practice.

After disk cleanup is completed, launch StaffCop using the following command:

```
sudo service staffcop start
```

Optimization

Postgresql optimization

Use this calculator to determine optimal settings for your configuration and load.

Program part optimization

If you are using virtual machine, we do not recommend you to use VirtualBox if you have more than 10 monitored computers. User server options of OS.

Disk subsystem optimization

We recommend to use **noatime** in **mounting** option:

```
/dev/sdX /point/mounting ext4 rw,noaitime 0 2
```

If you have more than 100 of StaffCop Agents, we recommend you to implement the following scheme:

1. OS is moved to separate disk;

2. Database is moved to separate disk, for example ssd;

3. File storage is moved to separate big disk.

Moving database to another hard disk

Hard disk/partition should exist in the system and be physically connected. In general, moving database to another hard disk looks like this:

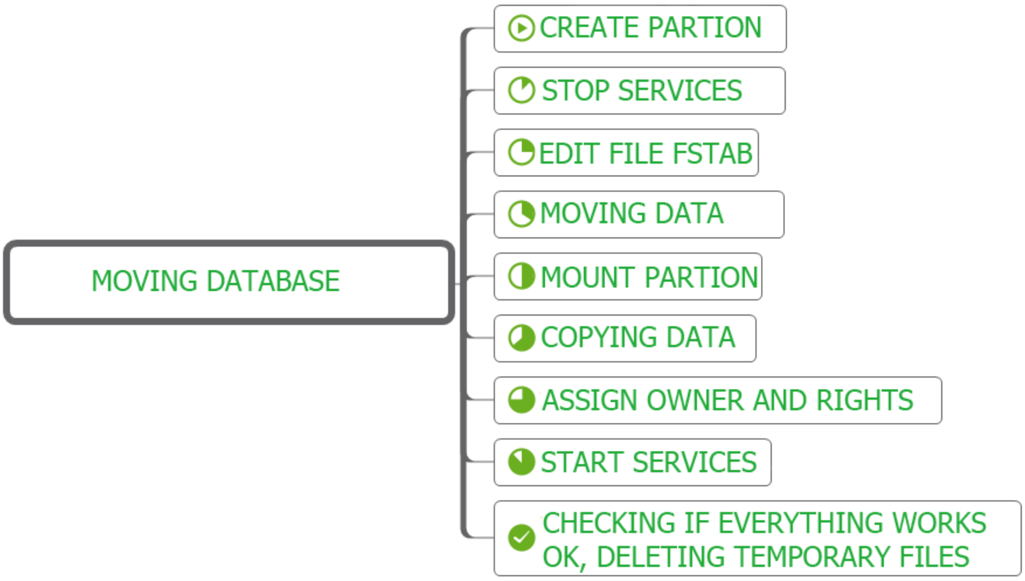


Figure 75. Moving database.

0. If hard disk contains required partitions, then go to item 1;

cfdisk works only with MBR partitions. If your hard disk is larger than 2 Tb, you should use GPT partitions.

If not, partition your disk, for example, like the following:

```
cfdisk /dev/sdX
```

and create file system on it, executing the following command:

```
sudo mkfs.ext4 /dev/sdX
```

where X is completion of disk name.

---

1. Stop postgresql and staffcop using corresponding commands:

```
sudo service postgresql stop
sudo service staffcop stop
```

---

2. Edit file /etc/fstab

```
sudo nano -w /etc/fstab

Specify the following line there:
/dev/sdX  /var/lib/postgresql/ ext4 rw,noatime 0 2
```

Where **/dev/sdX** is your hard disk, **/var/lib/postgresql/** is catalogue displaying hard disk contents, **ext4** is a type of file system (if you are using another file system -

jfs/xfs/reiser, and etc. this option changes.) **rw** means permission to read-write on disk.

Also, you can specify disk UUID. You can retrieve disk UUID by executing the following command:

```
 ls -l /dev/disk/by-uuid
```

In this case, first part of the line will look like this: **UUID=« «** in quotes insert the result of above mentioned command.

---

3. Create backup folder, and move data from database folder there:

```
mkdir /home/user/reserv && sudo mv /var/lib/postgresql/* /home/user/rezerv
```

where user is user’s home catalogue, replace it with the name of your home catalogue. You can find out user’s home catalogue name by executing similar type of command:

```
env | grep -E "home|HOME"
```

As a result, you will see user’s home catalogue name on behalf of which this command was executed.

4. Check if mounting is correctly done by executing the following command:

```
sudo mount -a
```

The disk is mounted by executing this command, the disk is specified in fstab, but its mounting is not over yet.

So if you specified some data incorrectly or made a mistake then you will see mounting errors, and will have a chance to correct your mistake.

Check if disk is mounted correctly by executing this type of command:

```
 df -h
```

Also, you can check if current partition is available for writing. For example, let’s create text file and check its availability by executing the following commands:

```
 touch /var/lib/postgresql/9.3/main/test_write.txt && ls -l
/var/lib/postgresql/9.3/main/
```

Of by simply executing **mount** command without specifying any parameters: as a result, all mounted systems will be displayed. Our new device should be rw mounted.

5. Copy all to hard disk:

```
cp -R  /home/user/reserv/* /var/lib/postgresql/
```

In case you moved data to another catalogue, make changes according to real location of files.

6. Change owner on postgres.

```
chown -R postgres:postgres /var/lib/postgresql/9.3/main
```

7. Assign him rights on 700.

```
chmod -R 700 /var/lib/postgresql/9.3/main
```

8. Launch staffcop and postgresql.

```
sudo service postgresql start
sudo service staffcop start
```

Execute command:

```
 sudo staffcop sql
```

in displayed invite, write **analyse;** and wait.

9. Access web interface and check if everything works ok, all reports are visible, and etc. If everything works ok, you can delete files created due to **mv**

```
 rm -R /home/user/folder_with_copies
```

As with any rm, it should be applied carefully.

Moving files and screenshots

StaffCop Enterprise separately stores metadata (DB) and intercepted files enabling to apply DB and files, stored on different hard disks, on large volume of data. For example, store DB on swift SSD storages, and files – on separate RAID or in network storage.

Below you can see instruction for sdb1 disk, your disk name may differ.

