



SecureTower™

Administrator Guide

Table of Contents

1 Program Overview	7
2 Preparing to start: Connecting to the server	8
3 Monitoring system status	10
3.1 Starting and stopping services	11
3.1.1 Service startup parameters	11
3.1.1.1 Service startup modes	12
3.1.1.2 Selecting a user account to start up	14
3.2 Setting up connection ports for services	14
3.3 Configuring log of system events	19
3.4 Managing system configuration	20
4 Configuring Licence Server	23
4.1 Viewing licence information	23
4.2 Setting up connection to the license server	25
4.3 Updating licence information	27
5 Setting up Interception Server	28
5.1 Interception of tagged VLAN traffic	28
5.1.1 Using specialized drivers	29
5.1.2 Special flag settings	29
5.2 Configuring general parameters	31
5.2.1 Selecting data storage type	32
5.2.1.1 Setting up a connection to a MS SQL Server database	33
5.2.1.2 Setting up a connection to a Oracle database	39
5.2.1.3 Setting up a connection to a Postgre SQL database	41
5.2.1.4 Setting up a connection to a SQLite database	42
5.2.1.5 Setting up a connection to a MySQL database	43
5.2.1.6 Changing current database settings	44

5.2.2	Advanced interception settings	44
5.2.3	License server information	46
5.3	Setting up supported protocols for centralized traffic interception	47
5.3.1	List of supported protocols and default ports	48
5.3.2	Assigning protocol ports for interception	50
5.3.3	Configuring interception of protocols	50
5.3.3.1	POP3, SMTP and IMAP settings.....	51
5.3.3.2	OSCAR settings	52
5.3.3.3	XMPP settings.....	54
5.3.3.4	HTTP settings.....	55
5.3.3.5	FTP settings.....	66
5.3.3.6	Mail.Ru Agent settings.....	67
5.3.3.7	Yahoo settings.....	67
5.3.3.8	MAPI settings	67
5.3.3.9	Disabling interception for certain accounts.....	68
5.4	IP-filter settings	70
5.5	Assigning MAC address filters for traffic interception	73
5.6	Network adapters settings	75
5.6.1	Assigning network adapters for traffic interception	76
5.6.2	Advanced settings	76
5.7	Interception statistics	77
5.7.1	Calculating statistics for a specified interval	78
5.7.2	Interception statistics for a certain network adapter	78
6	Setting up data indexing.....	79
6.1	Viewing list of indexes	79
6.2	Creating a search index	81
6.2.1	Setting up index parameters	81
6.2.2	Configuring the scheduler	88
6.3	Modifying a search index	94
6.4	Deleting a search index	95
6.5	Updating index	96
6.6	Clearing a search index	96
7	Setting up digital fingerprints.....	97
7.1	Creating Data Banks	97
7.1.1	Setting up data bank parameters	98

- 7.1.2 Configuring the scheduler 105
- 7.2 Other operations with data banks106
- 8 Configuring files hash banks.....107**
- 9 Setting up system events and notifications.....108**
- 9.1 System events 109
- 9.2 System notifications 111
- 9.3 General settings113
- 10 Setting up user identification service.....116**
- 10.1 General settings 116
 - 10.1.1 Active Directory and domains integration 116
 - 10.1.2 Setting user authentication mode 128
- 10.2 User management129
 - 10.2.1 Creating a user card 129
 - 10.2.1.1 General user information..... 130
 - 10.2.1.2 User Network identification..... 130
 - 10.2.1.3 User contact identification..... 134
 - 10.2.1.4 User groups..... 134
 - 10.2.2 Modifying a user card 135
 - 10.2.3 Deleting a user card 136
 - 10.2.4 Importing users from Active Directory 137
 - 10.2.5 Updating user information from Active Directory..... 138
- 10.3 Managing user groups and access rights139
 - 10.3.1 Creating a user group 139
 - 10.3.2 Modifying a user group 144
 - 10.3.3 Deleting a user group 144
- 10.4 Authentication journal review144
- 11 Configuring Endpoint Agents.....146**
- 11.1 Installing endpoint agents on workstations147
 - 11.1.1 Centralized installation 147
 - 11.1.1.1 The list of objects to install agents on..... 149
 - 11.1.1.2 The list of excluded computers..... 151
 - 11.1.1.3 Assigning access credentials..... 152
 - 11.1.1.4 Agents deinstallation..... 152

11.1.1.5 Managing list of objects.....	153
11.1.2 Remote agent installation by Group Policy	153
11.1.3 Manual agent installation	160
11.2 Server information	163
11.3 Configuring the database	164
11.4 Agent settings profile	164
11.4.1 Creating agent settings profile	165
11.4.1.1 Settings profile information.....	165
11.4.1.2 Network traffic interception.....	167
11.4.1.3 Control of storage devices.....	179
11.4.1.4 Control of devices.....	184
11.4.1.5 Printer interception.....	185
11.4.1.6 Skype interception	187
11.4.1.7 Viber interception.....	189
11.4.1.8 Telegram interception.....	190
11.4.1.9 SIP interception.....	191
11.4.1.10 Lync interception	192
11.4.1.11 Browser interception.....	193
11.4.1.12 Control of network shares	193
11.4.1.13 Cloud storage control.....	197
11.4.1.14 Desktop activity.....	200
11.4.1.15 Audio/video Monitoring.....	204
11.4.1.16 Data blocking.....	205
11.4.1.17 File system control.....	216
11.4.1.18 Miscellaneous agent settings.....	216
11.4.1.19 Managing interception exclusions.....	219
11.4.2 Managing profile list	220
11.4.3 Priority of agent profile	220
11.5 Automatic assignment of contact information	221
11.6 Updating endpoint agents version	224
11.7 Setting up computers indexing.....	224
11.8 License server information	229
11.9 Monitoring endpoint agents status	229
12 Setting up mail processing.....	240
12.1 Setting up mail interception	240
12.1.1 MS Exchange connection	240
12.1.2 Connecting to mail server over POP3 protocol	242

- 12.1.3 Receiving mail from server over SMTP protocol 243
- 12.2 Miscellaneous mail processing settings244
- 12.3 Configuring a mail journaling mechanism248
 - 12.3.1 Journaling to internal mailbox..... 248
 - 12.3.2 Journaling to external mailbox 253
- 13 Setting up ICAP server.....257**
 - 13.1 General settings257
 - 13.2 IP filter settings260
 - 13.3 HTTP filter settings260
 - 13.4 Data blocking260
 - 13.5 ICAP statistics261
- 14 Configuring image recognition.....262**
 - 14.1 Setting up built-in plugin262
 - 14.2 ABBYY settings267
 - 14.3 Setting up data storages274
 - 14.4 Image recognition statistics275

1 Program Overview

SecureTower Overview

Falcongaze SecureTower is a complex software product for ensuring internal information security through network traffic interception and analysis.

This solution enables enterprises to control leak and undesired disclosure of confidential information over Internet by intercepting such information as incoming and outgoing e-mail, chat in instant messengers, transferred documents, files, viewed web pages, etc.

The administrator application (console) of the program is used for adjusting operation settings of all services: Interception, Database, Search, Indexing, Endpoint Agent Control, etc. One can set and change data interception and filtration parameters, indexing frequency, create network user cards. It also enables one to view capture statistics in a real-time mode, arrange delivery of notifications about the system operation (such events as database overloading) and install endpoint agents on local workstations in a remote mode to arrange Skype, USB, Network shares and SSL traffic interception.

Getting started

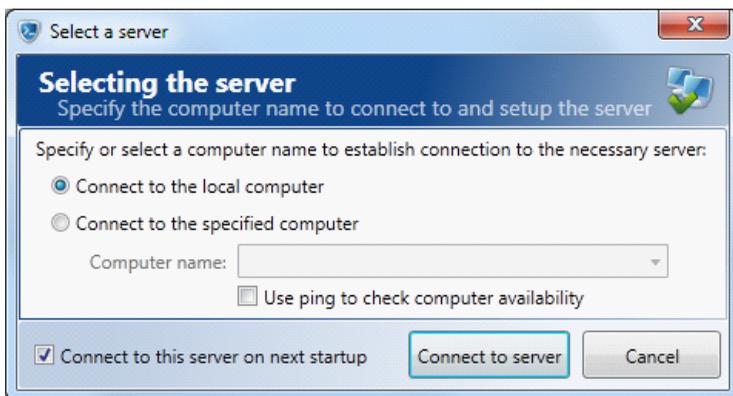
- Study this guide to familiarize yourself with the basics of the program.
- Even if you are an experienced **Falcongaze SecureTower** user please run through the **Administrator Guide** sections to get up to speed with what has changed in the latest version of the program.
- To access parameters of any service, just click on a relevant tab in the left sidebar in the main window of console.

2 Preparing to start: Connecting to the server

Upon the first startup of Administrator Console one must select the server to start working. Taking into account that the interception system can be scaled, the system's components can be installed on different physical servers. The system configuration is performed in the console by individually setting up each server responsible for different services.

Note: *In an individual case, all the interception system components can be installed on the same server. Correspondingly, their setup will be performed on a single server.*

The server to connect to can be selected in the Select a server dialogue box that automatically appears on the screen upon the first program startup.



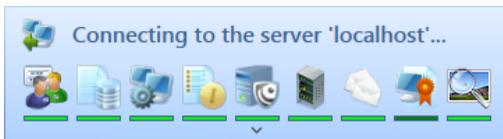
Selecting the server to connect to window

Note: *To work with Administrator Console you must have administrator rights on the server you are connecting to or you must be included in group with the corresponding access rights (for more information, see [Managing user groups and access rights](#)).*

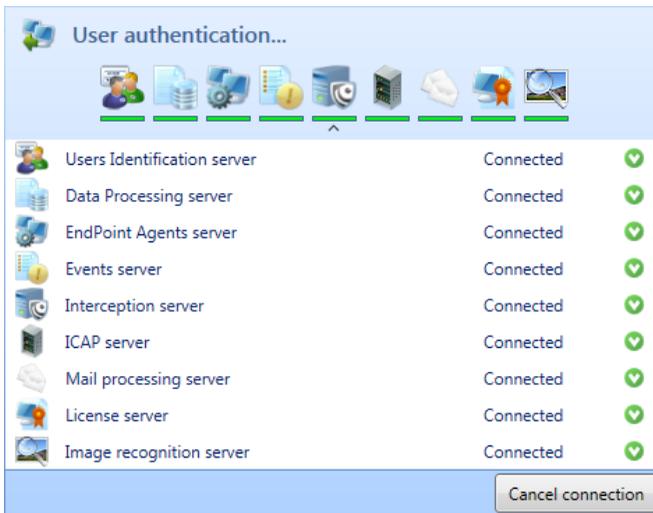
Directions:

1. If any components that should be configured are installed on the local computer, click the **Connect to the local computer** button. If components to be set up are installed on a different servers, click the **Connect to the specified computer** button and specify the name of the required computer in the **Computer name** text box. If this computer name has already been entered before, one can select it from the drop-down menu opened by clicking the arrow icon located in the right corner of the text box.
2. To send a ping request to the remote computer before actual connection, select the **Use ping to check computer availability** check box. This will shorten the delay in case the remote computer is unavailable, as ping takes much less time than the system needs to detect the unavailability of the remote computer by trying to connect to it directly. Clear this check box if ping is disabled in your network.
3. Connecting is followed by connection status bar. To display a detailed report for each

server state, click the expand arrow.

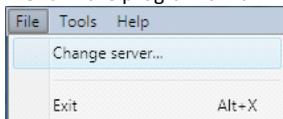


4. To interrupt connection, click **Cancel connection**.



5. After connecting to the necessary server, one can start configuring of components installed on it. If it is necessary to establish connection to previously specified server automatically upon subsequent startups, select the **Connect to this server on next startup** check box while selecting the server. This option is switched off by default.

6. If the components to be configured are installed on another physical server, on the **File** menu in the program's main window, click **Change server**.



7. In the **Select a server** dialogue box, click the **Connect to the specified computer** button and specify the name of the required computer as described above.

8. Once connection to a particular server is established, the **Status monitor** window is displayed.

Note: Click **Apply changes** located in the right bottom corner of the program's main window every time when you finish configuring the necessary service settings in Administrator Console.

3 Monitoring system status

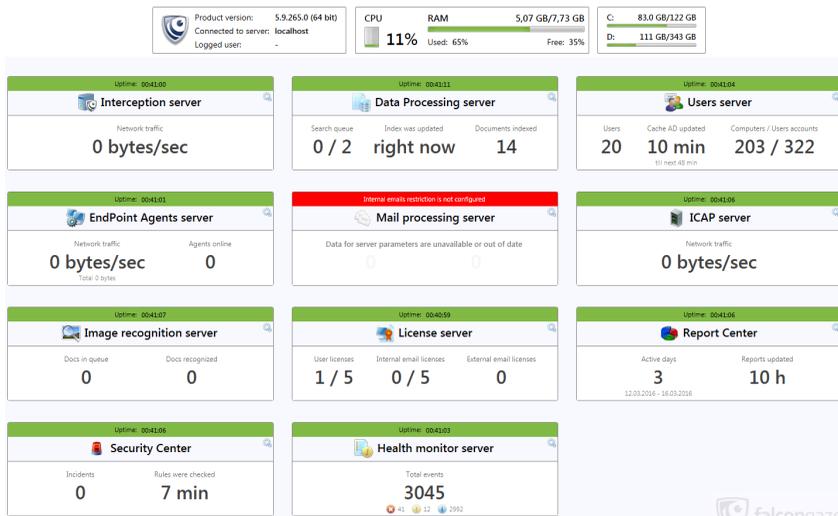
To monitor the status and administrate **SecureTower** server components in the real-time mode click the **Status monitor** tab on the left sidebar of the program's main window.

The set of dashboards are displayed in the Status monitor window:

- **Falcongaze SecureTower** dashboard displays information about the product version number, connected server name and logged user name;
- computer resources dashboard provides information about the currently connected computer CPU load and RAM;
- local drive dashboard provides a total capacity and available free disk space for all local disks.



Attention: To provide the local drive dashboard display the operating system performance counters must be enabled. To enable the counters, the "0" value must be set for the "Disable Performance Counters" entry in the registry: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib] "Disable Performance Counters"=dword:0



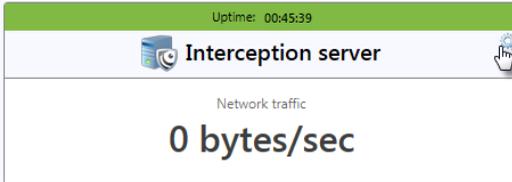
Status monitor enables access to the set of **SecureTower** components dashboards and their startup settings.

A dashboard of components with any error is marked with the red color header. In this case the error message is displayed on the header line. To navigate between errors use the navigation buttons in the header.

Attention: Make sure you have logged in as a user with enough access permissions before start working with server components and settings. To change access permissions, follow the recommendations given in [Managing user groups and access rights](#) or contact your system administrator.

3.1 Starting and stopping services

Starting and stopping a certain service is available only if Administrator Console is connected to the computer where this service is installed and this computer is switched on.



Starting a service

1. Select the necessary service dashboard in the **Status monitor** window.
2. Click the "Settings" button  in the right top corner of the dashboard.
3. Click **Start service**.

Stopping a service

1. Select the necessary service dashboard in the **Status monitor** window.
2. Click the "Settings" button  in the right top corner of the dashboard.
3. Click **Stop service**.

Restarting

Restarting a service will turn it off and then on.

1. Select the necessary service dashboard in the **Status monitor** window.
2. Click the "Settings" button  in the right top corner of the dashboard.
3. Click **Restart service**.

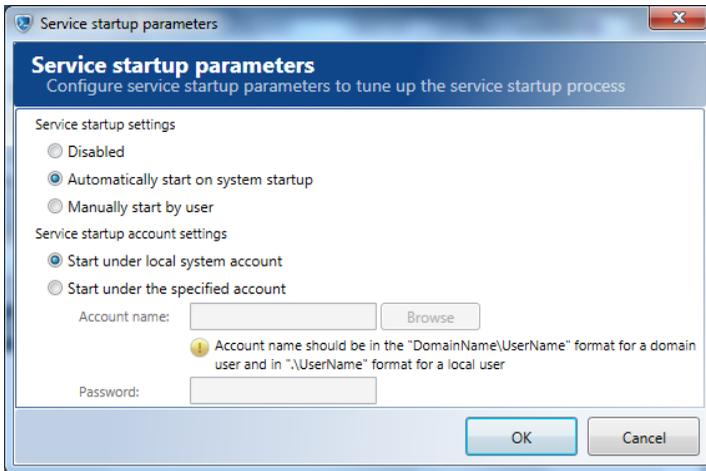
3.1.1 Service startup parameters

To configure the startup parameters:

1. Select the necessary service dashboard in the **Status monitor** window (**Status monitor** tab in the left sidebar of the program's main window).
2. Click the "Settings" button  in the right top corner of the dashboard.
3. Click **Service startup parameters**.

Note: Configuring startup parameters of any service is available only if the computer where this service is installed is switched on. Herewith, the service which it is necessary to configure may be switched off.

4. Set the startup type and startup account type in the **Service startup parameters** window. For more information, see [Service startup modes](#).
5. Select one of the login conditions for service startup.
 - To start service under local system account, click the respective radio button (used by default).
 - To start service under the particular account, click the respective radio button and type an account name with the sufficient access rights in the corresponding field or click **Browse** to select the account from AD structure or from the list of local machine users (for more information, see [Selecting a user account to start up](#)). Type the password for specified account name in the corresponding text box.



6. Click **OK** to apply settings.

The account name under which a server is started and operates is appeared in the right bottom corner of the server dashboard.

3.1.1.1 Service startup modes

Automatic service startup

If continuous operation of any service is important, select the **Automatically start on system startup** radio button in the **Service startup parameters** window. This startup mode is set by default.



Thus, upon the operating system boot, **SecureTower** Interception Server will automatically starts monitoring and will be active while the system is working. To access and work with captured data, one only needs to start Client Console; to view interception statistics in real time mode – Administrator Console.