RAID and NAS are mounted similarly.

---

1. Stop staffcop service:

```
sudo service staffcop stop
```

2. Mount new disk on **/mnt:**

Note: **sdb1** is just an example. Replace it with original name of your disk.

```
sudo mount /dev/sdb1 /mnt
```

3. Move contents of **/var/lib/staffcop/upload/filedata** folder to new disk, specify its owner, group and rights:

```
 sudo mv /var/lib/staffcop/upload/filedata/* /mnt

sudo chown -R staffcop:staffcop /var/lib/staffcop/upload/filedata
sudo chmod -R 774 /var/lib/staffcop/upload/filedata
```

4. Unmount disk:

```
sudo umount /dev/sdb1
```

5. Edit **/etc/fstab** file by specifying new disk there:

```
sudo nano -w /etc/fstab
```

Add similar type of line there:

```
/dev/sdb1/ /var/lib/staffcop/upload/filedata/ ext4  rw,noatime  0 2
```

Check if disk was mounted correctly by executing the following command:

```
sudo mount -a
```

6. Launch staffcop service:

```
sudo service staffcop start
```

Steps after StaffCop Enterprise installation

In case you deployed operation system by importing it from ova file, you should change user password.

If you deployed operation system using StaffCop image or Ubuntu official built, check if you password corresponds with requirements listed below:

Do not use simple passwords like “123”,”password”, etc. they are easy to guess. Do not use your date of birth, company name, and other words that are easy to guess.

To be on a safe side, use online password generator. If, for some reason, you do not have Internet access, or you are installing StaffCop Enterprise on server, where there is no javascript supported web browser, you can execute the following command to generate password:

```
 date | md5sum
```

or use **passwgen** utility, if you have it installed in your system.\\

Change password by executing the following command:

```
passwd
```

Change password of another user (if you have rights to do this) by executing the following command:

```
 passwd user
```

where "user" is other user’s login.\\

Remember or save this password in a safe place.

Activating StaffCop Enterprise

To activate your copy of StaffCop Enterprise enter IP of your computer on which you installed StaffCop Enterprise Server as URL in your web browser (we recommend to use either Firefox, or Google Chrome, Internet Explorer is not supported).

```
xxx.xxx.xx.xxx
```

If you do not know your StaffCop server IP, you can find it by entering the following command on console:

my_IP.sh

```
ifconfig | grep inet | grep -v inet6 | grep -v 127.0.0.1 | cut -d: -f2 | awk
'{printf $1"\n"}'
```

As a result, four groups of numbers, divided by decimal dots will be displayed. This is your StaffCop server IP address.

When you enter this IP address in your web browser, you gain access to admin panel.

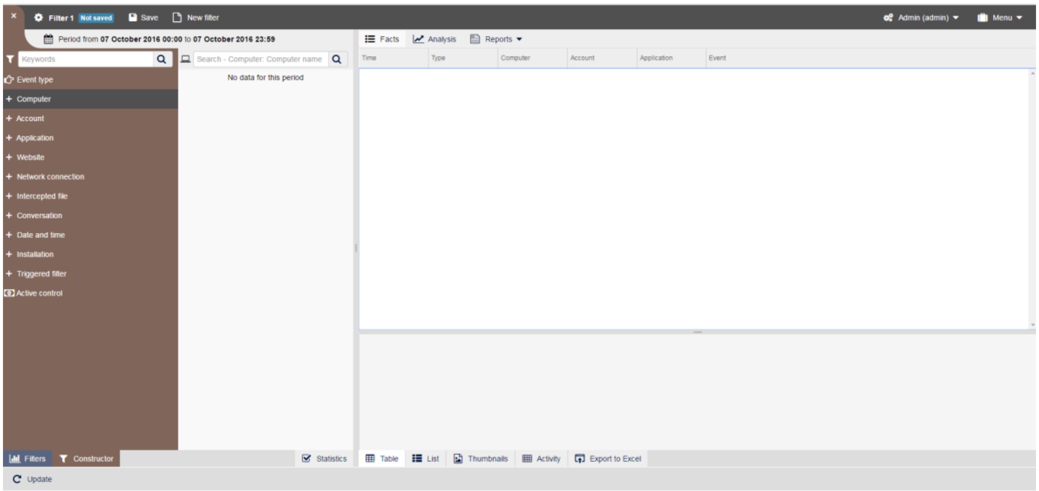
Create password for admin account, according to instructions contained in the previous section. Please remember admin account has a lot of access rights, so to protect it create a complex password.

NOTE: when you create password to admin panel, you can use any symbols except the following: quotes (“, '), dollar sign ($), forward slash (/).

Enter your license key or activate trial period. Trial period is 14 days.

Accessing web interface

Access admin panel using login “admin”, and password you’ve created yourself. The following admin panel will be displayed to you:


Period from **07 October 2016 00:00** to **07 October 2016 23:59**

No data for this period

Figure 76. Admin panel. First access.

Download StaffCop Agent from the admin panel, in order to install it on monitored workstations.

Complete the Agent installation according to instructions contained in Installation of StaffCop Enterprise Agent section of this guide.

Checking e-mail service performance

Check how are your e-mail auto alerts about important events related to system performance and security data are send out.

Auto cleanup

Consider data for what time period you would like to keep and what data you want to delete. After this, launch Disk auto cleanup.

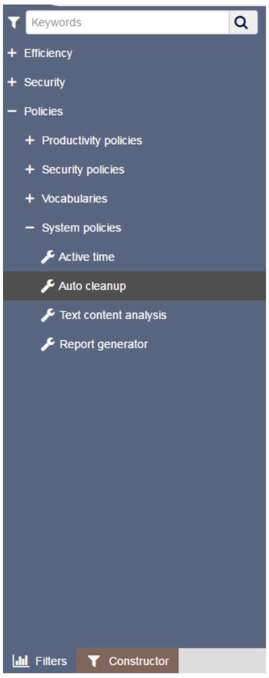


Figure 77. Auto cleanup.

Certificate access rights error

If certificates access error occurs after the agent is installed, please execute the following sequence of commands:

1. sudo chown postgres /etc/ssl/private/ssl-cert-snakeoil.key
2. sudo chown postgres /etc/ssl/certs/ssl-cert-snakeoil.pem
3. sudo chmod 600 /etc/ssl/private/ssl-cert-snakeoil.key
4. sudo chmod 600 /etc/ssl/certs/ssl-cert-snakeoil.pem

Changing time zone

In most cases, the time and time zone should be the same on StaffCop server and monitored workstations with installed StaffCop Agents.

You can set time and time zone during StaffCop Enterprise installation.

If you require to change time zone after StaffCop Enterprise is installed, execute the following command:

```
sudo dpkg-reconfigure tzdata
```

Next, you select geographic region and city.

To change current time execute date command:

```
sudo date 010412002016
```

Replace numbers with your date-time: Day/Month/Hour/Minute/Year, where two digits assigned to each value, except year, which has four-digit value.

Also, you can use time auto synchronization by applying **Network Time Protocol daemon** (NTPd)

Changing standard port 443

Sometimes you might require to change port to which StaffCop Agent sends aggregated data.

To do this, complete the following steps:

1. Change your password in StaffCop server settings:

```
nano /etc/nginx/sites-available/ssl.staffcop
```

Specify required value in a line instead of standard port 443.

Restart the service:

```
sudo service staffcop restart; sudo service nginx restart
```

2. Change port in StaffCop Agent settings.

You can implement this by reinstalling the Agent (the version you will be installing should be at least the same as the version of previously installed Agent or higher), or to change values in registry:

ADD HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TimeSvc3\ServiceConfiguration

Creating/deleting partitions

We will consider partitions creation based on work with real partitions under OS Linux.

In case when virtual machine is installed under VirtualBox VM, it works the same. The fact that we are working with virtual machine, does not change neither sequence nor syntaxes of executed commands.

General terms

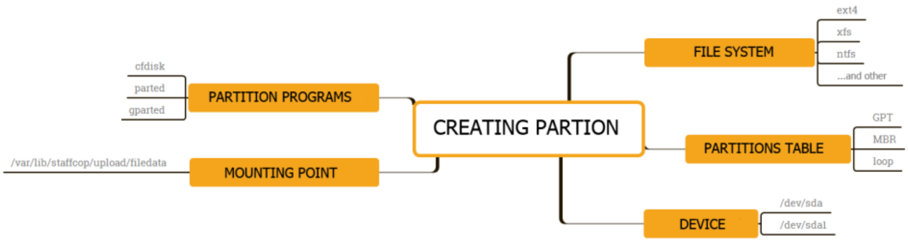


Figure 78. Creating partitions.

- Partition programs;
- Mounting point: this folder will contain contents of connected devices, for example, hard disk;
- Device: any device (hard disk, flash storage, CD, and etc.) that is seen under Linux as file. Usually it is displayed as /dev/sda, for example;
- Partitions table;
- File system.

Concept scheme of actions

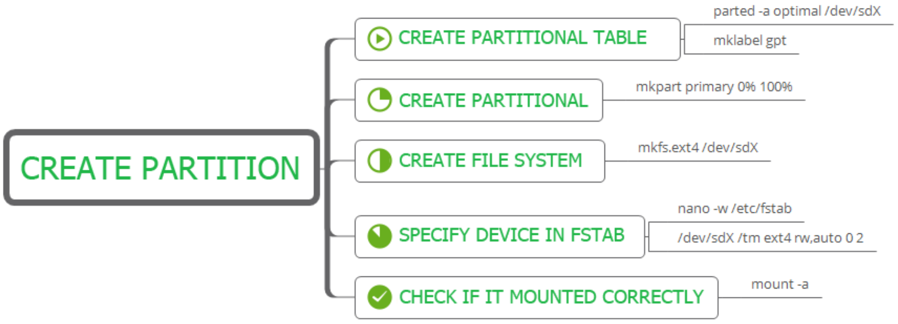


Figure 79. Create partition.

Be attentive during the following operations. They permanently delete information from hard disk. If you make mistake during these operations and will select different hard disk, you will loose all aggregated data.

If it is more convenient to you to work with graphic interface, you can download Live-Cd gparted, launch it and partition the disk as you require.

1. Select device (hard disk) which will be partitioned using the following command:

```
sudo parted -a optimal /dev/sdX
```

Go to command line interface.

2. Create partition table using a command similar to the following:

```
mklabel gpt
```

since we are using text interface of **parted** command, launched using superuser rights, you don't have to enter **sudo**.

3**.** Create partition using the following command:

```
mkpart primary 0% 100%
```

This means that we create one partition, which will allocate whole disk from the beginning to the end, and will be primary.

If you require for partition to occupy just a part of a disk, you can change its beginning or partition end.

4. Create file system.

There are several file systems in OS Linux. By default, **ext4** is used.

If you do not have a clear picture regarding advantages and disadvantages of each file system, the best choice is **ext4**. You can create it using the following command:

```
sudo mkfs.ext4 /dev/sdX
```

5. Specify device in **/etc/fstab** so it will be mounted automatically during each launch.

The command line will look approximately like this: **/dev/sdX /folder ext4 rw,auto 0 2**

6. Check if it is mounted correctly by executing the following command:

```
sudo mount -a
```

This command mounts all devices, specified in **/etc/fstab**, but not those which were mounted already.

Changing partition sizes

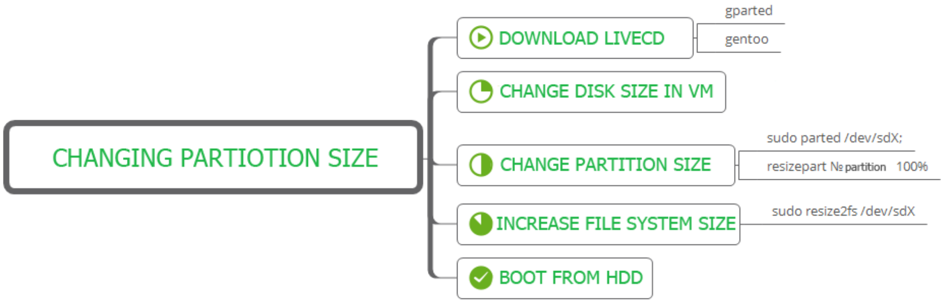


Figure 80. Changing partition size.