Note: *If this startup mode is disabled for a certain service or the server on which this service is installed is turned off, the functions of such a service will be unavailable upon the startup of other services. For example, if **Data interception server** works, but **Data Indexing service** is disabled, the intercepted data will not be indexed, and Client Console user will not be able to search them.*

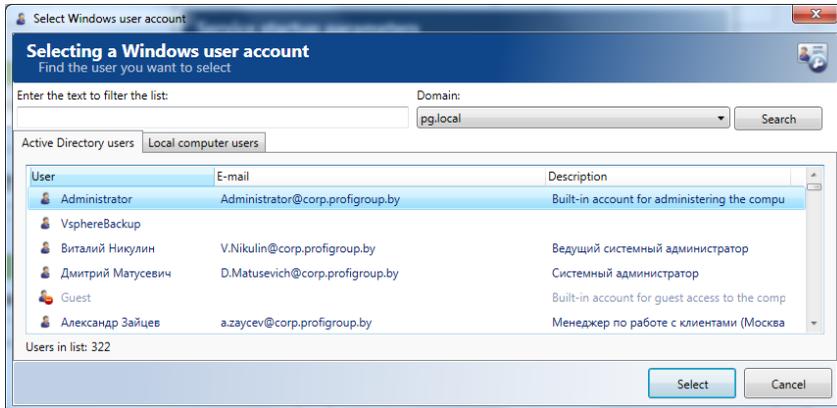
Manual service startup

If there is no need in continuous operation of the service, select the **Manually start by user** radio button in the Service startup parameters window.

Disabling service startup options

To block service, select the **Disabled** radio button in the Service startup parameters window.

3.1.1.2 Selecting a user account to start up



To select a user account of the current domain or from the list of users of local machine:

1. Click the drop-down button related to **Domain** field in the **Select a Windows user account** window.
2. Click the necessary domain to search a user account in (only domains included in network appear in the list), and then click **Search**.
3. Click the the corresponding tab to select a user:
 - To select a user account from AD, click the **Active Directory users tab**.
 - To select a user account from the list of users of local machine, click the **Local computer users** tab.
4. To arrange the user name in the list by **User**, **E-mail** or **Description**, click the header of corresponding column.
5. To find a particular user name in the list, type the user account name in the text field. As you type, only the account that have the entered symbols in their names will be displayed in the list.
6. Click the necessary account in the list, and then click **Select**.

3.2 Setting up connection ports for services

If a certain port of a computer that is set as default port for a certain **SecureTower** component is already used by another program, it is recommendable to change the server port settings.

In the configuration files of the server components of **SecureTower**, change default ports to the ports that should be used to connect to the servers. Please note that **Interception server** uses a different connection technology, so there are no port settings available for this server.

Server port settings in the configuration files:

1. The configuration files should be normally located in the folder at the following address: **C:\Documents and Settings\All Users\Application Data\FalconGaze SecureTower** (OS Windows under Windows Vista) or **C:\Program Data\FalconGaze SecureTower** (Windows Vista and Windows 7).

Use the following information to find server port settings in the configuration files:

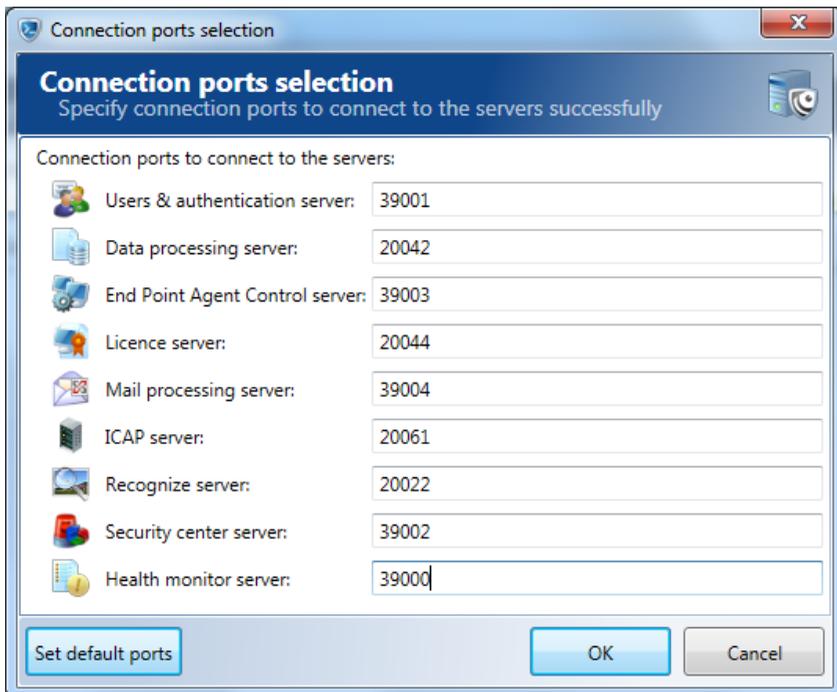
Configuration File	Line values
License Server	
LicenseServer.Config.xml	<Server port="20044" />
Security Center	
SecurityCenterServer.config	<SearchServerConnection Port="20043" /> <AuthServerConnection Port="39001" /> <TcpChannel Port="39002" />
Indexing Service	
SearchService.xml	<Indexer port="20042">
Search Service	
SearchService.xml	<Searcher port="20043">
EndPoint Agents Control Server	
FgSTEndPointAgentControlServerSettings.dat	<TCPChannel Port="39003" /> <EndPointAgentControlServerSettings Version="1" VersionChangeTime="20140522122055" VersionChangeComputer="FGSERVER" VersionChangeUser="" EndPointAgentInstallStrategy="0" ServerName="FGSERVER" Port="10500" AgentCheckInterval="30" UseICMP="1" UseSSLEncryption="0" LicenceServerName="localhost" LicenceServerPort="20044">
User Identification Server	
FgSTAuthServerSettings.xml	<TCPChannel Port="39001" />
Events Server	
FgSTEventsServerSettings.xml	<TCPChannel Port="39000" />
Icap Server	
IcapServerPluginSettings.xml	<IcapServer ISTAG="5BDEEEA9-12E4-2" MaxConnections="3000" OptionsTTL="7200" Port="1344" Preview="4096" ServeID="Falcongaze SecureTower ICAP Server" TransferPreview="*">

Configuration File	Line values
	<LicenseInfo Port="20044" Server="localhost" />
icap_server_settings.xml	<port>20061</port> <address>localhost:20044</address>
Image recognition Server	
Recognize_server_api.xml	<Port>20022</Port>
Recognize_server_licence.xml	<ServerPort>20044</ServerPort>
Mail processing Server	
MailProcessingServer.config	<TcpChannel Port="39004" /> <LicenceServer LicenceServerName="localhost" LicenceServerPort="20044" />

2. Click the **Status monitor** tab in the left sidebar of the program's main window, and restart the services that you have modified the connection ports for.
3. On the **Tools** menu click **Configure connection ports**.

Selecting server connection ports:

On the **Tools** menu click **Configure connection ports**.



1. In the **Connection ports selection** window, specify the same ports that you have specified for each server in the respective configuration files.
2. If you need to restore the default ports, click **Set default ports**.
3. Click **OK** to save the settings.

Firewall configuring

To provide the correct way of **SecureTower** activity (to prevent unauthorized connections to the server components and problems with the licenses distribution) one should configure the firewall in a specific way.

The list of following ports should be created while firewall configuring:

1. Obligatorily **SecureTower** connection ports
 - Connection ports to provide connection to the system server:
 - Data processing server (IndexationServer) 20042
 - Licence server (LicenceServer) 20044
 - User and authentication server (AuthServer) 39001
 - Security Center Server 39002

EndPoint Agent Control Server 39003

Mail Processing Server 39004

ICAP Server 20061

Recognize Server 20022

Health Monitor 39000

- EndPoint agent port
EndPoint agent control server connection port 10500

2. Recommended ports

- TCP (standard ports for normal local network activity):

135

139

445

5985

- UDP (if necessary): 137
- Operating system standard ports :

FTP 21

SSH 22

Telnet 23

SMTP 25

WHOIS client application port 43

Hostname conversion system 53

HTTP 80

POP 110

SSL/TLS POP 995

IMAP 143

Secure IMAP connection 993

SSL HTTP 443

MySQL Server 3306

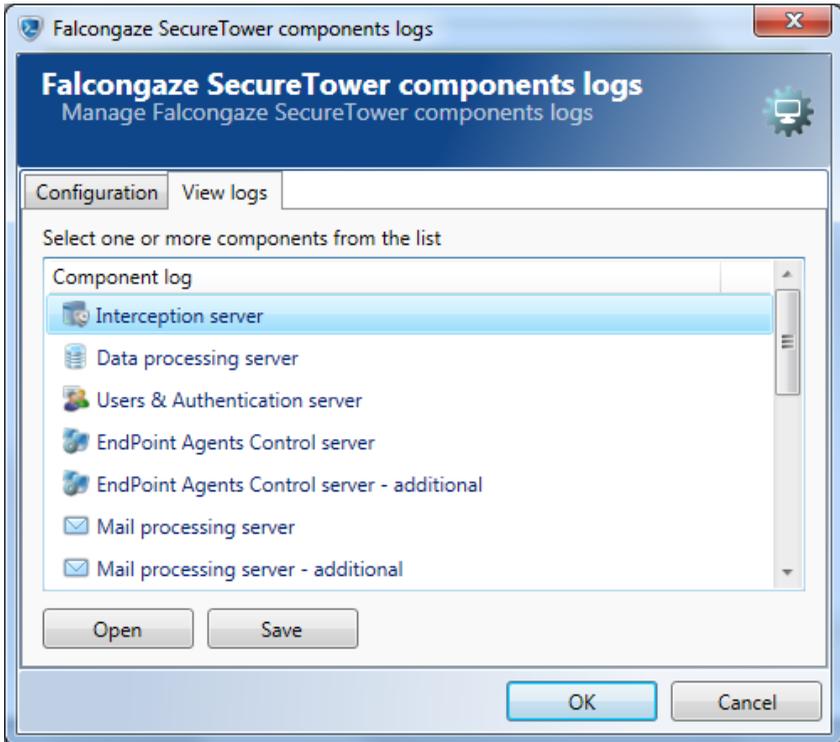
Network Printing Protocols 631

Virtual Network Computing (VNC) 5900

Note: UDP 5000 and above must be opened on the workstation with **SecureTower Client Console** installed to provide audiomonitoring function.

3.3 Configuring log of system events

SecureTower events are logged automatically, herewith all components logs are accessible for viewing from the console directly. To manage and view logs on the **Tools** menu click **System log options**.



Viewing and exporting system logs

In the **Falcongaze SecureTower components logs** window, click the **View logs** tab.

To view logs, select one or more in the list (to select multiple fields hold down Ctrl or Shift on your keyboard and click the fields' titles) and click **Open**. The selected logs will be opened in the default text file viewer application (for example, Notepad).

In case you need to save one or several logs (for example, for subsequent submission to the **Falcongaze** technical support service), click the logs you wish to save and click **Save**. Specify a name for the file and a folder to save it into. Logs will be packed into a ZIP archive.

Extended logging

In the **FalconGaze SecureTower components logs** window click the **Configuration** tab.

In some cases you may need to enable extended logging of **SecureTower** server components to diagnose and solve certain issues. To activate extended logging, click the corresponding option. Please note that extended logging significantly increases the size of system logs, therefore it is not recommended to use this option on a regular basis – enable it temporarily as needed.

To enable extended logging:

1. Make sure you are logged in as user with rights to configure all the system servers (for more information about access permissions, see [Creating a user group](#)).
2. Select the relevant check box.
3. To activate extended logging, the system needs to restart all server components. Click **Yes** in the confirmation dialog window.
4. Wait until the servers restart.
5. To continue and reconnect to the server, click **Yes**.

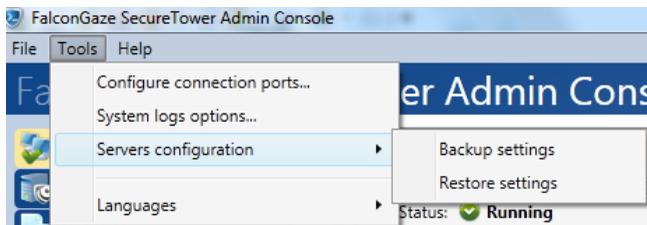
Note: *If it is impossible to restart them automatically, a corresponding notification will appear. In this case you will need to restart all services manually for every component (for more information, see [Starting and stopping services](#)).*

3.4 Managing system configuration

System configuration data can be backed up and restored by user.

Configuration data for the system provides information about operating mode of the system and the servers components that are defined in it. It is recommended to back up the system data regularly.

To operate with the configuration data of the system on the **Tools** menu, point to **Server configuration** and use the corresponding command.

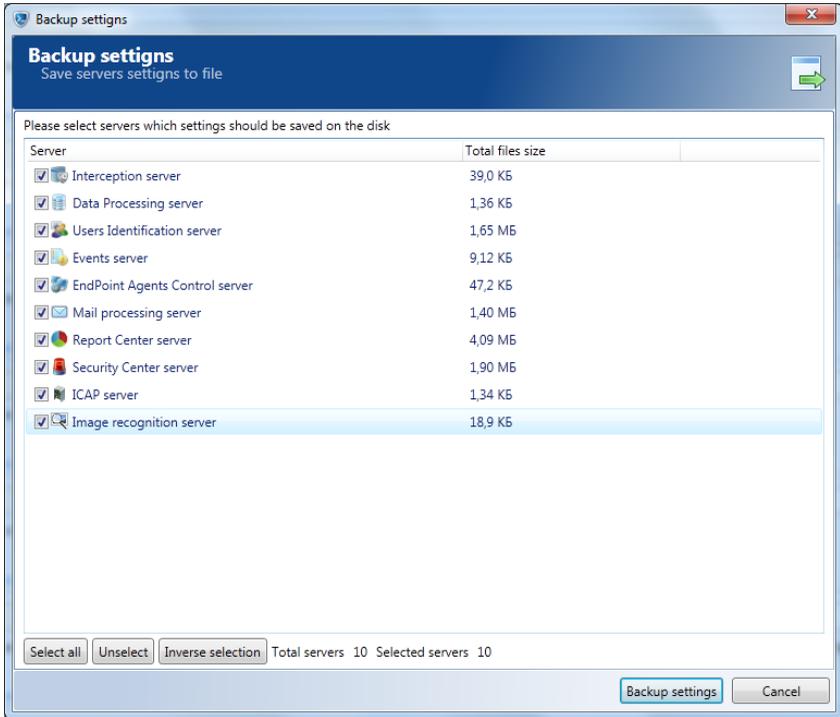


Backing up the system configuration

System configuration can be saved to a backup configuration *.zip file and can be used later for restoring in the cases of system failure or etc.

To save your system configuration data:

1. On the **Tools** menu, point to **Server configuration** and click **Backup settings**.



2. To select the server which configuration data must be saved, click the related check box in the **Backup settings** window.
3. Click **Backup settings** to proceed.
4. Specify the network path and the name of the configuration file and click **Save**.

One can also use the selection buttons below the list:

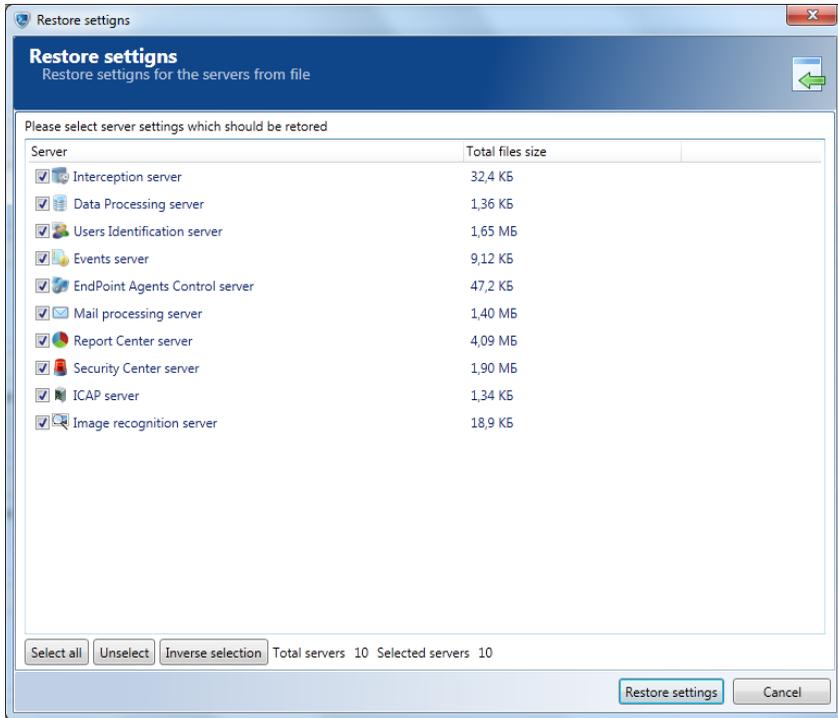
- Click **Select all** to select all servers check boxes from the list.
- Click **Unselect** to cancel selection that was made before.
- Click **Inverse selection** to clear check boxes and select all unselected items in the list simultaneously.

Restoring the system configuration

To restore the configuration data of the system servers:

1. On the **Tools** menu, point to **Server configuration** and click **Restore settings**.

2. In the newly opened window, select a configuration *.zip file and click **Open**.



3. To select the server which configuration data must be restored, click the related check box in the **Restore settings** window.

4. Click **Restore settings** to proceed.

5. In the confirmation window click **OK**.

One can also use the selection buttons below the list:

- Click **Select all** to select all servers from the list.
- Click **Unselect** to cancel selection that was made before.
- Click **Inverse selection** to clear check boxes and to select all unselected items in the list simultaneously.

4 Configuring Licence Server

To view licence information for your application copy, click the **Licence Information** tab on the left sidebar of the program's main window.

4.1 Viewing licence information

The common data for currently valid **SecureTower** licence, licensed modules data, intercepted protocols, controlled workplaces and mail accounts are displayed and available for configuring in the **Licence information** window.

General information

General information includes the name of the server with connected USB-dongle as well as the approximate date of the product's first startup and currently used version build date. The **Available installed licence** section contains USB-dongle data. In case of single USB-dongle is connected the data is displayed in the right part of the **Licence information** section.

If any new **SecureTower** server components was added or any changes in other licensed parameters were made, the system supplier will send new licence settings that must be added to the currently used USB-dongle. To update the licence click the **Update licence** link (for more information, see [Updating licence information](#)).

Internal emails restrictions

In the **Internal emails restrictions** section, the list of e-mails domains and addresses can be configured for internal licence count. Click **Internal emails** to specify restrictions.

Internal emails restrictions:

Internal emails licence options allow to specify mail domains or email addresses to divide intercepted messages on internal and external mails

[Internal emails](#)

Modules restrictions

In the **Modules restrictions** section, the list of licensed application components is displayed with the following information indicated:

Quantity	For example, 1/5, in which the first digit stands for the number of installed and working modules, and the second digit –for the maximum permitted number of component copies in accordance with the licence token
Currently working servers	IP addresses/names of servers on which modules are installed

Modules restrictions:

Module name	Quantity	Locations
 Data processing server	1 from 1	127.0.0.1
 Interception server	0 from 1	
 EndPoint Agents Control server	0 from 1	

Protocols restrictions

In the **Protocols restrictions** section the list of protocols is displayed that are currently controlled by the system. If the licence does not include interception of specific groups of protocols, the corresponding option will be inactive.