Sometime it is required to change partition size.

You have several options to do this. All of them are based on one main requirement: the partition which size you want to change should be unmounted:

unmount /dev/partiotion.

After this, launch **parted** and change partition size.

```
sudo parted /dev/disk

resizepart partition # 100%
```

this command will extend partition over whole free space left on hard disk if there is one.

Please note: any operations with partitions are potentially dangerous, and threaten integrity of your data, stored on partition you are changing.

The disk was expanded, but if you will not complete the following step, then new space won’t be available to your system.

Additionally, you have to exit from parted and execute the following command:

```
 sudo resize2fs /dev/sdX
```

After you change partition size, it is useful to check it:

```
 sudo fsck.ext4 -f /dev/sdX
```

Do not launch fsck on mounted partition. This can result in loosing all data.

Also, to change partition size you can launch from livecd gparted, and access graphic interface to work with your partitions.

You can use boot disk of majority of modern Linux distributives as live-cd.

Expanding hard disk

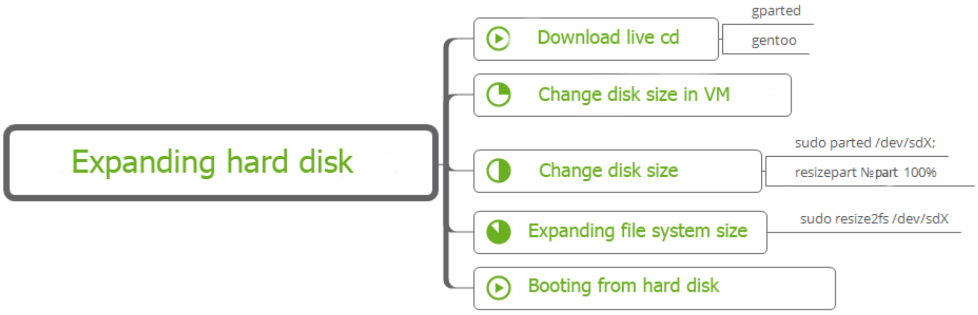


Figure 81. Expanding hard disk.

If your specified disk size is not enough, you have to expand it the disk.

Please note that any manipulations with partitions are potentially dangerous to your data. Make sure to create backups first.

In case with real physical server, increase the disk size by purchasing a new one and copying all data. In case with virtual server, if you have free space on physical – configure its settings.

The whole disk expansion procedure includes the following steps:

0. Create backups of OS, Database **backup**, and intercepted files;

1. Download live cd and stop virtual machine;

2. Change disk size in VM settings (see documentation to your virtualization environment);

3. Change partition size graphically using **gparted** or using **parted** in console mode;

4. Check file system;

5. Launch from hard disk;

StaffCop Enterprise Licensing policy

Activation key.

After purchasing StaffCop Enterprise, the user should activate StaffCop licenses via admin panel by entering Activation key issued by Licensor during the purchase of licenses. The Activation key can be used just once. After the licenses are activated, the Activation key is blocked. In case when additional activations are required, the user should contact Licensor and provide information about the reasons for additional activation. Licensor must consider this request and decide whether a new Activation key for the licenses can be additionally issued free of charge or for additional fee.

Starting with release of StaffCop Enterprise v. 3.1. we are introducing two types of StaffCop licenses: standard and competitive (“floating”) license.

Standard license.

One standard StaffCop Enterprise software license (one license for one workstation) gives the user the right to install and use the agent module (endpoint module) on a single workstation, the license binding is made to hardware ID. The number of installations on the same workstation (i.e. workstation with the same hardware ID) is not limited.

NOTE: Workstation’s hardware ID can be changed when workstation hardware is replaced or if OS Windows is replaced on monitored workstation. In this case, another standard license with new Activation key have to be issued.

Competitive license.

One competitive StaffCop Enterprise software license (one license for one workstation) gives the user the right to install and use the agent module (endpoint module) on a single workstation, the license binding is made to hardware ID. But unlike the case with standard license, if necessary the user is able to “free” this license, and re-install the agent on another workstation with another Hardware ID.

Both types of StaffCop licenses have unlimited time span. This means that you can use the product for which you have purchased StaffCop license for as long as you like. When you make an order for required number of licenses, we provide you with single activation key for all the licenses included in that order.

License agreement with end user of StaffCop Enterprise

ATTENTION! Current software was not sold to you, you are purchasing a license to use it according to the License Agreement provided below.

NOTICE TO USER:

THIS IS A CONTRACT. THIS END USER LICENSE AGREEMENT IS A LEGALLY BINDING CONTRACT THAT SHOULD BE READ IN ITS ENTIRETY. AT THE END, YOU WILL BE ASKED TO ACCEPT THIS AGREEMENT AND CONTINUE TO INSTALL OR, IF YOU DO NOT WISH TO ACCEPT THIS AGREEMENT, TO DECLINE THIS AGREEMENT, IN WHICH CASE YOU WILL NOT BE ABLE TO USE, INSTALL OR OPERATE THE PRODUCT, AS DEFINED

BELOW. BY INSTALLING THIS SOFTWARE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. THIS INSTALLATION PROCESS (WHICH MAY BE VIA A CD-ROM OR A WEB-BASED DOWNLOAD) PERMITS YOU TO INSTALL THE CURRENT VERSION OF THE SOFTWARE.

This Electronic End User License Agreement (the “Agreement”) is a legal agreement between you (either an individual or an entity), (the “Licensee”), and Atom Security Inc. (the “Licensor”), regarding the software Security Curator that you about to download, downloaded, or otherwise obtained through Licensor’s website(s) or other resources or media including without limitation CD or DVD disks or though a network in object code form via websites, file sharing networks, P2P networks, file archives, FTP servers or other related services, including without limitation (a) all of the contents of the files, disk(s), CD-ROM(s) or other media with which this Agreement is provided (the “Software”), and (b) all successor upgrades, revisions, patches, enhancements, fixes modifications, copies, additions or maintenance releases of the Software, if any, licensed to you by the Licensor (collectively, the “Updates”) provided that the Updates shall not include a new subsequent releases of the Software bearing a new first numeral such as 2.0 or 3.1 (“New Releases”) but include any minor revisions of the Software version indicated by a change in the decimal numeral, such as 2.3 or 2.4; and (c) related user documentation and associated materials or files provided in written, “online” or electronic form ((the “Documentation” and together with the Software, the “Product”). You are subject to the terms and conditions of this End User License Agreement whether you access or obtain the Product directly from the Licensor, or through any other source. For purposes hereof, “you” means the individual person installing or using the Product on his or her own behalf or, if the Product is being downloaded or installed on behalf of an organization, such as an employer, “you” means the organization for which the Product is downloaded or installed and you represent that you have authorized the person accepting this agreement to do so on your behalf. For purposes hereof the term “organization,” without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

For the purposes of this Agreement, “Licensor Site” shall mean the Internet website maintained by or on behalf of Licensor from which the Software is available for download pursuant to a license from Licensor. The Licensor Site is currently located at http://www.staffcop.com.

By accessing, downloading, storing, loading, installing, executing, displaying, copying the Product into the memory of a computer or otherwise benefiting from using the functionality of the Product in accordance with the Documentation (“Operating”), you agree to be bound by the terms of this Agreement. If you do not agree to the terms and conditions of this Agreement, the Licensor is unwilling to license the Product to you. In such event, you may not Operate or use the Product in any way.

BEFORE YOU CLICK ON THE “I AGREE” BUTTON CAREFULLY READ THE TERMS AND CONDITIONS OF THIS AGREEMENT. YOUR CLICK OF THE “I AGREE” BUTTON IS A SYMBOL OF YOUR SIGNATURE AND BY CLICKING ON THE “I AGREE” BUTTON, YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE “EXIT” BUTTON AND THE SOFTWARE WILL NOT BE INSTALLED ON YOUR COMPUTER. This Product will not install on your computer unless or until you accept the terms of this Agreement. You may also receive a copy of this Agreement by contacting the Licensor at: sales@staffcop.com.

1. Proprietary Rights and Non-Disclosure.

1.1. Ownership Rights. You agree that the Product and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Product, are proprietary intellectual properties and/or the valuable trade secrets of the Licensor or its suppliers and/or licensors and are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the United States, other countries and international treaties. You may use trademarks only insofar as to identify printed output produced by the Product in accordance with accepted trademark practice, including identification of trademark owner’s name. Such use of any trademark does not give you any rights of ownership in that trademark. The Licensor and/or its suppliers own and retain all right, title, and interest in and to the Product, including without limitations any error corrections, enhancements or other modifications to the Software, whether made by the Licensor or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Product does not transfer to you any title to the intellectual property in the Product, and you will not acquire any rights to the Product except as expressly set forth in this Agreement. All copies of the Product made hereunder must contain the same proprietary notices that appear on and in the Product. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Product and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Licensor reserves all rights not expressly granted to you in this Agreement.

1.2. Source Code. You acknowledge that the source code for the Product is proprietary to the Licensor or its suppliers and/or licensors and constitutes trade secrets of the Licensor or its suppliers and/or licensors. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Product in any way.

1.3. Confidential Information. You agree that, unless otherwise specifically provided herein, the Product, including the specific design and structure of individual programs and the Product, constitutes confidential proprietary information of the Licensor or its suppliers and/or licensors. You agree not to transfer, copy, disclose, provide or otherwise make available such confidential information in any form to any third party. [For purposes hereof, “License Key” shall mean a file or a unique sequence of digit and/or symbols provided to you by the Licensor confirming the purchase of the license from the Licensor, which may carry the information about the License, i.e. its type, the user name and the number of licenses purchased, and enabling the full functionality of the Product in accordance with the License granted under this Agreement.] You agree to implement reasonable security measures to protect such confidential information provided however, that you may make and distribute unlimited copies of the Product in object code only as long as each copy that you make and distribute contains this Agreement subject to end user’s acceptance before the first use, and the same copyright and other proprietary notices pertaining to the Product that appear in the Product. If you download the Software from the Internet or similar on-line source, you must include the copyright notices resident on the Software with any on-line distribution and on any media you distribute that includes the Software.

1.4. No Modification. You agree not to modify or alter the Product in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Product.

2. Grant of License.

2.1. License. THE LICENSE AND DOCUMENTATION MAY SPECIFY OTHER TERMS, CONDITIONS AND RESTRICTIONS OF OPERATING OF THE PRODUCT, INCLUDING WITHOUT LIMITATION, THE NUMBER OF EMPLOYEES AND ACCOUNTS THAT COULD BE ANALYZED OR MONITORED WITH EACH COPY OF THE PRODUCT, THE TYPE OF PERMITTED MONITORING, AND TYPE OF REPORTS GENERATED. The Licensor grants you the non-exclusive and non-transferable license to store, load, install, execute, and display (to “Use”) the specified version of the Software on a specified number of computers, workstations, personal digital assistants, ‘smart phones,’ mobile phones, hand-held devices, or other electronic devices for which the software was designed (each a “Client Device”) pursuant to the terms and conditions of this Agreement (“License”) and you hereby agree and accept such License as further provide below:

a) Personal Use License. If the Product is licensed under Personal Use License as reflected in the terms specified in the applicable invoicing or packaging for the Product you may use one copy of the Product on [one (1) Client Device] solely for

Personal Use. For purposes of this Agreement, “Personal Use” shall mean personal non-commercial use, and not on behalf or for the benefit of any clients and excludes any commercial purposes whatsoever, which include without limitation: advertising marketing and promotional materials/services on behalf of an actual client, employer, employee or for your own benefit, any products that are commercially distributed, whether or not for a fee, any materials or services for sale or for which fees or charges are paid or received.

b) Commercial Use License. If the Product is licensed under Commercial Use License as reflected in the License Key and/or invoicing terms specified in the applicable invoicing or packaging for the Product you may use the Product for Personal or Commercial Use (as defined below) in accordance with the Documentation and published functionality of the Product. For purposes hereof, “Commercial Use” shall mean any Operation of the Product for legal business, commercial, or government purpose in accordance with Documentation. One purchased Commercial Use License for the Product entitles you to Operate one copy of the licensed Product on one (1) Client Device provided that if multiple or volume licenses for Product are purchased, the number of the Client Devices and/or the number of permitted users shall be as provided and permitted by invoicing terms and/or applicable License Key.