Protocols restrictions:

<input checked="" type="checkbox"/>	 Mail
<input checked="" type="checkbox"/>	 Messengers
<input checked="" type="checkbox"/>	 Web
<input checked="" type="checkbox"/>	 Files

Controlled workplaces restrictions

In the **Controlled workplaces restrictions** section the number of IP addresses or workstations, network activities of which are currently monitored and controlled by the application (the first number), and the maximum permitted number of IP addresses in accordance with the terms of the licence token (the second number) are displayed.

Below you can see the list of IP addresses currently monitored by the system. The list is reset and updated every 24 hours.

Controlled workplaces restrictions: 3/26

IP address	Computer name	Quantity	Users
192.168.1.30	FG01	1	John Smith
192.168.1.31	FG02	1	Adam White
192.168.1.32	FG03	1	William Grey

Controlled mail processing server mail accounts restriction

In the **Controlled mail processing server internal mail accounts restriction** section the number of internal mail accounts, network activities of which are currently monitored and controlled by the application (the first number), and the maximum permitted number of internal mail licences in accordance with the terms of the licence token (the second number) are displayed.

In the **Controlled mail processing server external mail accounts restriction** section the number of external mail accounts, network activities of which are currently monitored and controlled by the application (the first number), and the maximum permitted number of external mail licences in accordance with the terms of the licence token (the second number) are displayed.

Note: *Mail licence is allocated for a mail sender account. Mail licences dividing on internal and external is performed in accordance with type of sender account (sender account may belong to internal or external mail domain).*

To configure the list of mail licences click the **Mail Processing** tab and configure the mail processing strategy (set the list of mail accounts for interception) as described in the [Miscellaneous mail processing settings](#) chapter.

4.2 Setting up connection to the license server

The system includes six licensed server components: Data Processing Server, Interception Server, Endpoint Agent Control Server, ICAP server, Image Recognition Server and Mail Processing Server. All these components receive licensing information from the Licence Server, which, in turn, reads it from a USB dongle connected to computer where the server is installed.

In case all system components are installed on the same physical server, you do not need to configure anything manually, as all components will use their default settings to connect to the License Server.

In case the system components are installed on different computers, you have to set up their connection to the Licence Server manually. The following parameters should be set:

- Licence Server address. The name of the machine where Licence Server is installed. Therefore, in case of manual setup, the Licence Server address is the name of the computer with connected USB-dongle.
- Licence Server port number for connection establishment. Port number should be equal to the one specified upon connection between components configuring (for more information, see [Setting up connection ports for services](#)). By default the port number is 20044.
- If there are more than one dongle connected to the Licence Server computer, and the license should be requested from the particular one - the dongle serial number and the licence number separated by dot must be specified. If there are more than one dongle connected to the Licence Server computer, but the serial number wasn't specified manually - **SecureTower** use the first initialized dongle to use licence information.

Licence server information



Licence server connection parameters:

Server address: localhost

Server port: 20044

Serial key: (default key)

Note: After you have configured connection of all components to License Server, do not forget to **Apply changes** in the right lower part of the main window.

Connection between Interception Server and Licence Server

1. To connect Interception Server to Licence Server, click the **Data Interception** tab in the left sidebar of the program's main window.
1. In the **Licence server information** section of the **General** tab, set parameters to connect the Interception Server to the Licence Server by specifying the Licence Server's address and port.
2. If there are more than one dongle connected to the Licence Server computer, specify the number of the particular dongle to use its licence information.

Connection between Endpoint Agent Control Server and Licence Server

1. To connect Endpoint Agent Control Server to Licence Server, click the **EndPoint Agents** tab in the left sidebar of the program's main window.
2. Click the **Endpoint agents options** tab and scroll down to the **Licence server information** section. Specify Licence Server's address and port.
3. If there are more than one dongle connected to License Server computer, specify the number of the particular dongle to use its licence information.

Connection between Mail Processing Server and Licence Server

1. To connect Mail Processing Server to Licence Server, click the **Mail Processing** tab on the left sidebar of the program's main window.
2. In the **License server information** section specify Licence Server's address and port.
3. If there are more than one dongle connected to Licence Server computer, specify the number of the particular dongle to use its licence information.

Connection between ICAP Server and Licence Server

1. To connect ICAP Server to Licence Server, click the **ICAP server** tab on the left sidebar of the program's main window.
2. Specify Licence Server's address and port.
3. If there are more than one dongle connected to Licence Server computer, specify the number of the particular dongle to use its licence information.

Connection between Recognition Server and Licence Server

1. To connect Recognition Server to Licence Server, click the **Image Recognition** tab on the left sidebar of the program's main window.
2. Scroll down to the **Licence server information** section. Specify Licence Server's address and port.
3. If there are more than one dongle connected to Licence Server computer, specify the number of the particular dongle to use its licence information.

4.3 Updating licence information

When you purchase additional server components of **SecureTower** or change the number of workstations to be monitored, you receive new licence information from the manufacturer and need to update it in your licence token.

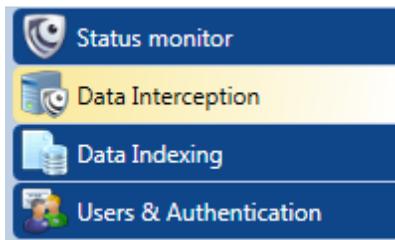
1. Click **Update licence** link under the licence key number in the right part of the **Licence information** window.

Note: *If a number of licence keys are used, select the appropriate licence number in the list of **Available installed licences**. Click **Update licence** link. In case of multilicence key is used, click **Update licences on key** to update all licences simultaneously or select the particular licence and click the corresponding link. If there are no the licence key you need to update, make sure the USB dongle is connected to the computer with installed Licence Server.*

2. Click the button  in the **Update licence** window, and in the dialogue window, select the file with the new licence information that Falcongaze sent to you. Please note that the file should have the **.licx** extension.
3. Click **Open**. The licence information will be updated, and you may verify the licence terms and conditions in the section below.
4. Make sure the new licence information corresponds to purchased parameters.
5. If any controversies are occurred contact Falcongaze technical support (direct link is available from the **Help** menu).

5 Setting up Interception Server

To configure Data Interception server, click the **Data Interception** tab on the left sidebar of the program's main window.



In the **Traffic interception server options** window, one can configure interception settings, enable IP filtering and MAC filtering rules and set up necessary network adapters. Also the statistics of server operation is available.

Note: *Configuring server parameters is available only if the computer where this service is installed is switched on. In that, the interception server can be disabled.*

After the necessary interception server parameters are entered, the program will request restarting the service. Click **Yes** in the respective dialogue box. To cancel the changes, click **No**.

Note: *To avoid traffic losses, the interception server should be restarted as rarely as possible. Therefore, it is recommended to restart it only when all the necessary changes were made to the interception settings.*

5.1 Interception of tagged VLAN traffic

SecureTower enables interception of tagged VLAN (Virtual Local Area Network) traffic according to IEEE 802.1Q standard. This function can be useful in huge networks with complex topology using VLANs. However, processing this traffic is more resource-intensive as compared to regular traffic.

The problem with VLAN traffic interception lies in the absence of built-in support mechanisms for VLAN in Windows. As a result, many network adapters are unable to forward this type of traffic to **SecureTower**. There exists two ways of solving this problem – stripping VLAN packets of tags on the driver level with subsequent packet forwarding to **SecureTower**, or configuring the network adapter so that it would pass tagged VLAN packets to the system for processing, the latter variant being more resource-intensive.

Thus, in case of problems with interception of VLAN traffic, you can use one of the two variants: installation of specialized driver for your network adapter or reconfiguring the device using special flags.

5.1.1 Using specialized drivers

Hardware manufacturers, like Intel, Broadcom, 3Com and SysConnect provide specialized drivers which add support for VLANs and thus facilitate passing the traffic to **SecureTower**.

Intel Advanced Networking Suite (iANS)

Intel has a virtual mini port driver that splits VLAN enabled interfaces to virtual interfaces. It is possible to capture from these interfaces without any known problems.

Broadcom Advanced Server Program (BASP)

For servers, Broadcom has a virtual mini port driver, the Broadcom Advanced Server Program (BASP), which splits VLAN enabled interfaces to virtual interfaces. It is possible to capture from these interfaces without any known problems.

5.1.2 Special flag settings

For some of the more sophisticated adapters, a flag can be set in Windows registry to disable stripping of VLAN tags.

Intel

Some Intel Ethernet adapters and their drivers will, by default, strip VLAN tags when processing packets or strip tagged packets completely. In order to enable **SecureTower** to process VLAN tags on Windows, you will need to disable this feature. You may also need to upgrade your driver for that. This is unrelated to working with Intel's specialized driver that adds VLAN support.

Abstract from Intel's original support note <http://www.intel.com/support/network/sb/CS-005897.htm>

To allow tagged frames to be passed to the packet capture software you must go into the registry and either add a registry DWORD and value or change the value of the registry key. Depending on the bus type of your network adapter you will either create the keyword "MonitorModeEnabled" for PCI/PCI-X Network Adapters, or "MonitorMode" for PCI-e based Network Adapters.

The new key (DWORD) should be placed at:

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class  
\{4D36E972-E325-11CE-BFC1-08002BE10318}\00xx
```

where **xx** is the instance of the network adapter that you need to see tags on. (Check by opening and viewing the name of the adapter).

Note: *ControlSet001 may need to be CurrentControlSet or another 00x number. In this case the rest of the address will remain the same.*

If you are using a PCI or PCI-X Network Adapter the registry dword is:

MonitorModeEnabled

Set the DWORD value to either:

- 0 - disabled (do not store bad packets, do not store CRCs, strip 802.1Q VLAN tags);
- 1 - enabled (store bad packets, store CRCs, do not strip 802.1Q VLAN tags).

If you are using a PCI-Express Network Adapter the registry DWORD is:

MonitorMode

Set the DWORD value to either:

- 0 - disabled (do not store bad packets, do not store CRCs, strip 802.1Q VLAN tags)
- 1 - enabled (store bad packets, store CRCs, do not strip 802.1Q VLAN tags)
- 2 - enabled strip VLAN (store bad packets, store CRCs, strip 802.1Q VLAN tags)

In most cases you should set **MonitorMode=1** or **MonitorModeEnabled=1**.

Note: *This modification should be made very carefully and only by skilled technicians since changes to the registry may disable your machine. This change should only be made for promiscuous mode/sniffing use.*

Broadcom

BASP driver is not supported on laptops, but, at least for the BCM5751M NetXtreme Gigabit chips in IBM T43 and HP laptops, there is a registry key under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet` that can be set to cause the driver and chip not to strip the 802.1Q headers. In order to set that key, you need to find the right instance of the driver in Registry Editor and set that key for it. You can do this the following way:

1. Run the Registry Editor (regedt32);
2. Search for "**TxCoalescingTicks**" and ensure this is the only instance that you have;
3. Right-click on the instance number (eg. 0008) and add a new string value;
4. Type "**PreserveVlanInfoInRxPacket**" and give it the value "1".
5. This should set you up to be able to intercept the VLAN tag information.
6. If VLAN traffic is still not intercepted, you need to update the firmware of your Broadcom network controller:
7. Fetch the user diagnostic application from Broadcom website;
8. Burn a CD using the downloaded ISO image;
9. Boot to Live CD;

10. Select install to hard drive;
11. Change to the **b57udiag** directory and run "**b57udaig-cmd**";
12. At the prompt type "**setasf-d @**".

Marvell Yukon 88E8055

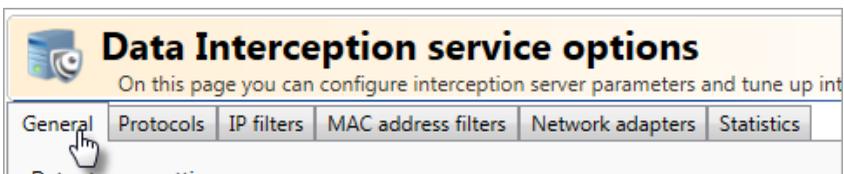
In case you have a Marvell Yukon Ethernet controller, you can disable stripping VLAN tags by adding a DWORD parameter **SkDisableVlanStrip** with a value of **1** under the registry key: "HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\000", where **000** is the number of the folder for the Marvel Ethernet controller.

Other network adapters

In case you have other network adapters, contact the manufacturer's support team to obtain detailed instructions on disabling VLAN tag stripping.

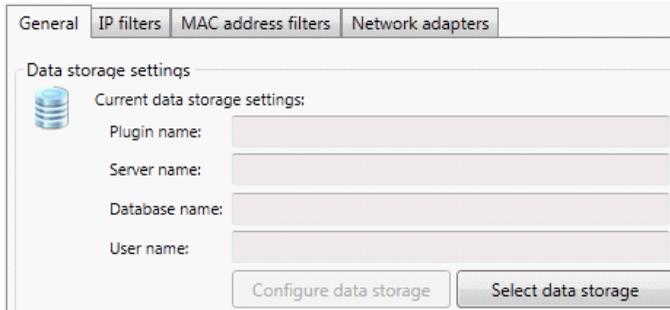
5.2 Configuring general parameters

To configure general settings of centralized interception such as database connection, rules of sessions and packets processing and licence, click the **General** tab of the Data interception service window.



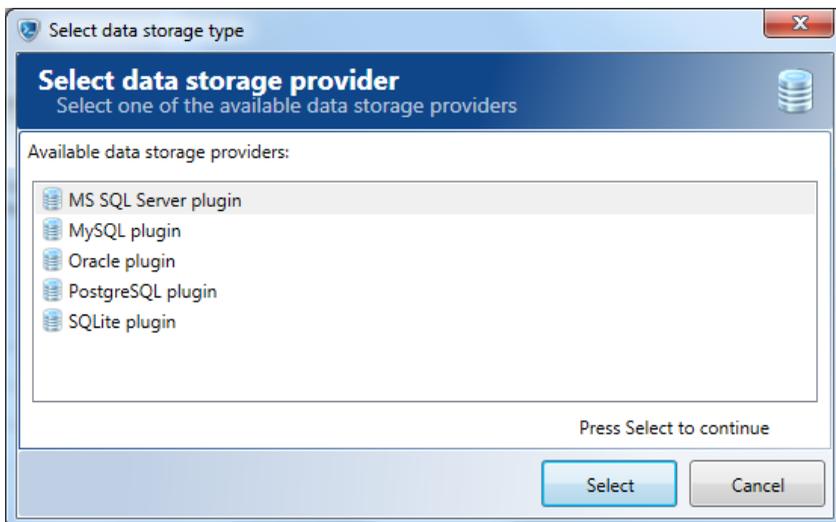
5.2.1 Selecting data storage type

To configure the database where the information retrieved from network traffic will be stored, click the **General** tab of the Data interception service window, navigate to the **Data storage settings** section, and click **Select data storage**.



The screenshot shows a software interface with a tabbed menu at the top containing 'General', 'IP filters', 'MAC address filters', and 'Network adapters'. The 'General' tab is active. Below the tabs is a section titled 'Data storage settings' with a database icon on the left. To the right of the icon, the text 'Current data storage settings:' is followed by four stacked text input fields labeled 'Plugin name:', 'Server name:', 'Database name:', and 'User name:'. At the bottom of this section are two buttons: 'Configure data storage' and 'Select data storage'.

In the **Select data storage type** dialogue box, the user is suggested selecting the necessary database management system from the list of the supported systems. Currently, the program supports working with **MS SQL Server**, **MySQL**, **Oracle** and **Postgre SQL**. The distribution package of the product also includes an embeddable database library – **SQLite** – that can be used for testing purposes or in a small network upon low network loads.



To select a database management system

1. Click the desired type of system in the list of available DBMS's and click **Select**. After selecting the DBSM, one should connect to the server on which the required database is installed. The database connection configuration window will open automatically.
2. For detailed information on DBMS connection settings refer to sections [Setting up a connection to an MS SQL Server database](#), [Setting up a connection to an Oracle database](#), [Setting up a connection to a PostgreSQL database](#), [Setting up a connection to an SQLite database](#), [Setting up a connection to a MySQL database](#) of this Guide.

5.2.1.1 Setting up a connection to a MS SQL Server database

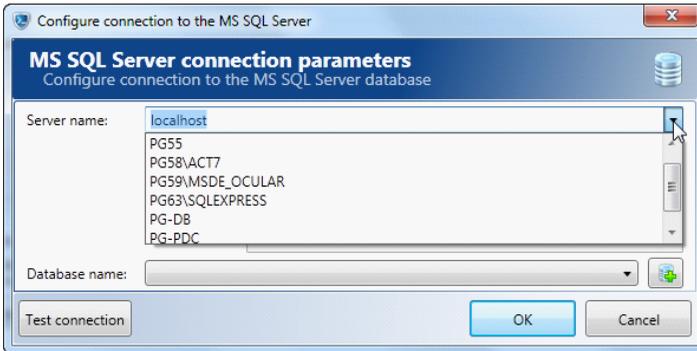
1. In case you selected MS SQL Server plugin, a window will open in which you need to specify the name of the server on which the configured database is installed or select it in the drop-down menu opened by clicking the arrow icon in the right corner of the text box.



2. If Windows authentication system is used to access the database, select the respective option (**Use windows authentication**).
To access the database with the SQL Server authentication system, select the **Use SQL Server authentication** option. Specify user name and password for database access in the respective fields and proceed with [paragraph 8](#).
3. To use **Windows authentication** you need first to configure startup parameters for **Interception server** and **Data processing server**. To do this, close the SQL Server configuration window by clicking **Cancel**.
4. Click the **Status monitor** tab on the left sidebar of the main application window, configure startup parameters for **Interception server** and **Data processing server** (for more information, see [Selecting interception server startup account](#)).
5. Specify the same parameters as for **Interception server** and click **OK**.
6. Reopen the [Configure connection to MS SQL Server](#) window. To do this, select **Data interception** in the left sidebar of the program's main window, click **Select data storage** in the **General** tab. In the newly opened window select **MS SQL Server plugin** and click **Select**.
7. Select the option **Use Windows authentication**.

Attention: In case of connection of any other **SecureTower** server to MS SQL Server database in Windows authentication mode it is necessary to make sure that this server startup account has access rights to MS SQL Server. Otherwise specify startup account with access rights to the database in the Service startup parameters window available from this server tab (for more information, see [Service startup parameters](#)).

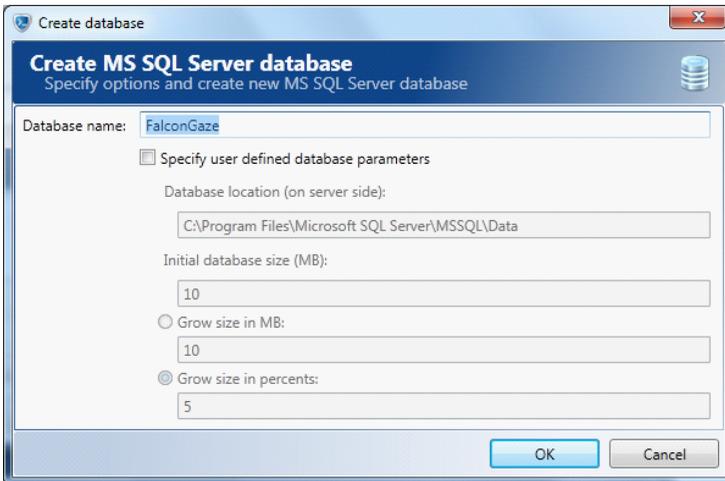
- Specify the name of the server your database is stored on. The database can be stored on the local computer (**localhost**) or on any other computer you can see in the drop-down menu after clicking on the downward arrow in the right end of the **Server name** entry field.



- In case you already have an **MS SQL Server** database for intercepted information, select its name in the drop-down menu **Database name**, click **OK** and proceed with [paragraph 18](#).

In case you need to create a new database, click the "Add" button  next to the **Database name** field.

- In the opened window enter the name of the new database in the **Database name** text field.



11. If you need to specify user-defined parameters for the database, select the relevant check box. If the check box is clear, the default parameters will be applied to the new MSSQL Server database.

Specify user defined database parameters

Database location (on server side):

Initial database size (MB):

Grow size in MB:

Grow size in percents:

12. Type the path to the newly created database in the **Database location (on server side)** text field. You have to specify the path on the server you have selected previously ([paragraph 8](#)).
13. Type the minimum value of the disk space (in Megabytes) that will be used by the empty database in the **Initial database size (MB)** text field.
14. In the **Grow size in MB** text field you need to type the value of the disk space (in Megabytes) the database will be enlarged by whenever a traffic volume exceeding the initial size of the database is stored in it. As an alternative, you can specify the grow size in percentages (see paragraph below).
15. In the text field **Grow size in percents** you need to specify the percentage of the initial database size, the database will be enlarged by whenever a traffic volume exceeding the **current** database size is stored in it. *For detailed information on the configuration of the newly created database refer to the Section **Database creation** of the MS SQL Server documentation.*
16. Click **OK** to create the database.
17. Select the name of your newly created database in the drop-down menu **Database name** of the [MS SQL Server database configuration](#) window. If you cannot see the name of the database, it means that the specified authentication parameters are incorrect.
18. After all the parameters for the connection to the MS SQL Server database are specified, you can check the connection by clicking **Test connection**. In case there is a server connection error, make sure that the selected database is installed on the specified server and the authentication parameters are correct.
19. In case of successful connection to the database, click **OK** to save your settings. To cancel the settings click **Cancel**. The settings will appear in the **Current data storage settings** on the main application window.

Current data storage settings:

Plugin name:	MS SQL Server plugin
Server name:	pg-db
Database name:	FalconGaze
User name:	sa

20. To enable all entered settings click **Apply changes**, located in the lower right corner of the main application window.

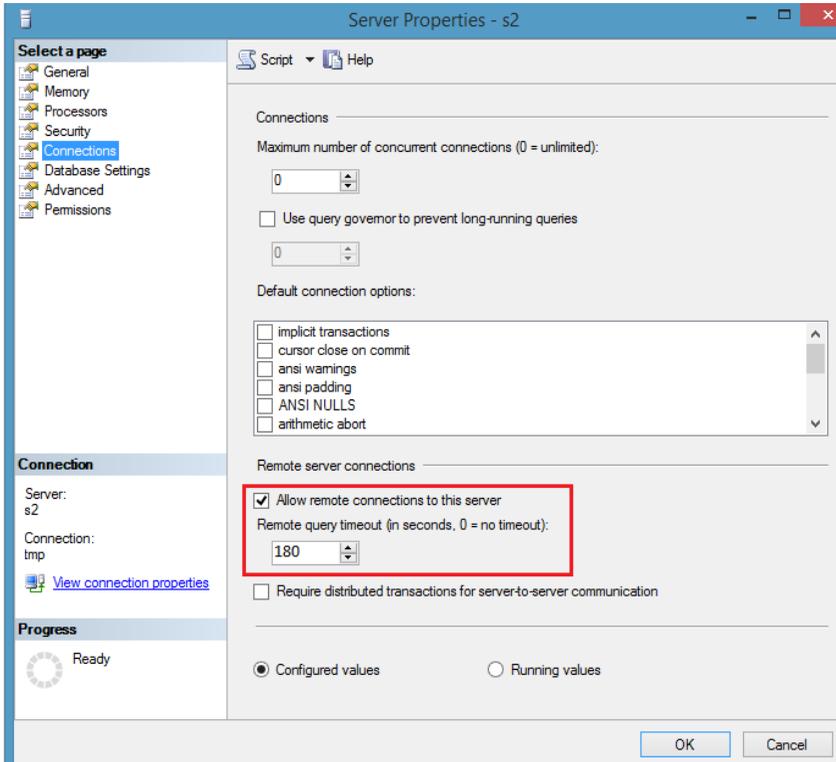
Implementations notes

1. If using **MS SQL Server** is necessary to keep in mind that the size of files saved to **MS SQL Server database** sometimes is limited to 1GB (due to **MS SQL Server** restrictions). Therefore, all system data size restrictions should be in compliance. Otherwise, saving of files with the size more than 1GB will be interrupted and files will not be placed in a database.
2. The query timeout for server-to-server communication established with **MS SQL Server** is restricted to 30 sec by default, hence if more than 30 sec is requested for transaction, the communication between **MS SQL Server** and **SecureTower Server** will be interrupted

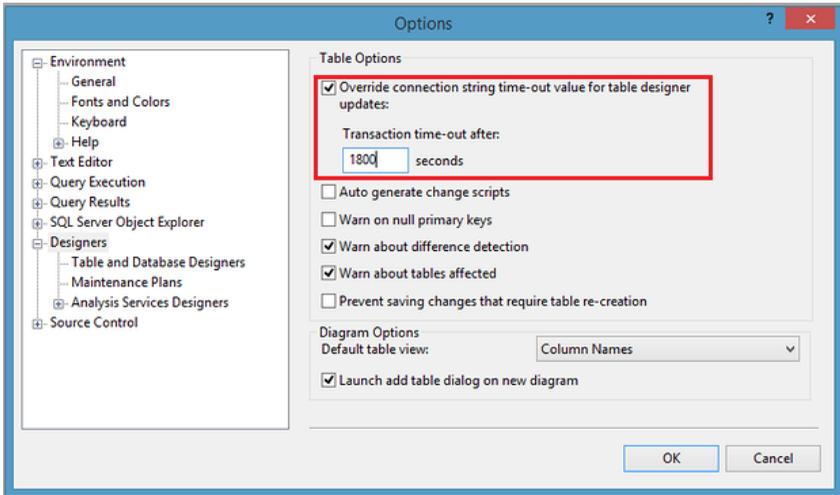
by the database server and the transaction will not be performed. The corresponding alert will be generated in the system event log.

To increase the query timeout modify the default configuration of the **MS SQL Server** with Microsoft SQL Server Management Studio:

- **Specify the query type that is enough for transaction.** Use the *Server Properties* option from the server context menu. Select the *Allow remote connections to the server* option from the *Remote server connections* section in the *Server Properties* window and enter the appropriate time limit.

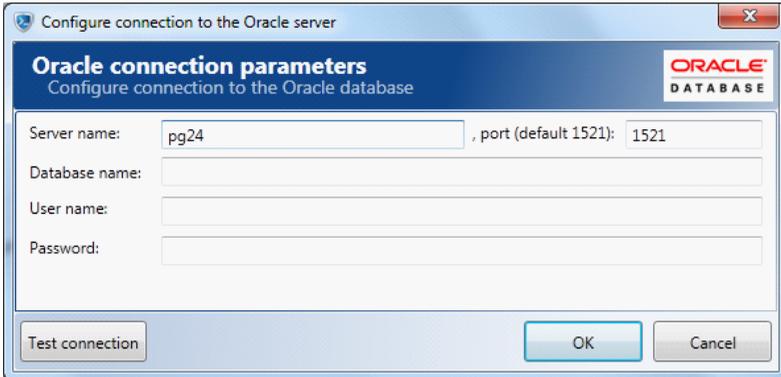


- **Sure that the timeout of transaction specified for DBMS in compliance with specified previously one for sever.** On the *Tools* menu of Microsoft SQL Server Management Studio, click *Options*. In the newly opened window select *Designers* from the objects tree. Enter the timeout equal or bigger than was specified on the previous step in the *Transaction time-out after:* field or disabled the *Override connection string time-out value for table designer updates option*.



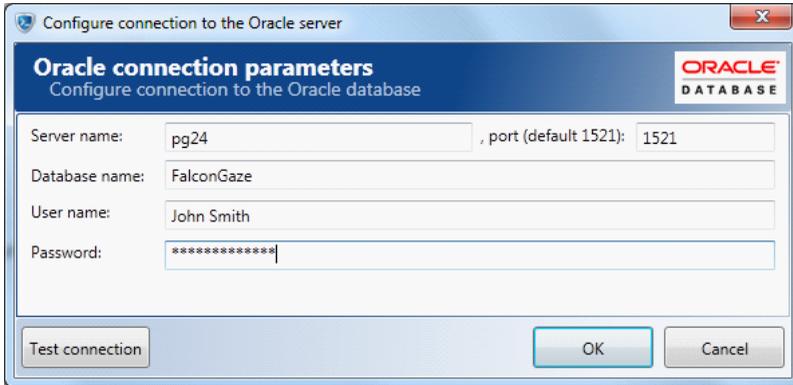
5.2.1.2 Setting up a connection to a Oracle database

1. If you selected **Oracle plugin**, a window will open suggesting the user to enter the server, on which the database is or will be stored. The database can be located on the local computer (**localhost**) or on any other computer entered in the **Server name** text field. Enter the number of the port which will be used to connect to the database.

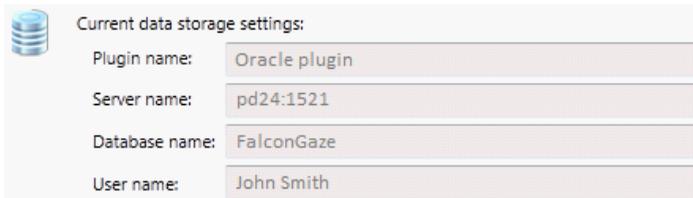


2. In the **Database name** text field, enter the name of the database used to store the intercepted traffic. If such database does not exist, you first have to create it on the local computer or on other computer in the network (specified in the **Server name** field). After a new database is created, reopen the Oracle connection parameters windows to proceed with its configuration.

3. Specify the authentication parameters for the database by entering the user name and the password used to access the database in the corresponding text fields.



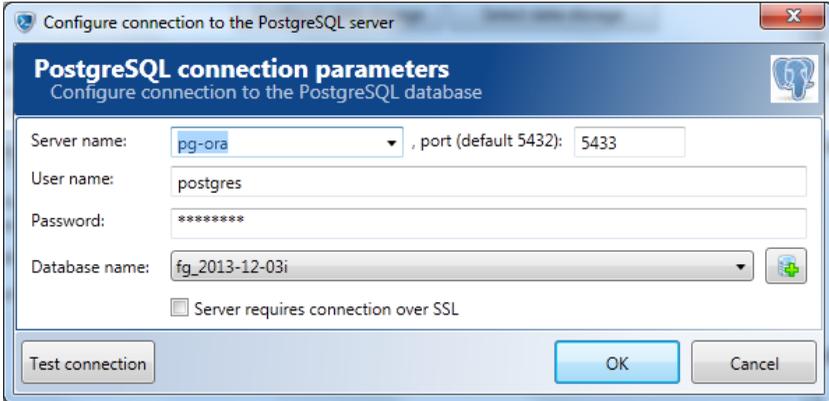
4. After all necessary settings are configured, you can test the connection to the database by clicking **Test connection**. In case there is a server connection error, make sure the selected database is installed on the specified server and the authentication parameters are correct.
5. In case of successful connection to the database, click **OK** to save your settings. To cancel the settings click **Cancel**. The current settings will be displayed as **Current data storage settings** in the main application window.



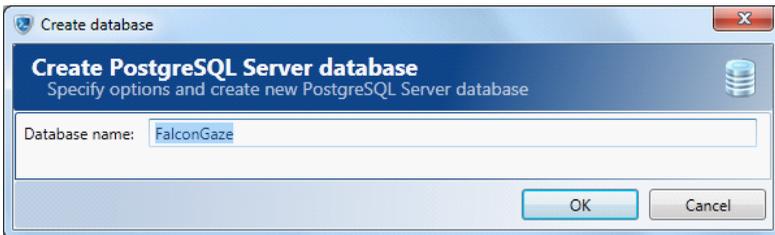
6. To apply the configured settings, click **Apply changes**.

5.2.1.3 Setting up a connection to a Postgre SQL database

1. If you selected **Postgre SQL plugin**, a window will open suggesting the user to select the server, on which the database is or will be stored. The database can be located on the local computer (**localhost**) or on any other computer entered in the **Server name** text field. Enter the number of the port which will be used to connect to the database.



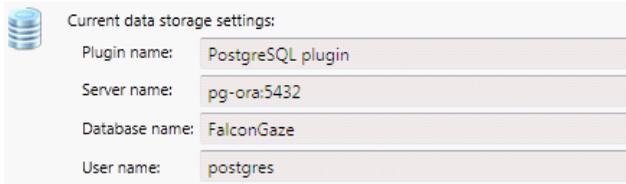
2. If you already have a Postgre SQL database to store the intercepted traffic, proceed with [paragraph 4](#). Otherwise, you can create a database on the specified server right from Administrator Console. To do this, specify the authentication parameters of the user having the necessary rights in the DBMS to create new databases by entering such user's name and password in the corresponding text fields and click the **Add** button , located to the right of the **Database name** drop-down menu.
3. Enter the name for a new Postgre SQL database in the text field **Database name** and click **OK**.



4. Specify the authentication parameters for the database by entering the user name and the password in the corresponding text fields.
5. Click on the drop-down menu **Database name** and select the name of the database used for storage of the intercepted traffic. If the authentication parameters are correct, the list will contain all databases that can be accessed using these parameters.