c) Evaluation License. If the Product is licensed under Evaluation License terms as reflected in the License Key and/or invoicing terms specified in the applicable invoicing or packaging for the Product you may use the Product solely for purposes of demonstration and internal testing, examination and evaluation of the Product [on one (1) Client Device] for the period of fifteen (15) days.

d) [Site License. If the Product is licensed with site license terms specified in the applicable product invoicing or packaging for the Product, you may install and Use the Product on up to [100 Client Devices] within a single building owned or leased by your company unless otherwise specifically agreed by the Licensor or the number of maximum Client Devices within a single building owned or leased by your company as permitted by invoicing terms or applicable terms and conditions regarding the Site License set forth [on the Licensor’s web site ___________ at the time of purchase of the Commercial Use License]. Additionally, the individual licensing terms may specify other terms, conditions and restrictions of Using the Product.]

e) Educational Purpose License; Educational Institution Site License; Governmental and Non-profit License. If the Product is licensed to you under an Educational Purpose License, Educational Institution Site License, Governmental or Non-profit Use License upon the terms specified in the applicable invoicing or packaging for the Product, you may make use of the Product solely for the following purposes, respectively:

i. “Educational Purpose” means that you may make use of the Product solely for non-commercial study or research that is undertaken solely in furtherance of one’s education, whether or not completed by a student in pursuit of an educational degree, certificate or diploma and as used by teachers or facilitates teaching of a class, and all administrative staff, faculty and employees, of any college, university, trade school or other school (“Educational Institution”). Under “Educational Institution Site License” Licensee may install and Operate the Product by a number of users determined by the applicable invoicing terms within one Educational Institution in one geographic location. Educational License may be granted exclusively at the discretion of the Licensor upon your submission of a written request discussing your and your employer/employees activities, when applicable, and your reasons for and purposes of Operating the Product.

ii. “Governmental Purpose” means any non-commercial study or research that is undertaken solely in furtherance of one’s duties as a government employee; and

iii. “Non-profit Purpose” means any non-commercial activity or research that is undertaken solely in furtherance of one’s duties as part of the non-profit organization purposes narrowly interpreted.

Government License and Non-profit License may be granted exclusively at the discretion of the Licensor upon your submission of a written request discussing your and your employer/employees activities, when applicable, and your reasons for and purposes of Operating the Product..

2.2. Special provisions applicable to monitoring Software and Products. The monitoring Software and Products are offered and designed by Licensor for legal purposes only. You are granted a non-exclusive license to Use such Products to monitor programs, data, and files that You legally own, or where You obtained the express permission of the lawful owner to use the Product to monitor subject programs, data or files. Any illegal use of the Product automatically, without any notice, terminates this Agreement. By agreeing to this Agreement, You affirm that You have the legal right to monitor and access all data, information and files. YOU HEREBY EXPRESSLY AGREE THAT THE PRODUCT AND THE MONITORED DATA, PASSWORDS, INFORMATION AND/OR FILES ARE NOT USED FOR ANY ILLEGAL PURPOSE OR ANY OTHER PURPOSE PROHIBITED BY LICENSOR IN THE DOCUMENTATION, LICENSOR WEB SITE OR THIS AGREEMENT. NOTE THAT ILLEGALLY OBTAINED FILES, PASSWORDS, DATA AND OTHER INFORMATION MAY CONSTITUTE THEFT OR ANOTHER WRONGFUL ACTION AND MAY RESULT IN YOUR CIVIL AND (OR) CRIMINAL PROSECUTION.

2.3. Multiple Environment Product; Multiple Language Product; Dual Media Product; Multiple Copies; Bundles. If you use different versions of the Product or different language editions of the Product, if you receive the Product on multiple media, if you otherwise receive multiple copies of the Product, or if you received the Product bundled with other software, the total permitted number of your Client Devices on which all versions of the Product are installed shall correspond to the number of licenses you have obtained from the Licensor provided that unless the licensing terms provide otherwise, each purchased license entitles you to install and Use the Product on one (1) Client Device. Unless provided otherwise in this Agreement, you may not rent, bundle with other products or materials, lease, sublicense, lend or transfer any versions or copies of the Product regardless of whether you use the Product or not without Licensor's written consent.

2.4. [Updates; Support and Maintenance Services. Licensor will provide you with e-mail Support and Maintenance Services for a period of [one (1) year] from the purchase date, provided however that you may extend the Support and Maintenance Services, as available, by signing up and paying the appropriate annual subscription and fees to Licensor per applicable terms and conditions set forth on the Licensor's web site [www.____________.com]. Among other benefits of Maintenance and Support Services is that, during the term thereof, you may download [free] Updates to the Product when and as the Licensor publishes them in its website or through other online services. Maintenance and Support terms and conditions are subject to change without notice. Notwithstanding any provision to the contrary herein, nothing in this Agreement shall be construed as to grant you any rights or licenses with regard to the New Releases of the Product or to entitle you to any New Release. This Agreement does not obligate the Licensor to provide any Updates. Notwithstanding the foregoing, any Updates that you may receive become part of the Product and the terms of this Agreement apply to them (unless this Agreement is superseded by a further Agreement accompanying such Update or modified version of to the Product).]

2.5. Term and Termination. The term of this Agreement ("Term") shall begin when you download or install the Product (whichever is earlier) and shall continue, unless otherwise terminated pursuant hereto, in perpetuity or for the term specified in the License granted hereunder. The Licensor may terminate this Agreement by offering you a superseding Agreement for the Product or any replacement or modified version of the Product and conditioning your continued use of the Product or such replacement, modified or upgraded version or New Release on your acceptance of such superseding Agreement. This Agreement may be also terminated by the Licensor immediately and without notice if you fail to comply with any of your obligation or conditions of this Agreement. Without prejudice to any other rights, this Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately cease use of the Product and destroy all copies of the Product.

2.6. No Rights Upon Termination. Upon termination of this Agreement you will no longer be authorized to Operate or use the Product in any way.

2.7. Material Terms and Conditions. You specifically agree that each of the terms and conditions of this Section 2 are material and that failure of you to comply with these terms and conditions shall constitute sufficient cause for Licensor to immediately terminate this Agreement and the License granted under this Agreement, without any further notification. The presence of this Section 2.5 shall not be relevant in determining the materiality of any other provision or breach of this Agreement by either party hereto.

3. Restrictions.3.1. No Transfers. Under no circumstances you shall sell, loan, rent, lease, loan, license, sublicense, publish, display, distribute, or otherwise transfer to a third party the Product, any copy or use thereof, in whole or in part, without Licensor’s prior written consent, provided that if such non-waivable right is specifically granted to you under applicable law in your jurisdiction you may transfer your rights under this Agreement permanently to another person or entity, provided that a) you also transfer this Agreement, the Product, all accompanying printed materials, and all other software or hardware bundled or pre-installed with the Product, including all copies and prior versions, to such person or entity; b) retain no copies, including backups and copies stored on a Client Device; and c) the receiving party accepts the terms and conditions of this Agreement and any other terms and conditions upon which you legally purchased a license to the Product. Notwithstanding the foregoing, you may not transfer education, pre-release, or “not for resale” copies of the Product. In no case you may permit third parties to benefit from the use or functionality of the Product via a timesharing, service bureau or other arrangement, except to the extent such use is specified in the application price list, purchase order or product packaging for the Product.

3.2. Prohibitions. Except as otherwise specifically provided for in this Agreement, you may not use, copy, emulate, clone, rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, or otherwise reduce any party of the Product to human readable form or transfer the licensed Product, or any subset of the licensed Product, nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Notwithstanding the foregoing sentence, decompiling the Software is permitted to the extent the laws of your jurisdiction give you the non-waivable right to do so to obtain information necessary to render the Software interoperable with other software; provided, however, that you must first request such information from the Licensor and the Licensor may, in its discretion, either provide such information to you (subject to confidentiality terms) or impose reasonable conditions, including a reasonable fee, on such use of the Software to ensure that the Licensor's and its suppliers and/or licensors proprietary rights in the Software are protected. You may not modify, or create derivative works based upon the Product in whole or in part. Any such unauthorized use shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution. Neither Product’s binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary, without written permission of the Licensor. All rights not expressly granted here are reserved by Licensor and/or its suppliers and licensors, as applicable.

3.3. Proprietary Notices and Copies. You may not remove any proprietary notices or labels on the Product. You may not copy the Product except as expressly permitted in Section 2 above.

3.4. No Transfer of Rights. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.

3.5. [License Key. You may not give, make available, give away, sell or otherwise transfer your registration License Key or any copy thereof to a third party. Product’s License Key may not be distributed, except as provided herein, outside of the area of legal control of the person or persons who purchased the original License, without written permission of the Licensor. Doing so will result in an infringement of copyright. The Licensor retains the right of claims for compensation in respect of damage which occurred by your giving away the License Key or registration code contained therein. This claim shall also extend to all costs which the Licensor or its licensors incur in defending themselves.]

3.6. Compliance with Law. You agree that in Operating the Product and in using any report or information derived as a result of Operating this Product, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law. Furthermore, in operating the Product, you specifically agree not to engage in any activity, which has been made illegal pursuant to CAN-SPAM Act of 2003, 15 U.S.C. 7701 et seq., including sending and distributing spam e-mails.

3.7. Indemnification. You agree to indemnify, defend and hold harmless Licensor and its respective officers, directors, employees, Agents, successors, and assigns from any and all losses, liabilities, damages and claims, and all related expenses (including reasonable legal fees and disbursements and costs of investigation, litigation, settlement, judgment, interest and penalties) and costs related to, arising from, or in connection with any third-party claim related to, arising from, or in connection with the actual or alleged: (i) infringement by Licensee (except when such breach is exclusively attributable to Product) of any third-party intellectual property and/or proprietary right, including, but not limited to, patent, trademark, copyright, trade secret, publicity and/or privacy, (ii) personal injury (including death) or property damage due to the gross negligence or intentional misconduct of Licensee, and/or (iii) breach by Licensee of any of its representations, warranties, obligations, and/or covenants set forth herein.

3.8. Additional Protection Measures. Solely for the purpose of preventing unlicensed use of the Product, the Software may install on your computer technological measures that are designed to prevent unlicensed use, and the Licensor may use this technology to confirm that you have a licensed copy of the Product. The Licensor will not collect any personally identifiable information from your computer during this process.

4. NO WARRANTY AND DISCLAIMER.

4.1. Customer Remedies. The Licensor and its suppliers' entire liability and your exclusive remedy for any breach of the foregoing warranty shall be at the Licensor's option: (i) return of the purchase price paid for the license, if any, (ii) replacement of the defective media in which the Product is contained, or (iii) correction of the defects, "bugs" or errors within reasonable period of time. You must return the defective media to the Licensor at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period.

4.2. NO IMPLIED OR OTHER WARRANTIES. EXCEPT FOR THE FOREGOING LIMITED WARRANTY AND FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM TO THE EXTENT TO WHICH THE SAME CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO YOU IN YOUR JURISDICTION, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY WHATSOEVER AND THE LICENSOR MAKES NO PROMISES, REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE, REGARDING OR RELATING TO THE PRODUCT OR CONTENT THEREIN OR TO ANY OTHER MATERIAL FURNISHED OR PROVIDED TO YOU PURSUANT TO THIS AGREEMENT OR OTHERWISE. YOU ASSUME ALL RISKS AND RESPONSIBILITIES FOR SELECTION OF THE PRODUCT TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE PRODUCT. THE LICENSOR MAKES NO WARRANTY THAT THE PRODUCT WILL BE ERROR FREE OR FREE FROM INTERRUPTION OR FAILURE, OR THAT IT IS COMPATIBLE WITH ANY PARTICULAR HARDWARE OR SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, LICENSOR DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, INTEGRATION, SATISFACTORY QUALITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH RESPECT TO THE PRODUCT AND THE ACCOMPANYING WRITTEN MATERIALS OR THE USE THEREOF. SOME JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU HEREBY ACKNOWLEDGE THAT THE PRODUCT MAY NOT BE OR BECOME AVAILABLE DUE TO ANY NUMBER OF FACTORS INCLUDING WITHOUT LIMITATION PERIODIC SYSTEM MAINTENANCE, SCHEDULED OR UNSCHEDULED, ACTS OF GOD, TECHNICAL FAILURE OF THE SOFTWARE, TELECOMMUNICATIONS INFRASTRUCTURE, OR DELAY OR DISRUPTION ATTRIBUTABLE TO VIRUSES, DENIAL OF SERVICE ATTACKS, INCREASED OR FLUCTUATING DEMAND, AND ACTIONS AND OMISSIONS OF THIRD PARTIES. THEREFORE, THE LICENSOR EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY REGARDING SYSTEM AND/OR SOFTWARE AVAILABILITY, ACCESSIBILITY, OR PERFORMANCE. THE LICENSOR DISCLAIMS ANY AND ALL LIABILITY FOR THE LOSS OF DATA DURING ANY COMMUNICATIONS AND ANY LIABILITY ARISING FROM OR RELATED TO ANY FAILURE BY THE LICENSOR TO TRANSMIT ACCURATE OR COMPLETE INFORMATION TO YOU.