6. To establish SSL-connection, select the check box of corresponding option.
7. After all necessary settings are configured, you can test the connection to the database by clicking **Test connection**. In case there is a server connection error, make sure the

selected database is installed on the specified server and the authentication parameters are correct.

8. In case of successful connection to the database, click **OK** to save your settings. To cancel the settings click **Cancel**. The current settings will be displayed as **Current data storage settings** in the main application window.



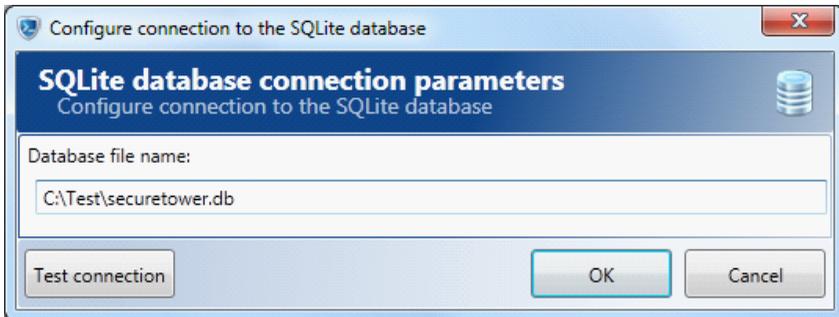
The screenshot shows a dialog box titled "Current data storage settings:" with a database icon on the left. It contains four input fields:

- Plugin name: PostgreSQL plugin
- Server name: pg-ora:5432
- Database name: FalconGaze
- User name: postgres

9. To apply the configured settings, click **Apply changes** located in the right lower corner of the main application window.

5.2.1.4 Setting up a connection to a SQLite database

1. In case you selected **SQLite plugin**, create an SQLite database by specifying a full path to the directory where the database will be stored, and a file name with a **".db"** extension.



The screenshot shows a dialog box titled "Configure connection to the SQLite database" with a close button (X) in the top right corner. The main area has a blue header with the text "SQLite database connection parameters" and "Configure connection to the SQLite database" next to a database icon. Below the header is a text input field labeled "Database file name:" containing the path "C:\Test\securetower.db". At the bottom, there are three buttons: "Test connection", "OK", and "Cancel".

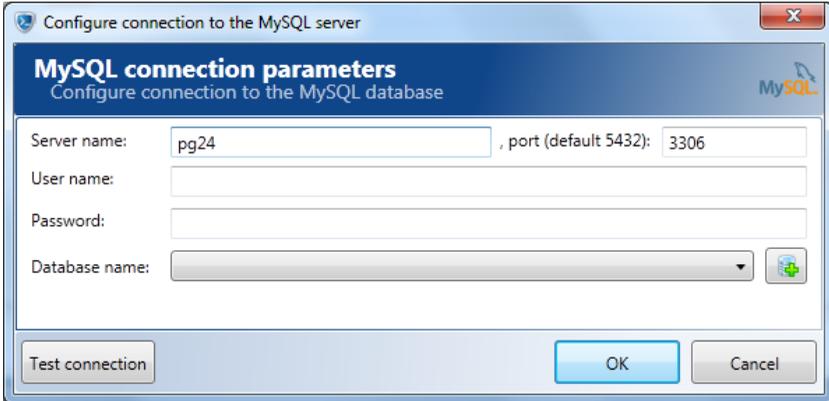
2. After the name of the database is entered, you can test the connection to the database by clicking **Test connection**. After you click **OK** a database with the specified name will be created in the corresponding folder.

Implementations notes

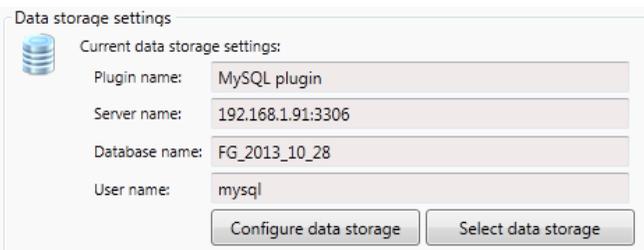
If using **SQLite** as the data storage is necessary to keep in mind that the size of files saved to it sometimes is limited to 1GB (due to database restrictions). Therefore, all system data size restrictions should be in compliance. Otherwise, saving of files with the size more than 1GB will be interrupted and files will not be placed in a database.

5.2.1.5 Setting up a connection to a MySQL database

1. If you selected **MySQL plugin**, a window will open suggesting the user to enter the server, on which the database is or will be stored. The database can be located on the local computer (**localhost**) or on any other computer entered in the **Server name** text field. Enter the number of the port which will be used to connect to the database.



2. Specify the authentication parameters for the database by entering the user name and the password used to access the database in the corresponding text fields.
3. In the **Database name** text field, enter the name of the database used to store the intercepted traffic. If such database does not exist, you first have to create it on the local computer or on other computer in the network (specified in the **Server name** field). After a new database is created, reopen the Oracle connection parameters windows to proceed with its configuration.
4. After all necessary settings are configured, you can test the connection to the database by clicking **Test connection**. In case there is a server connection error, make sure the selected database is installed on the specified server and the authentication parameters are correct.
5. In case of successful connection to the database, click **OK** to save your settings. To cancel the settings click **Cancel**. The current settings will be displayed as **Current data storage settings** in the main application window.
6. To apply the configured settings, click **Apply changes** located in the right lower corner of the main application window.



Implementations notes

If using **MS SQL Server**, **MySQL** or **Postgre SQL** as the data storage it is necessary to keep in mind that the size of files saved to it is limited to 1GB. Therefore, all system data size restrictions should be done in compliance. Otherwise, saving of files with the size more than 1GB will be interrupted and files will not be placed in a database.

If using MySQL as the data storage it is necessary to specify the following values: `max-allowed-packet = 1G` and `bulk_insert_buffer_size = 1G` for MySQL server settings. In this case a data packet with size more than 1GB (up to 4GB) will be implemented in several stage, herewith 1GB within 1 transaction will be transferred. Otherwise, the intercepted information will not be placed to the MySQL data storage.

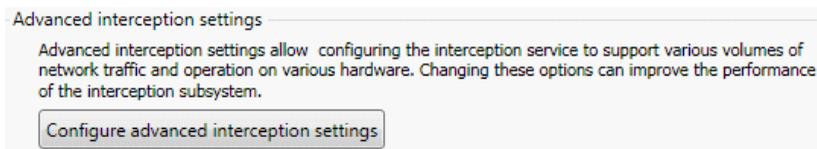
5.2.1.6 Changing current database settings

To connect to another database (within the current DBMS) or to change the settings of the current database, click **Configure data storage** in the [Data storage settings](#) section of the **Traffic Interception server options** window, the **General** tab.

Detailed instructions on configuring database connections are provided in sections [Setting up a connection to an MS SQL Server database](#), [Setting up a connection to an Oracle database](#), [Setting up a connection to a Postgre SQL database](#), [Setting up a connection to an SQLite database](#) of this Guide.

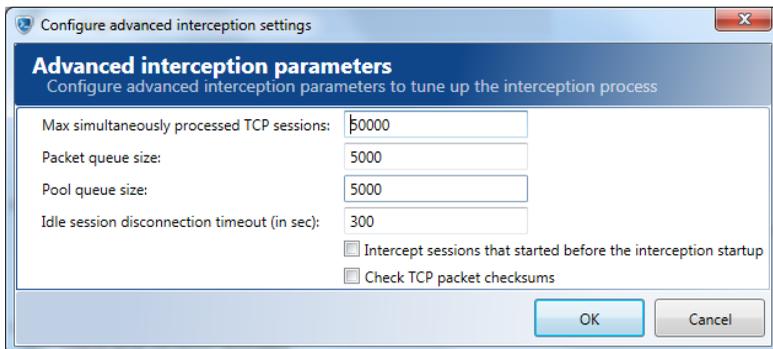
5.2.2 Advanced interception settings

The efficiency of the interception server can be regulated by varying advanced interception settings. To do this, go to the **Advanced interception settings** section in the **Data Interception service options** window, the **General** tab, and click **Configure advanced interception settings**.



Maximum simultaneously processed sessions

Maximum number of TCP sessions processed by the interception server in parallel can be set in the corresponding text box (Max simultaneously processed TCP sessions) of the Configure advanced interception settings dialogue box (see the figure below). Restriction of this parameter is necessary for reducing the interception server CPU load and disk space used. However, upon setting too low values some sessions are likely to be skipped if the number of started sessions exceeds the maximum number of simultaneously processed sessions. By default, the value for this parameter is set at 50000.



Packet queue size

The queue is used for buffering and synchronizing multithreaded traffic processing. Pending pool packets are the key element of the queue. The queue size is defined by the number of packets and should not be less than the size of the pool (see section *Packet pool size*). The default value for this parameter is 5000.

Packet pool size

This parameter determines the packet pool size for traffic transfer from the service to the traffic interception internal NDIS-driver. By changing the values of this parameter you can reach the desired ratio between the required efficiency of the application and the size of the disk space it uses. In that, the size of the packet pool should not exceed the size of the packet queue (see section *Packet queue size*). The default value for this parameter is 5000.

Session disconnection timeout

One can specify the wait time for some activity (for example, data transfer) over a TCP-connection that has been idle for some period of time. This can be done in the **Session disconnection timeout (in sec.)** text box. If the specified timeout period has elapsed and no data have been transferred over this TCP-connection, the session will be closed. This will help to free some space for the interception and processing of data transferred within other TCP-sessions. The default value for this parameter is 300.

Interception of sessions started before the interception startup

To ensure interception of sessions that started before the service was launched,

select the **Intercept sessions that started before the interception startup** check box. If this option is enabled, the service will be able to intercept the sessions that were started, but were not closed before the interception startup.

Note: *If the interception server is turned on after instant messaging starts, it is possible that the intercepted conversation parties' information will be incomplete. For example, for an ICQ chat, only the remote user's UIN would be intercepted. As for the local user, their IP address only will be known. After some time elapses, the local user's UIN can also be extracted from traffic, and in this case this conversation will be considered by the program as a conversation between/among other users, and, therefore, will be displayed in Client Console as a new conversation. Thus, it is possible that the same conversation will appear in several search results with "different" conversation parties mentioned.*

Checking TCP packet checksums

The **Check TCP packet checksums** option means that the interception system will check packet checksums (CRC) before their analysis. This option can be enabled in case the intercepted network adapter does not support CRC. If this option is enabled, the system will not accept for analysis the packets with checksums that do not match the CRC value calculated by the operating system because it indicates presence of a damaged packet.

If a network card supports CRC, it is recommendable to disable this option. Taking into consideration that packet checksums will not be calculated by the operating system and local packets are intercepted before they are transferred to the network adapter driver, the system may receive packets with an uncalculated checksum (its value will be "0") when intercepting a session from the local computer. Correspondingly, when checking the packet checksum, the system will identify such packets as damaged and will not process them.

Saving and applying changes

1. Click **Configure** to save the settings in the [DBMS selection](#) window.
1. Click **Cancel** to discard the settings.
2. To apply all the settings entered, click **Apply changes** in the bottom right corner of the program's main window.

5.2.3 License server information

In the license server information section it is essential to specify the parameters of access to **SecureTower** license server.

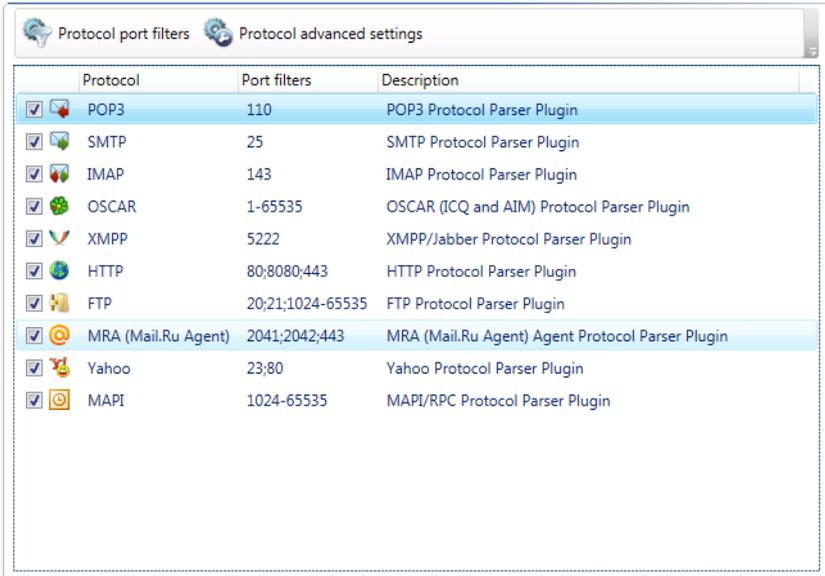
Specify the server address and port used to connect to it in the corresponding fields. Follow recommendations from [Setting up connection to the license server](#).

5.3 Setting up supported protocols for centralized traffic interception

To configure centralized interception of data transmitted over certain protocols, click the **Protocols** tab of the Data interception service window.

Note: To get access to protocols setup, one should connect to the server on which the interception server is installed.

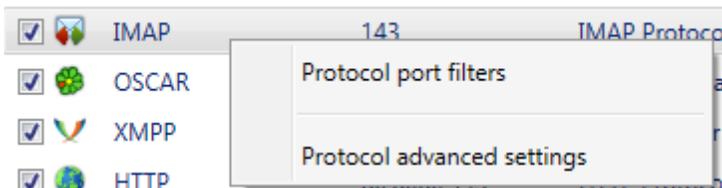
The list of available protocols (depending on the plug-ins installed) will be displayed in the protocol settings window. One can select the protocols the data of which should be intercepted.



Protocol	Port filters	Description
<input checked="" type="checkbox"/> POP3	110	POP3 Protocol Parser Plugin
<input checked="" type="checkbox"/> SMTP	25	SMTP Protocol Parser Plugin
<input checked="" type="checkbox"/> IMAP	143	IMAP Protocol Parser Plugin
<input checked="" type="checkbox"/> OSCAR	1-65535	OSCAR (ICQ and AIM) Protocol Parser Plugin
<input checked="" type="checkbox"/> XMPP	5222	XMPP/Jabber Protocol Parser Plugin
<input checked="" type="checkbox"/> HTTP	80;8080;443	HTTP Protocol Parser Plugin
<input checked="" type="checkbox"/> FTP	20;21;1024-65535	FTP Protocol Parser Plugin
<input checked="" type="checkbox"/> MRA (Mail.Ru Agent)	2041;2042;443	MRA (Mail.Ru Agent) Agent Protocol Parser Plugin
<input checked="" type="checkbox"/> Yahoo	23;80	Yahoo Protocol Parser Plugin
<input checked="" type="checkbox"/> MAPI	1024-65535	MAPI/RPC Protocol Parser Plugin

In the tab window, one can assign intercepted protocol ports and change protocol settings by clicking respective button.

These commands are also available in the protocol context menu opened by right-clicking the necessary protocol in the list of filters.



5.3.1 List of supported protocols and default ports

Protocol	Description	Ports*
POP3 (Post Office Protocol, version 3)	A mail protocol used by mail clients for receiving incoming e-mail messages from servers. Outgoing messages are sent over the SMTP protocol (see below). Checking POP3 in the list of protocols will enable system to intercept incoming e-mail messages received by mail clients.	110
SMTP (Simple Mail Transfer Protocol)	A mail protocol used by mail clients for sending outgoing e-mail messages from servers; works with POP3 in pair. Checking SMTP in the list of protocols will enable system to intercept outgoing e-mail messages sent by mail clients.	25
IMAP (Internet Message Access Protocol)	An e-mail access protocol. Analogically to POP3, it is used for incoming e-mail messages, but provides larger possibilities for working with a mail box. For example, access to processing incoming messages on the server as if they were on a local computer, without having to constantly resend files with the mail contents from and to the server. Outgoing messages are sent over the SMTP protocol (see above). Checking POP3 in the list of protocols will enable system to intercept incoming e-mail messages received by mail clients.	143
OSCAR	Instant and offline text messaging protocol used by ICQ, AIM, Miranda, QIP. Checking OSCAR in the list of protocols will enable system to intercept text messages transferred in the mentioned instant messengers.	1-65535
HTTP (HyperText Transfer Protocol)	A protocol for data transfer based on the client-server technology applied for receiving text information, in-stream video and audio from web-sites. Checking HTTP in the list of protocols will enable system to intercept all the data transferred via internet (visited URLs, portals, sent and received e-mail messages, posted messages).	80, 8080, 443

FTP (File Transfer Protocol)	A file transfer protocol used for transmitting commands, viewing files, file uploading to and downloading from a web-server. Checking FTP in the list of protocols will enable system to intercept all the files transferred via internet (uploaded or downloaded files, documents).	For data transfer – 20, for command transfer – 21 - 10
XMPP (Jabber)	An instant and offline messaging protocol used by Miranda, Google Talk, QIP Infium, PSI.	5222
Mail.Ru Agent	Instant messaging protocol	2041, 2042, 443
Yahoo IM	Instant messaging protocol	23;80
MAPI	A mail protocol used by client programs (Microsoft MAPI Controls, Microsoft Outlook)to communicate with different mail exchange systems.	1024-65535

** Note: The table provides default ports assigned for protocol. Programs may use other ports.*

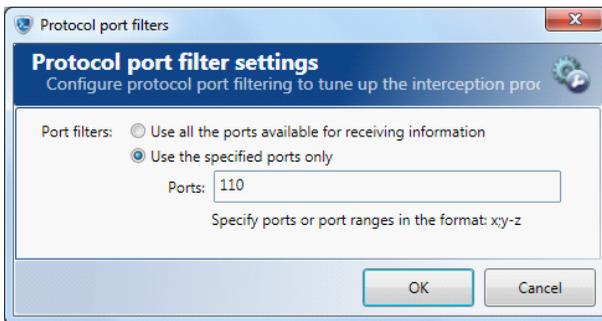
5.3.2 Assigning protocol ports for interception

By default, the program uses standard ports assigned for protocols (for more information, see [List of supported protocol and default ports](#) of this Guide). The provided values are, however, not stringent, and programs may use other ports.

1. To assign or change protocol ports to be intercepted, click the protocol which a new port should be assigned for in the protocols list.

	Protocol	Port filters	Description
<input checked="" type="checkbox"/>	POP3	110	POP3 Protocol Parser Plugin
<input checked="" type="checkbox"/>	SMTP	25	SMTP Protocol Parser Plugin

2. Click **Protocol port filters** in the toolbar. This command is also available in the context menu opened by right-clicking the protocol name.
3. In the appeared **Protocol port filters** window, one can select the **Use all the ports available for receiving information** option or the **Use the specified ports only** option. Please note that using all the ports for receiving information may reduce the performance of the system.



4. If intercepting data transferred over certain protocol ports is important, enter the values of the corresponding ports or port ranges in the **Ports** entry field in the suggested format: port values should contain whole numbers detached with a semicolon from one another; port ranges should contain hyphenated whole numbers.
5. To save the entered parameters, click **OK**. To apply all the entered settings, click **Apply changes** in the bottom right corner of the program's main window.

5.3.3 Configuring interception of protocols

Protocol setup is performed in the console by individual configuration of specific parameters for each protocol. To modify the parameters of a certain protocol, click the required protocol in the list of supported protocols and click **Protocol advanced settings** in the **Protocols options** window toolbar or choose corresponding option from the protocol context menu opened by right-clicking the necessary protocol name in the list.

To start with protocol configuration choose one you need from the list:

- [POP3, SMTP and IMAP](#)

- [OSCAR](#)
- [XMPP](#)
- [HTTP](#)
- [FTP](#)
- [Mail.Ru Agent](#)
- [Yahoo](#)
- [MAPI](#)

5.3.3.1 POP3, SMTP and IMAP settings

To configure interception of data transferred over POP3, SMTP and IMAP select or clear the check boxes available in the **Protocol advanced settings** window for the selected protocol.

TLS session warnings

The program can detect secure sessions and generate warnings thereof. To enable this feature, select the **Store warnings in data storage if a TLS session is detected** option.

If this option enabled, the details of such sessions will be saved in a database and will be available for viewing in the search module of the program.

Saving user names and passwords

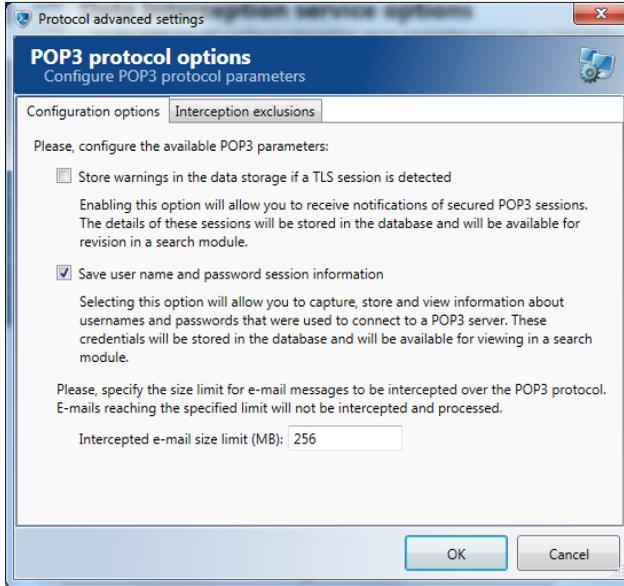
Selecting the **Save user name and password session information** option will enable system to intercept, save and provide user with information about user names and passwords used for the connection to a server. These data will be saved in a database and will be available for viewing in the search module of the program.

Setting size limits for e-mail interception

Specifying the limit for e-mail messages to be intercepted, you can avoid intercepting excessively heavy e-mails and, thus, avoid database overloading.

Saving message headers (for IMAP only)

Enabling the **Intercept and save mail headers** option will enable interception, saving and viewing e-mail message headers, even if only headers (with no text body) were transmitted from the server to the client. Message headers normally contain such information as sender addresses, message subjects, etc.



See also: [Disabling interception for certain accounts](#)

5.3.3.2 OSCAR settings

Interception of user information

Enabling this option will provide interception of additional information about users (user names, e-mail addresses, etc.). These data will be saved in a database and will be available for viewing in the search module of the program.

Interception of user avatars

Enabling this option will provide interception of user avatars (pictures used for ICQ user profile personification) and to view them with the help of the search module of the program.

It is possible to specify the particular UINs as excluded from interception. Upon including an OSCAR UIN to the ignored list any conversation that contains messages from/to the ignored OSCAR UIN will be skipped (including other participants messages within conversation).

Warnings on encrypted messages

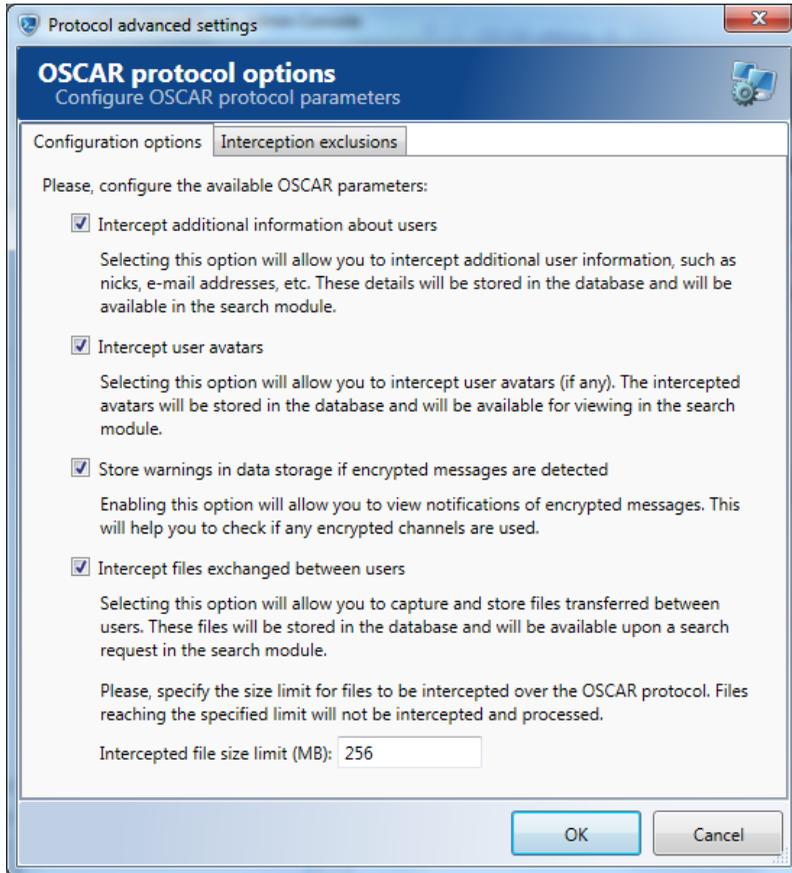
The program can detect and generate warning messages about the transfer of encrypted messages. To enable this feature, select the **Store warnings in data storage if encrypted messages are detected** check box in the **Protocol advanced settings** window for the selected protocol. With this option enabled, the details of such messages will be saved in a database and will be available for viewing in the search module of the program.

Interception of transferred files

Selecting this option will enable one to intercept and save files exchanged by the ICQ users.

Setting limits for file interception

By specifying the size limit for files exchanged by the ICQ users, you can avoid intercepting excessively heavy files and, thus, avoid database overloading.



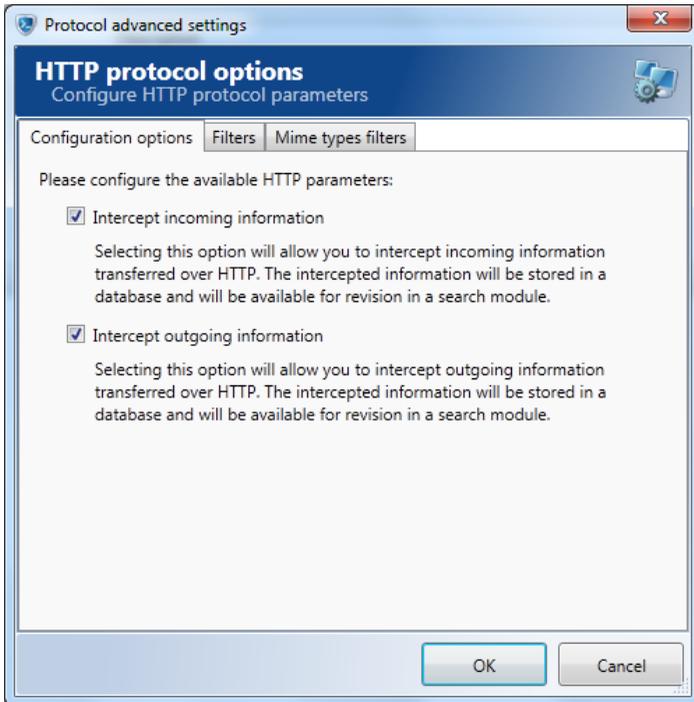
See also: [Disabling interception for certain accounts](#)

5.3.3.3 XMPP settings

The XMPP settings window includes only one tab – **Interception exclusions**. For details on adding and deleting ignored accounts, see [Disabling interception for certain accounts](#).

5.3.3.4 HTTP settings

General settings of HTTP interception can be accessed in the **Configuration options** tab.



Common options

For configuring HTTP interception the following parameters are available:

Interception of incoming data - Selecting this option will enable interception of the incoming information transmitted over HTTP (downloaded URLs).

Interception of outgoing data - Selecting this option will enable interception of the outgoing information transmitted over HTTP (posts, requests, and uploaded files).

The maximum intercepted HTTP POST size is specified within built-in Content-Length filtering rule for all web resources.

To specify custom restriction of maximum intercepted HTTP file size, click the **Filters** tab of the **HTTP protocol options** window and create a new filtering rule as described below with search condition for the necessary Content-Length value in the Web condition field.

Filtering incoming traffic

To configure filtering click the **Filters** tab of the **HTTP protocol options** window and select the **Enable filtration by HTTP requests parameters** check box.

Filtering outgoing HTTP traffic will help to avoid interception of data that does not contain user-requested data (“junk traffic”) and etc.

Filtering is implemented by the filtering rules.

The built-in group of rules contains following types of rules:

- filtering of the specified applications HTTP traffic;
- filtering of the requests to the specified web sites;
- request body size restriction;
- filtering data without “User-Agent” field in the request to prevent interception system application traffic;
- ignoring the request for a web site favicon;
- ignoring other specified type of requests.

The built-in rules can't be modified or deleted.

To configure a user defined filter add a new filtering rule or group of rules.

To activate a filter select the corresponding rule check box in the list of rules.

Note: To select or clear several selected filters check box right-click any selected rule in the list and click the necessary command on the context menu.

To allow or deny traffic interception regulated by the specified rules, select the check box with the corresponding filtering mode in the window:

- **Intercept HTTP requests that fulfills the filters listed above;**
- **Intercept all HTTP requests except the ones that fulfills the filters listed above.**

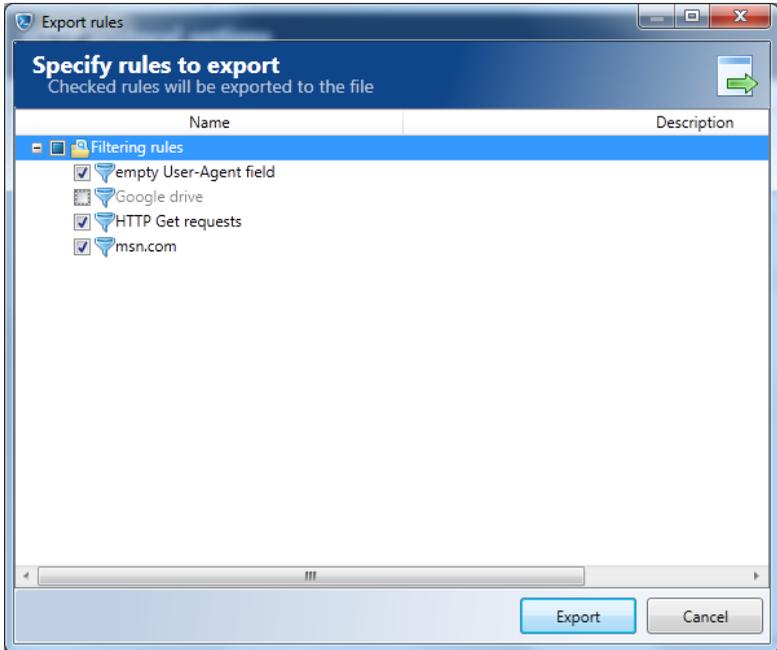
The information for each group (rule) with the name and the description of the group (rule) is displayed in the window. Content of the group can be expanded or collapsed by clicking expand or collapse button  to the left of group name.

To change filtering conditions of existed rule highlight it in the list and click **Modify**. To remove the rule click **Delete**.

Export/Import filters

The system support saving (export) the list of filters configured into a file (*.strf) and subsequently restore (import) the list.

1. To export the filter list on the **Tools** menu, click **Export**.



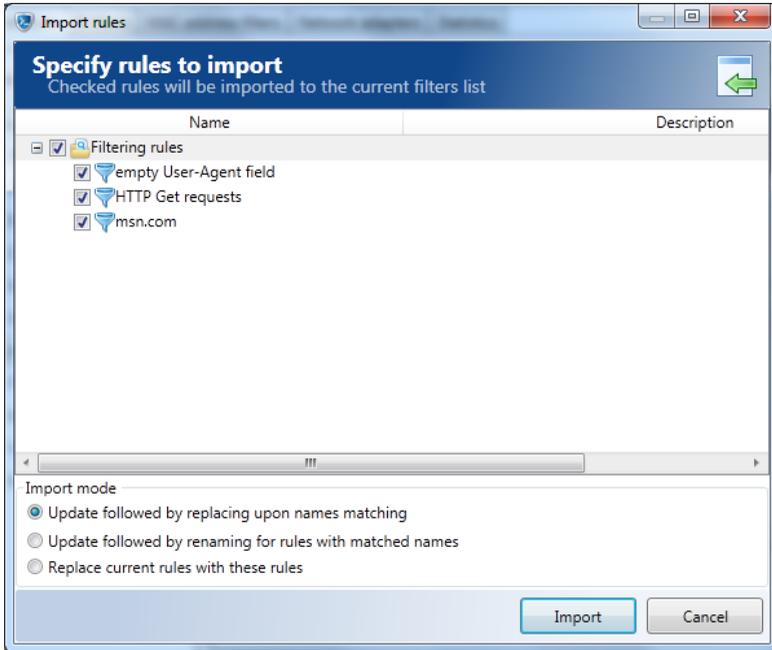
In the new window select the filters that will be exported by checking the boxes in the corresponding lines. After you have selected the necessary filters, click **Export**.

In the new window, select a folder where you wish to save the file, specify the name of the file and click **Save**.

2. To import a list of filters from a previously saved file, on the **Tools** menu, click **Import**.

In the new window select a folder and a *.strf file with filters.

After you have selected the file, click **Open**.



Next, you have to select the filters you wish to import by checking the corresponding boxes and specify one of the following import modes:

- Update with replacing if rules names matching - if any of the current rules has the same name as any imported rule, it will be replaced with the new one;
- Update with renaming if rules names matching - if any of the current rules has the same name as any imported rule, the new rule will be renamed and imported under the new name;
- Replace the current rules with a new - all the current rules will be deleted and the new ones will be imported.

Click **Import**.

Creating a group

To create a new group of rules, on the **Add** menu click **Group**.

In the **Group name** text box of the opened dialogue window, enter the name of the created group of rules, and fill out the **Description** text box (optional) with the group description.

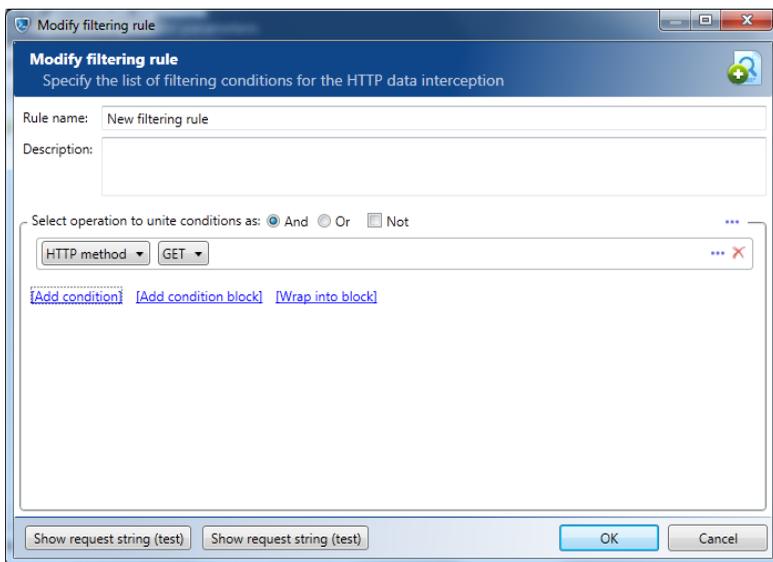


Upon finishing entering group settings, click **OK**. To discard creating a new group of rules, click **Cancel**. The newly added group of rules will be displayed in the list of filtering rules.

Creating a new rule

1. To create a new rule, select the group which this rule will be related to.
2. On the **Add** menu click the **Filtering rule**. In the opened dialogue window enter the name of the created rule in the **Rule name** text box and fill out the **Description** text box (optional) with the rule description. In the section under the **Description** text box specify the conditions for the data search that will be implemented by the system in an automatic mode.

Data can be searched by HTTP method type, IP address (as well as local or remote), by the specified port (as well as local or remote), by the size of data and by the interception date and by the Web-field parameters (field names of request header). Condition and parameters types are available in drop-down lists.



For various search conditions different relevant operations can be specified (see below).

Search conditions for data filtering

By date

Specify one of the following conditions: **Equal** (search for data transferred on the specified date), **Not equal** (search for data transferred on any date except specified), **Within range** (search for data transferred during the specified period), **Beyond range** (search for data transferred on any date except the specified period).

By time and day of week

To search by time you can specify conditions similar to the ones for search by dates.

To search by day of week you can specify one of the following conditions: **Equal** (search for data transferred on the specified days of week) or **Not equal** (search for data transferred on any day of the week except specified).

By IP address or port number

When searching by IP addresses or ports, one can set the following parameters:

- **local or remote** (to search for data transmitted from/to local or remote computers having the specified IP addresses or via specified local or remote ports), **local** (to search only for data transmitted from/to the local computer with the specified IP address or via specified local port), **remote** (to search only for data transmitted from/to the remote computer with the specified IP address or via specified remote port);
- **equal** (to search for data transmitted from/to specific computer having the specified IP address or via specified port), **not equal** (to search for data transmitted from/to any computers except for the one having the specified IP address or via any port except for the specified one), **within range** (to search for data transmitted from/to computer having IP addresses within the specified range or via specified range of ports), **beyond range** (to search for data transmitted from/to any computers except for those having IP addresses within the specified range or via any port except for the specified range of ports).

By HTTP method

The system enables identification and blocking of GET and POST HTTP(S) requests.

To block any HTTP(S) request by method it was sent use a corresponding parameter from the **HTTP method** blocking condition.

This type of blocking condition is useful to go with any other one to enhance a rule performance.

By Web - fields content

There are four fields names in preset for web-field condition:

- **URI**;
- **Host**;
- **Content-Length**;
- **User-Agent**.

1. To set condition value select the necessary one from the drop-down list of conditions types and select one from preset field name or type any other custom name instead.

2. Choose a value type of condition selected previously and specify it. Upon the **Value list** type selecting use the following input format:

- `*<value>*` - the header field **contains** this value;
- `*<value>` - the header field **ends with** this value;

- `<value>*` - the header field **starts with** this value;
- `<value>` - the header field **equal** to the value.

The combination of different types of search conditions helps to increase efficiency of blocking rules. For example, the combination of conditions which provide search for requests with both the **URI** field and the **Host** field contain specified symbols or text (parameters **Contains** or **Equal**), will deny access to separate web pages or elements of the particular web resource.

Using the **User-Agent** field with parameter **Is absent**, for example, enables disabling network activity of the service and harmful software which doesn't use this field in POST requests usually.

Using of customer field as search conditions can be the useful too. So, f. e., restriction of transferred message size by defining the **Content-Length** field with the **Beyond range** parameter value in bytes is possible and a blocking transfer of data with specified format, using a combination of **Content-Type** field name and either the **Contains** or the **Equal** parameter value.

Example 1: One see the following type of record in the intercepted HTTP traffic in Client Console: `http://www.facebook.com/plugins/likebox.php?id=185550966885&width=292&connections=10&stream=true&header=true&height=587" scrolling="no" frameborder="0" style="border:none; overflow:hidden; width:292px; height:587px;`

This kind of records can be filtered, for example, by a combination of **Host** and **URI** fields. To do this, create a new GET filter and specify the **Host** field which **ends with** `<facebook.com>`. Then click **Add** condition and specify the **URI** field which **starts with** `</plugins/>`.

Example 2: After you identify a “junk” HTTP post in the search results in Client Console, you can create a separate filter to exclude interception of similar posts in future. To do this, you have to open the HTTP header of the selected post (the **Show HTTP header** button in the toolbar). A typical HTTP header has the following structure:

```
POST /ubds/lookup_dst/HTTP/1.1
Accept-Encoding: identity
Content-Length: 2172
Host: ubds.uniblue.com
Content-Type: multipart/form-data;
boundary=192.168.1.68.1.304.1317362182.595.1
Connection: close
User-Agent: Python-urllib/2.6
```

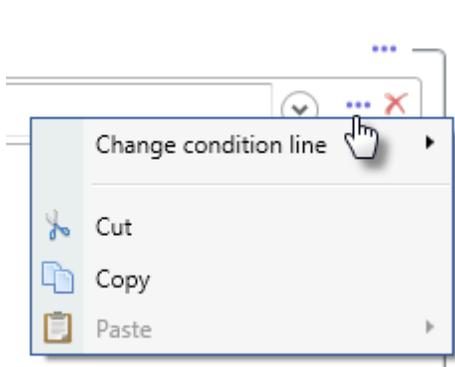
Similar HTTP posts can be filtered, for example, by the *User-Agent* field. Create a new filter, specify the name of the field **“User-Agent”**, which **starts with** `<Python-`

urllib».

Besides, such HTTP posts can be filtered by the *Host* field (in the filtering conditions, specify the name of the field «**Host**», which **equals to** «*ubds.uniblue.com*»), or by *URI* (in the filtering conditions, specify the name of the field «**URI**», which **equals to** «*/ubds/lookup_dst/*»).

Operating with search conditions

1. Search may be carried out with logical disjunction (the “**OR**” operation) or a logical conjunction (the “**AND**” operation) of several search conditions or condition block:
 - Upon selecting logical “**AND**” search operator, notifications will be delivered only in cases of information transfer is satisfy **ALL** the specified search conditions simultaneously. For this, in the **Select operation to unite conditions as section**, check the **And** option.
 - Upon selecting the “**OR**” search operation, notifications will be delivered in cases of information transfer is satisfy **ANY** of the specified search conditions or search condition blocks. For this, in the **Select operation to unite conditions as section**, check the **Or** option.
2. To add a new search condition, click the **Add condition** link. To delete some search condition, click the **Delete** icon  in the right part of the corresponding condition. By default, there is a form for entering the first search condition in this window, but it can be deleted if a search condition block should be created instead.
3. To add an entire search condition block, click the **Add condition block** link. Creating condition blocks helps conduct automatic search subject to complex or advanced search conditions. New blocks or conditions can be created within other blocks and conditions.
4. When creating a new or editing an existing rule numerous advanced procedures for search conditions and conditions block are available from the **Tools** menu (the icon in the end of a condition line).



To work with advanced procedures, click the **Tools** menu icon  and select a necessary one:

- To change the item line, point to **Conditions line change** and click one of available commands.
- Click **Cut** to remove selected item from the parent block body and copy it to clipboard. After applying this operation the **Paste** procedure is available for item that was cut within any blocking rule.
- Click **Copy** to copy selected item to clipboard. After applying this operation the **Paste** procedure is available for item that was copy within any blocking rule.
- The **Paste** procedure is available when any item was previously copied or cut. Point to **Paste**, and then:
 - To insert item from clipboard in the specified position within the parent block body, click **Paste into block**.
 - To paste item on the line above selected search condition or block, click **Paste above**.
 - To paste item on the line below selected search condition or block, click **Paste below**.
- Click **Copy search condition as image** to copy the root block of search conditions to clipboard as screenshot of the block body. This procedure is available for a root block only.
- Click **Save search condition as image** to save the root block of search conditions to clipboard as PNG format file with screenshot of the block body. This procedure is available for the root block only.

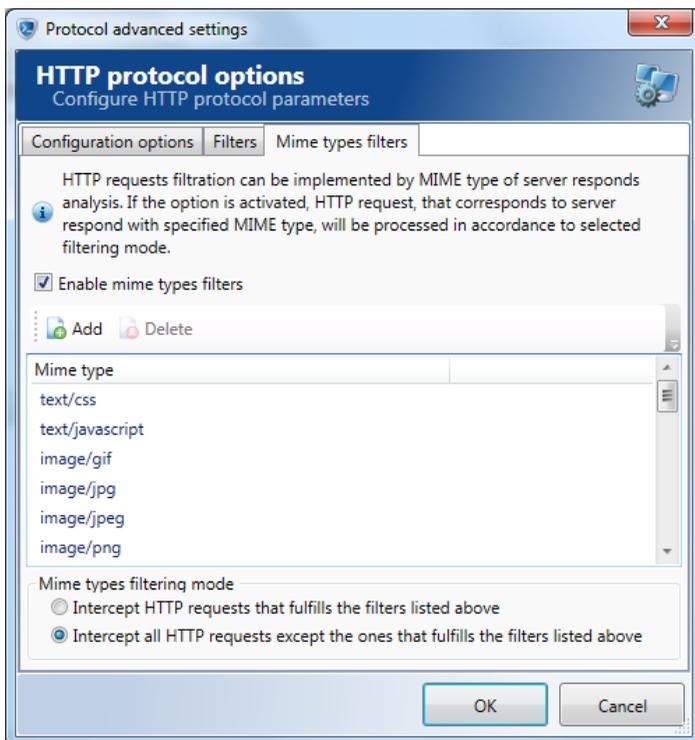
Setting up filtering by MIME data types

MIME describes transfer mechanisms for different types of information transmitted over the HTTP protocol. Such information can be represented by text (on languages other than

English) and non-text data formats, such as images, video, audio, and applications.

HTTP requests filtration implemented according to results of **server responds MIME type analysis**. Herewith HTTP request, that corresponds to server respond with specified MIME type, will be intercepted and saved in data base or skipped in accordance with filters settings.

One can configure interception filtration by MIME data types by the console means. This will help to intercept only the types of data you are interested in, as well as to avoid database overloading owing to disabling interception of the types of data that you do not need.



To set HTTP traffic interception filters by MIME data types:

1. Click the **Mime types filters** tab in the **HTTP Protocol advanced settings** window.
2. To enable/disable mime type filter, select/clear the corresponding box.
3. In the MIME types window, there is a default list of data types proposed by the program. You can apply only one of the available filtering modes to this list: enabling or disabling interception of the specified data types. The filter that disables interception of the suggested data types is set by default in the program. To enable or disable interception of the specified data types, deselect the corresponding filtering mode:

- **Intercept HTTP requests that meets the criteria listed above**

or

- **Intercept all HTTP requests except the ones that meets the criteria listed above.**

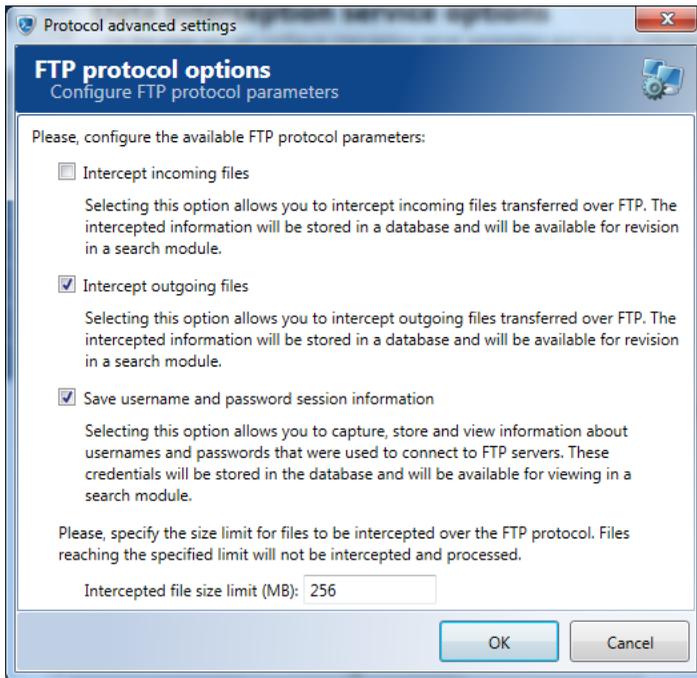
4. To add a new data type, click **Add** and specify a type in the text field .
5. To remove some MIME data type from the filter, click the necessary data type in the list and click **Delete**.
6. To save the settings made, click **OK**. To discard the changes, click **Cancel**.

See also: [Disabling interception for certain accounts](#)

5.3.3.5 FTP settings

Interception of received files

Selecting this option from the protocol's [context menu](#) will enable setting up the interception of files transferred over FTP.



Interception of sent files

Selecting this option will allow system to intercept the files sent over FTP.

Saving user names and passwords

Enabling this option will allow system to intercept, save and view information about user names and passwords used for the connection to an FTP-server. These data will be saved in a database and will be available for viewing in the search module of the program.

Setting limits for file interception

Specifying the limit for files to be intercepted, you can avoid intercepting excessively heavy files and, thus, avoid database overloading.

See also: [Disabling interception for certain accounts](#)

5.3.3.6 Mail.Ru Agent settings

Intercept files exchanged between users

If the **Intercept files exchanged between users** option is enabled, the system will intercept files transferred by users using Mail.Ru Agent protocol, in addition to capturing the messages.

To reduce the amount of data stored in the database of intercepted traffic, you can specify the maximum size of files that will be intercepted. Larger files sent or received by users via Mail.Ru Agent will not be intercepted and stored.

See also: [Disabling interception for certain accounts](#)

5.3.3.7 Yahoo settings

If the **Intercept files exchanged between users** option is enabled, the system will intercept files transmitted by users via Yahoo IM, in addition to capturing the messages.

To reduce the amount of data stored in the database of intercepted traffic, you can specify the maximum size of files that will be intercepted in the related field. Larger files sent or received by users via Yahoo IM will not be intercepted and stored.

See also: [Disabling interception for certain accounts](#)

5.3.3.8 MAPI settings

SecureTower enables interception of data transferred using MAPI (MAPI over RPC over HTTP and MAPI over RPC).

Intercept incoming mail

To intercept all incoming messages and files, transferred using MAPI protocol, select the **Intercept incoming mail** check box. The intercepted data will be stored in the database and will be available for review from Client Console.

Intercept outgoing mail

To intercept all outgoing messages and files, transferred over MAPI protocol check the **Intercept outgoing mail** option. The intercepted data will be stored in the database and will be available for review from Client Console.

All messages transferred over MAPI are intercepted by default.

See also: [Disabling interception for certain accounts](#)

Note: A preliminary connection configuring is required for network with Microsoft Exchange Server 2010 if interception of MAPI traffic is necessary. The PS Exchange console can be used for configuring - use **Get-RPCClientAccess | ft Server, EncryptionRequired** command for status checking and **Get-RPCClientAccess | Set-RPCClientAccess –EncryptionRequired:\$False** command for the “encryption required” parameter disabling. These settings are required for establishment client application unencrypted connection to Microsoft Exchange Server 2010.

Attention: MAPI traffic interception is not provided by **SecureTower** for Microsoft Exchange Server 2013.

5.3.3.9 Disabling interception for certain accounts

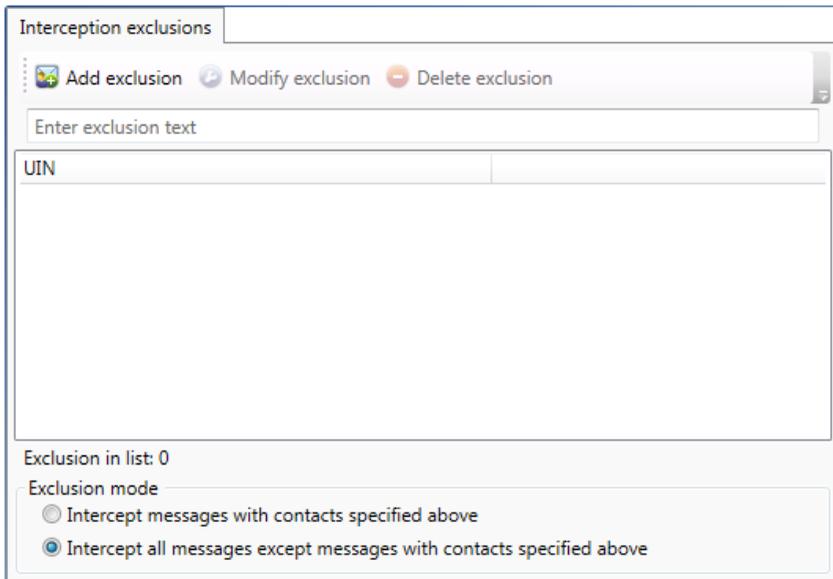
One can assign the list of email address and accounts or instant messenger user accounts (UINs for ICQ, e-mail addresses, etc.) that will be ignored by the interception system. If necessary to renew their interception, these accounts can be excluded from the list of ignored accounts.

5.3.3.9.1 Adding an account to ignored accounts

1. To disable interception for certain accounts, click the required protocol entry in the list of supported protocols and click **Protocol advanced settings**.

Note: If it is necessary to ignore during interception messages of a user with a particular email address or account, such an address can be included into the list of exclusions in the **Protocol advanced settings** window for SMTP, POP3, IMAP, MAPI; if it is necessary to skip conversations of a certain ICQ UIN, this UIN can be specified in the list of exclusions in the **Protocol advanced settings** window for OSCAR; to disable interception of a certain XMPP user conversations, the account of such a user can be specified in the list of exclusions in the **Protocol advanced settings** window for XMPP. The option is available for all the protocols, except for HTTP and FTP.

2. In the **Protocol advanced settings** window, click the **Interception exclusions** tab.



Interception exclusions

Add exclusion Modify exclusion Delete exclusion

Enter exclusion text

UIN

Exclusion in list: 0

Exclusion mode

Intercept messages with contacts specified above

Intercept all messages except messages with contacts specified above

3. Click **Add exclusion**.

4. In the text box in the opened window, type the necessary account, e-mail or UIN correspondingly.

5. Click **Add**. The added account will be displayed in the window with the list of ignored accounts.

6. To modify the exclusion, click it in the list and click **Modify exclusion**.

7. Select the interception mode. There are two available modes: white list and black list. Only one type of mode can be applied to the entire list of exclusions:

- If exclusions are included into the white list (the **Intercept messages with contacts listed above** radio button), only the messages which include any account from the list as recipient or sender (for the emails - in the "From", "To" or "Cc" fields) will be intercepted; messages with all other accounts will be ignored.
- If exclusions are included into the black list (the **Intercept all messages except messages with contacts listed above** radio button), all messages except for the ones which include any account from the list as recipient or sender will be intercepted; messages with listed accounts will be ignored.

Note: Upon including an IM account to the black (ignored) list, all messages from the account and conversations with this participant will be skipped. And vice versa, if any group chat contains account from the white list (specified for interception), all messages from this chat will be intercepted.

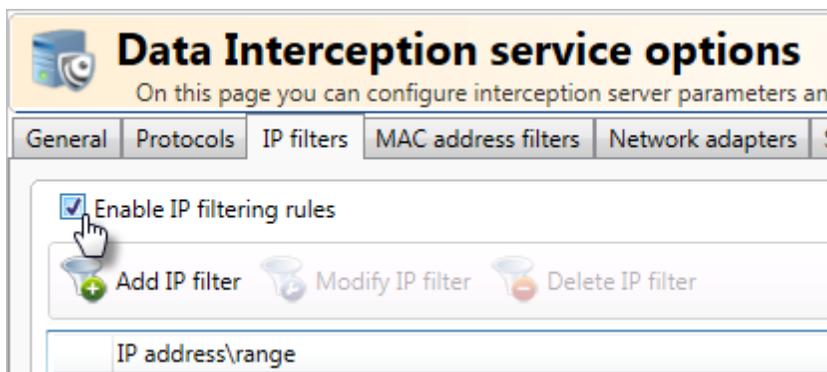
5.3.3.9.2 Deleting an account from ignored accounts

1. To renew the interception of certain accounts , click the required protocol entry in the list of supported protocols and click **Protocol advanced settings**.
2. In the **Protocol advanced settings** window, click the tab with the list of exclusions, then click the account the interception of which should be renewed (for more information, see [Ignored account list](#)), and click **Delete exclusion**.
3. In the action confirmation dialogue box, click **Yes**. The deleted account will disappear from the list of ignored accounts.

5.4 IP-filter settings

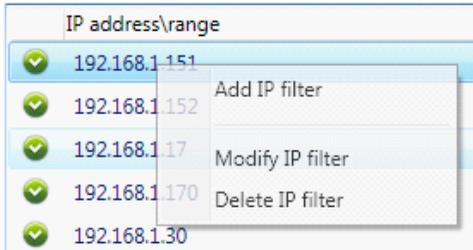
To set up traffic filtering upon interception, click the **IP filters** tab of the Data interception service window. On this page one can specify IP addresses or ranges that you want to allow or deny intercepting traffic from.

To enable filters or get access to modifying filters, select the **Enable IP filtering rules** check box. To temporarily disable the filters without canceling the settings, clear this check box.



Note: *IP filters are not applicable if dynamic IP addresses are used.*

You can add a new filter or modify and delete existed ones in the command section. These commands are also available form the context menu opened by right-clicking the necessary IP address in the IP filter list.



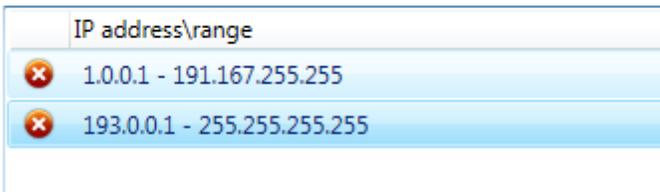
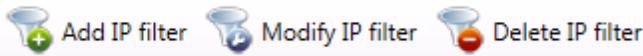
Rules of filtration:

1. Prohibiting type of the IP filter has the highest priority. Traffic from IP addresses covered by prohibited IP range will be ignored while interception, even if the IP addresses are allowed by another filters.