4.3. LIMITED LIABILITY; NO LIABILITY FOR CONSEQUENTIAL DAMAGES. YOU ASSUME THE ENTIRE COST OF ANY DAMAGE RESULTING FROM YOUR USE OF THE PRODUCT AND THE INFORMATION CONTAINED IN OR COMPILED BY THE PRODUCT, AND THE INTERACTION (OR FAILURE TO INTERACT PROPERLY) WITH ANY OTHER HARDWARE OR SOFTWARE WHETHER PROVIDED BY THE LICENSOR OR A THIRD PARTY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL THE LICENSOR OR ITS SUPPLIERS OR LICENSORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF GOODWILL, WORK STOPPAGE, HARDWARE OR SOFTWARE DISRUPTION IMPAIRMENT OR FAILURE, REPAIR COSTS, TIME VALUE OR OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR THE INCOMPATIBILITY OF THE PRODUCT WITH ANY HARDWARE SOFTWARE OR USAGE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LICENSOR’S TOTAL LIABILITY TO YOU FOR ALL DAMAGES IN ANY ONE OR MORE CAUSE OF ACTION, WHETHER IN CONTRACT, TORT OR OTHERWISE EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

5. U.S. Government-Restricted Rights.

5.1. Notice to U.S. Government End Users. The Product and accompanying Documentation are deemed to be “Commercial Items,” as that term is defined at 48 C.F.R. §2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” respectively, as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights, including any use, modification, reproduction, release, performance, display or disclosure of the Product and accompanying Documentation, as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

5.2. Export Restrictions. You acknowledge and agree that the Product may be subject to restrictions and controls imposed by the Export Administration Act and the Export Administration Regulations of the United States (the “Acts”). You agree and certify that neither the Product nor any direct product thereof is being or will be used for any purpose prohibited by the Acts. You may not Operate, download, export, or re-export the Product (a) into, or to a national or resident of, any country to which the United States has embargoed goods, or (b) to anyone on the United States Treasury Department’s list of Specially Designated Nationals or the U.S. Commerce Department’s Table of Deny Orders. By downloading or using the Product, you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list. You acknowledge that it is your sole responsibility to comply with any and all government export and other applicable laws and that the Licensor has no further responsibility for such after the initial license to you. You warrant and represent that neither the U.S. Commerce Department, Bureau of Export Administration nor any other U.S. federal agency has suspended, revoked or denied your export privileges.

6. Your Information and the Licensor’s Privacy Policy.

6.1. Privacy Policy. You hereby expressly consent to the Licensor’s processing of your personal data (which may be collected by the Licensor or its distributors) according to the Licensor’s current privacy policy as of the date of the effectiveness hereof which is incorporated into this Agreement by reference. By entering into this Agreement, you agree that the Licensor may collect and retain information about you, including your name, e-mail address and credit card information. The Licensor employs other companies and individuals to perform functions its behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, processing credit card payments, and providing customer service. They have access to personal information needed to perform their functions, but may not use it for other purposes. The Licensor publishes a privacy policy on its web site and may amend such policy from time to time in its sole discretion. You should refer to the Licensor's privacy policy prior to agreeing to this Agreement for a more detailed explanation of how your information will be stored and used by the Licensor. If "you" are an organization, you will ensure that each member of your organization (including employees and contractors) about whom personal data may be provided to the Licensor has given his or her express consent to the Licensor's processing of such personal data. Personal data will be processed by the Licensor or its distributors in the country where it was collected, and possibly in the United States and Russian Federation. The laws of such jurisdictions regarding processing of personal data may be less or more stringent than the laws in your jurisdiction.

7. Miscellaneous.

7.1. Governing Law; Jurisdiction and Venue. This Agreement shall be governed by and construed and enforced in accordance with the laws of European Union without reference to conflicts of law rules and principles. To the extent permitted by law, the provisions of this Agreement shall supersede any provisions of the Uniform Commercial Code as adopted or made applicable to the Products in any competent jurisdiction. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly disclaimed and excluded. The federal and state courts within the Commonwealth of Virginia shall have exclusive jurisdiction to adjudicate any dispute arising out of this Agreement. You agree that this Agreement is to be performed in the Commonwealth of Virginia and that any action, dispute, controversy, or claim that may be instituted based on this Agreement, or arising out of or related to this Agreement or any alleged breach thereof, shall be prosecuted exclusively in the federal or state courts in of the Commonwealth of Virginia and you, to the extent permitted by applicable law, hereby waive the right to change venue to any other state, county, district or jurisdiction; provided, however, that the Licensor as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

7.2. Period for Bringing Actions. No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

7.3. Entire Agreement; Severability; No Waiver. This Agreement is the entire agreement between you and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Product or to subject matter of this Agreement provided that the Licensor and you may limit, modify or changes the applicability of the terms of this Agreement by a prior, contemporaneous or subsequent written agreement by referencing this Section 6.3 of the Agreement and expressly providing for such limitation, modification or changes. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the fullest extent permitted by law. No waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach and no waiver will be effective unless made in writing.

7.4. Contact Information. Should you have any questions concerning this Agreement, or if you desire to contact the Licensor for any reason, please contact our Customer Department sales@staffcop.com.

7.5. The Product, Software and any accompanying Documentation, are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.