2. To set an IP range to intercept data from, it is necessary to deny interception of bottom and top external ranges of IP addresses.

For example, to intercept data from IP range 192.168.0.0/16:

- a) Deny interception from bottom external IP range, e.g., 1.0.0.1 - 191.167.255.255;
- b) Deny interception from top external IP range, e.g., 193.0.0.1 - 255.255.255.255.

Enable IP filtering rules



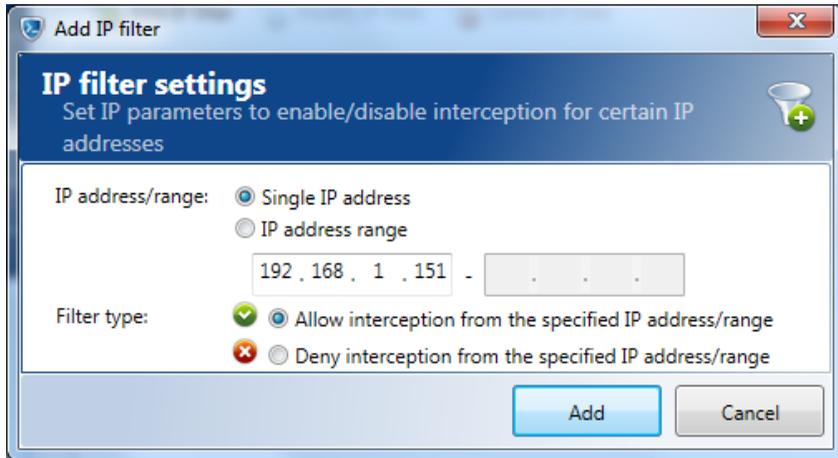
Assigning IP addresses for IP filters

To add a new IP filter click **Add IP filter** in the **IP filters** tab.

In the **Add IP filter** dialogue box, one can set filtering by an IP address or by an entire IP range. For this, click the relevant radio button (**Single IP address** or **IP address range**).

- If you choose the **Single IP address** option for the filter, provide a specific IP address for which you want to set a certain type of filter. This can be done in the entry field under the options.

- If you choose the **IP address range** option for the filter, provide an IP range for which you want to set a certain type of filter. This can be done in the entry fields under the options.



Note: The supported IP protocol version—IPv4 only. IP fragmenting is not supported.

Selecting the filter type

To allow or deny traffic interception from the specified IP address or IP range, click the radio button related to necessary filter type (see the figure above):

- Allow connections from the specified IP address/range
- or
- Deny interception from the specified IP address/range.

Saving a new filter

To add the specified filter, click **Add**. To discard the settings, click **Cancel**. The added filters will be displayed in the IP filter window as a list of IP addresses /ranges.

IP address\range
✓ 192.168.1.151
✓ 192.168.1.152
✓ 192.168.1.17
✓ 192.168.1.170

Modifying and deleting

To modify settings of a filter, click the necessary IP address or IP range in the list for which the corresponding filter is enabled, and click **Modify IP filter** or just double-click it. Follow the recommendations from this paragraph to make changes.

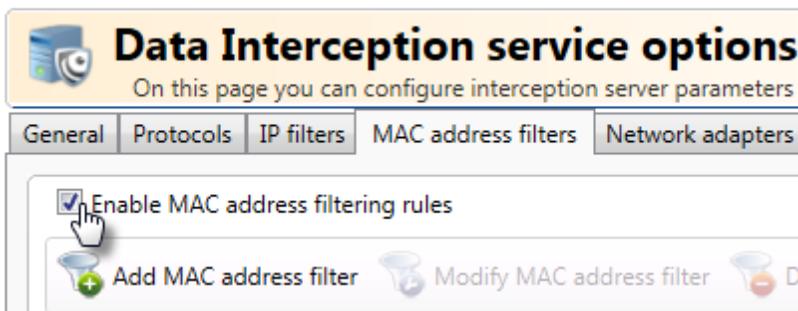
To delete a filter from the list, click the necessary IP address or IP range in the list for which the corresponding filter is enabled, and click **Delete IP filter**.

To apply all settings entered, click **Apply changes** in the bottom right corner of the program's main window.

5.5 Assigning MAC address filters for traffic interception

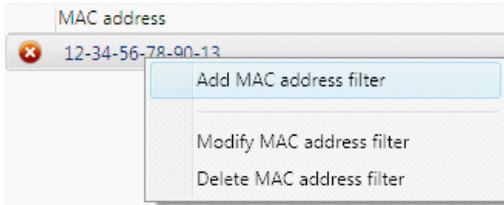
To set up traffic filtering upon interception by MAC addresses, go to the **Traffic interception server options** page, the **MAC address filters** tab. Data from all of the MAC addresses are intercepted by default. On this page you can specify MAC addresses that you want to deny for traffic interception.

To enable MAC address filters or get access to modifying the filters, select the **Enable MAC address filtering rules** check box. To temporarily disable the filters without canceling the settings, clear it's check box.

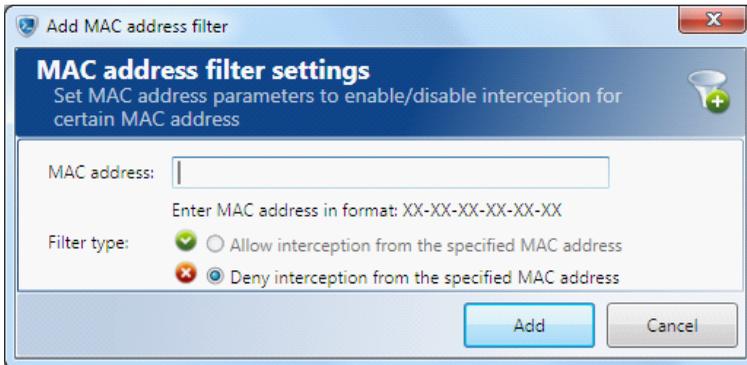


You can add, modify and delete MAC address filters in the command section.

These commands are also available in the context menu opened by right-clicking the necessary MAC address in the MAC address filter list.



To add a new MAC address filter click **Add MAC address filter** in the **IP filters** tab and open the **Add Mac address filter** window.



Assigning MAC addresses for MAC address filters

In the **Mac address** text field of the **Add MAC address filter** dialogue box, enter the MAC address that you want to exclude from traffic interception.

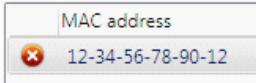
Selecting the filter type

Note: Please note that all MAC addresses in your network are automatically subject to interception. One can only deny interception from specified MAC addresses.

To deny traffic interception from the specified MAC address, select the radio button with the corresponding filter type (for more information, see [Fig. The Add Mac address filter window](#)) - **Deny interception from the specified IP address/range**.

Saving a new filter

To add the specified filter, click **Add**. To discard the settings, click **Cancel**. The added filters will be displayed in the Mac address filter window as a list of MAC addresses.



Modifying and deleting

To modify settings of a filter, click the necessary IP address or IP range in the list for which the corresponding filter is enabled, and click **Modify MAC address filter** or just double-click it. Follow the recommendations from this paragraph to make changes.

To delete a filter from the list, click the necessary IP address or IP range in the list for which the corresponding filter is enabled, and click **Delete MAC address filter**.

To apply all the settings entered, click **Apply changes** in the bottom right corner of the program's main window.

5.6 Network adapters settings

The interception server should have two network interface cards: one –for receiving the incoming mirrored traffic, the other one –to interact with the product's other services and clients .

5.6.1 Assigning network adapters for traffic interception

1. To assign network adapters from which traffic should be collected by the interception server, go to the **Traffic Interception server options** window, the **Network adapters** tab.



2. In the list of detected network adapters, one can select the adapters from which traffic should be intercepted. For this, select the check box next to the required adapter. All adapters are selected by default.

	Network adapter	MAC address
<input checked="" type="checkbox"/>	Realtek RTL8168C(P)/8111C(P) Family PCI-E Gigabit Ethernet	00:1F:D0:28:DC:D2
<input type="checkbox"/>	Realtek RTL8168C(P)/8111C(P) Family PCI-E Gigabit Ethernet	00:1F:D0:28:DC:D4
<input type="checkbox"/>	WAN Miniport (Network Monitor)	84:18:20:52:41:53

3. To view detailed information about a certain network adapter, click the desired adapter, and such data as IP addresses, IP masks, DNS-servers, DHCP-servers and gateways will be displayed in the **Network adapter information** section.

Network adapter information

IP addresses:	10.0.0.10
IP masks:	255.255.255.0
DNS servers:	
DHCP servers:	255.255.255.255
Gateways:	

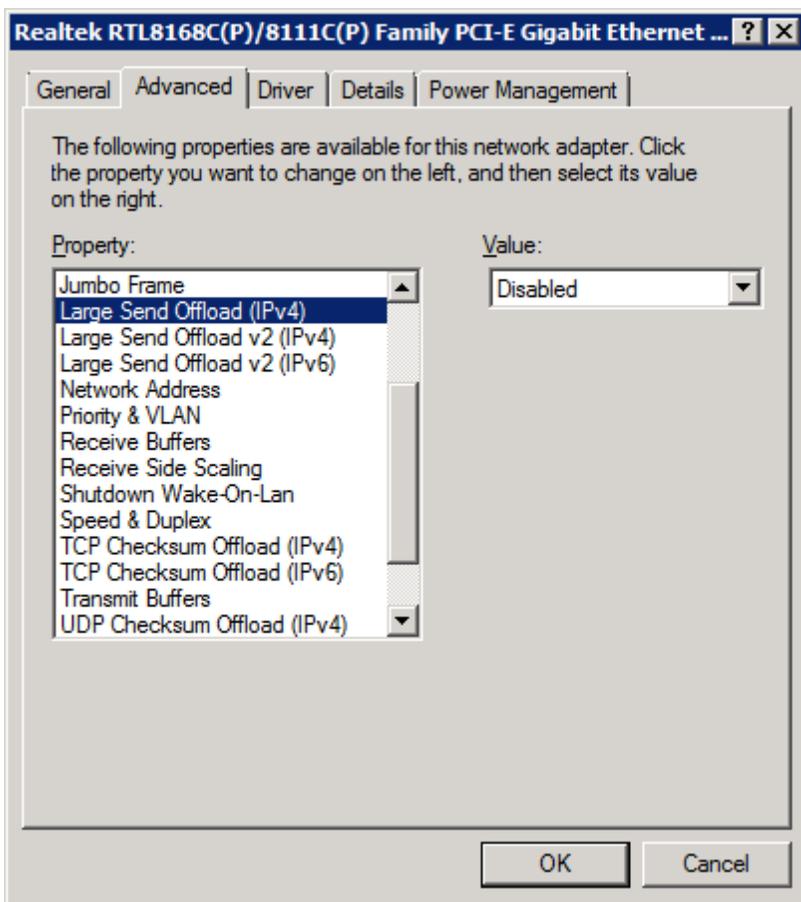
To refresh the list of network adapters, click **Refresh adapter list** in the **Commands** section.

4. To apply all the settings entered, click **Apply changes** in the bottom right corner of the program's main window.

5.6.2 Advanced settings

In order to ensure operation of the interception server, the Large Send Offload option should be disabled in the advanced settings of the network adapter allocated for receiving the intercepted traffic. This option is responsible for the reduction of the CPU workload upon the transmission of large IP packets. If it is disabled, IP packets are divided by the operating system into numerous 1.5 KB sized packets before being sent to the network adapter. If this option is enabled, large IP packets are sent to the network adapter directly without being first processed by the operating system. Taking into account that the only task performed by the interception server is receiving and processing network traffic, there is no need in enabling this option. Disabling the Large Send Offload option is a critical requirement for the operation of the interception system,

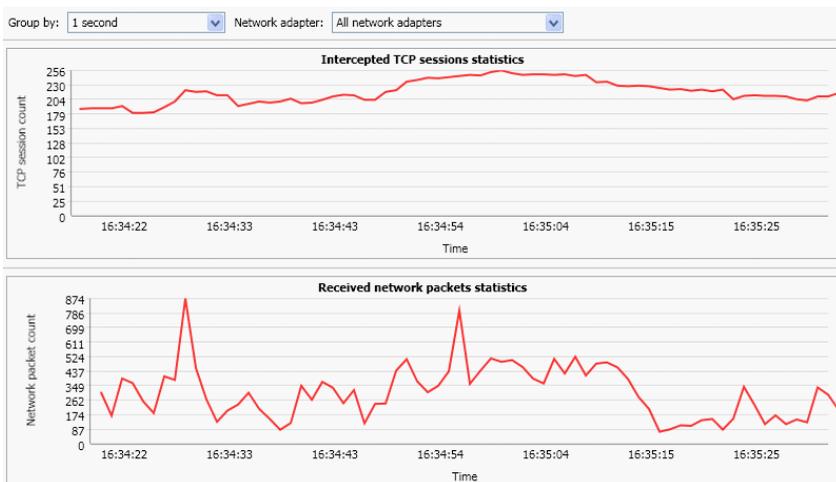
since the interception server does not support working with large IP packets, which may lead to some part of traffic being skipped.



5.7 Interception statistics

To view detailed data on connections and network activity as a statistics report in a real-time mode, select the **Statistics** tab of the **Traffic interception server options** page.

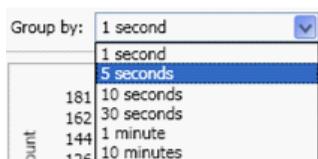
In the **Statistics** window, the following information is provided: **Intercepted TCP sessions statistics**, **Received network packets statistics** and **Sent network packets statistics** for each moment of time. The statistics is presented in form of graphs with the amount of the respective intercepted data for a certain time interval (for more information, see [Calculating statistics for a specified interval](#)).



5.7.1 Calculating statistics for a specified interval

The program groups statistic data by time intervals on the basis of which a simple average of the interception data is calculated. One can set time intervals for which a simple average will be calculated and subject to which statistic data will be provided in a real-time mode. For example, if a user sets 1 second as a time interval, the program will be calculating the data simple average for the interval of 1 second and will be providing statistic data as frequent as one second. Upon the time interval of 10 minutes, the program will be calculating average values for a ten-minute interval and will be providing statistics every 10 minutes.

To specify the interval for the program to calculate and provide statistics, select the necessary value from the **Group by** list box: 1, 5, 10, 30 seconds, 1 minute and 10 minutes.



5.7.2 Interception statistics for a certain network adapter

To view the statistics of data interception from a certain network adapter, select the necessary adapter from the **Network adapter** list box. By default, the console provides statistics for all the network adapters.



6 Setting up data indexing

Indexing service is responsible for extracting information from complex data formats and processing text documents to convert them into a searchable content. To accelerate full-text search, the index service creates indexes of the intercepted data including a list of all the words that the data contain together with their location within the indexed document. A data index contains not only the list of keywords of the intercepted data, but also such their attributes as message subject and size, e-mail address, UIN, IP address, etc.

One can **create data indexes** in Administrator Console **depending on the protocol** over which data are transferred: separate indexes for POP3, SMTP, Skype, etc. But this is not strictly required, and an index can be formed on the basis of several data sources. Creating separate indexes for each protocol is recommended in case it is necessary to set index update intervals for each protocol individually.

The accuracy of the search results displayed depends on the customizable **index update frequency** that can be set up in Administrator Console. The more often the data index is updated, the more up-to-date will be the information extracted from it by the search module of the program. The system supports a parallel mode processing of the included in index protocols data. The quantity of protocols processed simultaneously corresponds to the CPU core quantity. In this way processing of the data while searching, updating or deleting is performed for each data source simultaneously.

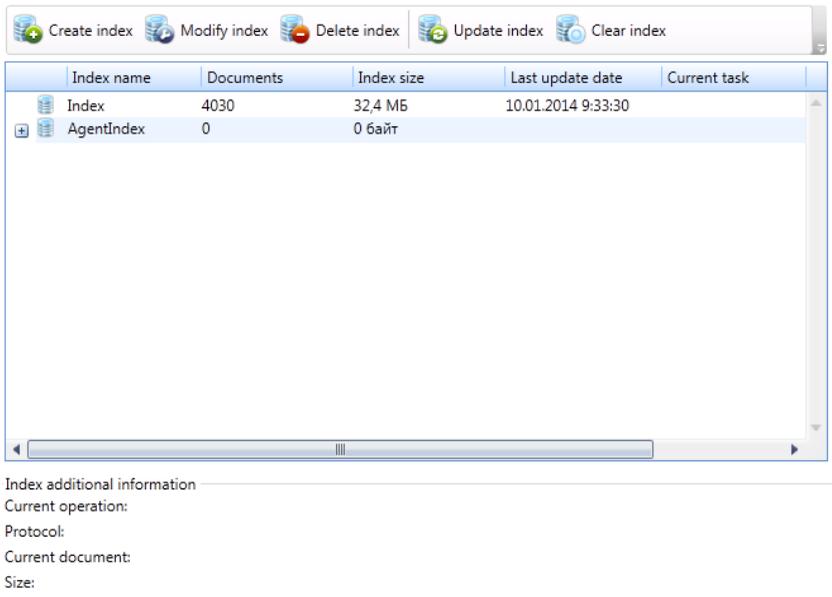
To create, modify and set up search indexes, select the **Data Indexing** tab in the left sidebar of the program's main window.

6.1 Viewing list of indexes

The list of available indexes (if any) is displayed in the **Data Indexing** settings window. The indexes can be sorted by the following parameters:

- Index name (alphabetically);
- Number of documents in the index (containing indexed data);
- Size;
- Last time updated.

By clicking the column header, one can get ascending or descending sorting of indexes by the values in the corresponding column.



In the ribbon toolbar of the data indexing window one can select the buttons for operating with indexes.

To perform any operation with index select the necessary index in the list and click the corresponding button. Index operations are available from the index popup menu as well.

Index context menu

The operation of [creating](#), [modifying](#), [deleting](#), [updating](#) and [clearing](#) are accessible from the context menu.

Beside this the following operation are accessible:

- **Defragment index.** Use to perform optimization of the index logical structure.
- **Make index not available for search operations.** Use to exclude the index from search if the source of data included in index is unwanted for considering while searching .
- **Convert index to new format.** Use to convert any index created in the older versions to the new format.

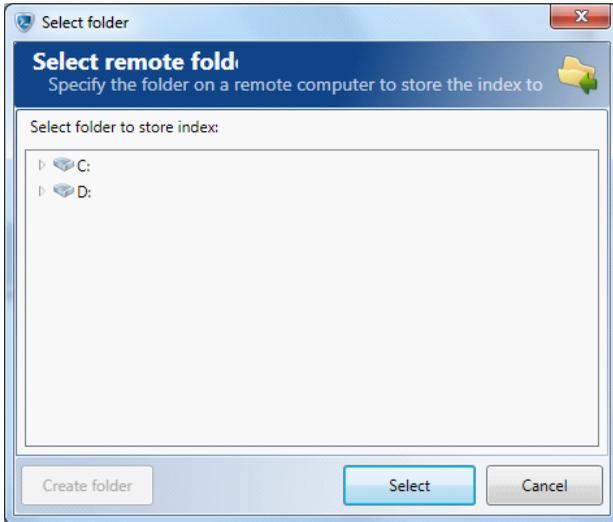
6.2 Creating a search index

To create a new index, click **Create index** in the **Data indexing** settings window toolbar.

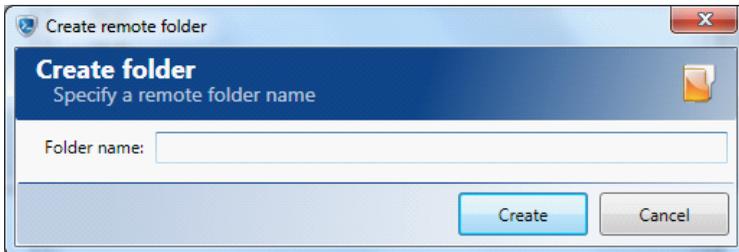
6.2.1 Setting up index parameters

1. In the **Properties** tab, enter the name of the index to be created in the **Index name** text box of the **Create index** window. For example, when creating an index for POP3, this index can be named as "POP3".
2. In the **Index Store Path** text box, specify a path on a remote server disk where this index will be stored. The index store path can also be selected by clicking the network folder icon to the right of the store path entry field.

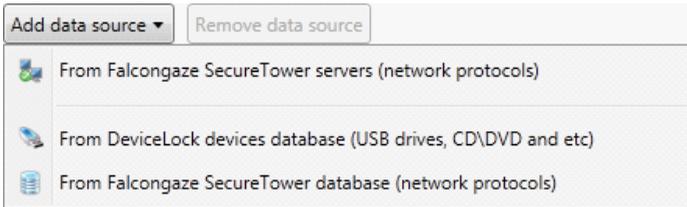
3. In the **Select folder** window, specify the folder in which the index should be saved. To expand/hide the content of the disks or folders, click the arrow button in front of the corresponding folder or disk. To select the folder, click **Select**.



4. If there is no suitable folder to save the index into, it can be created on one of the remote server's disks. To do this, click **Create folder** and specify the name of a new folder in a new window. To save the folder, click **Create**. To discard creating a new folder, click **Cancel**.



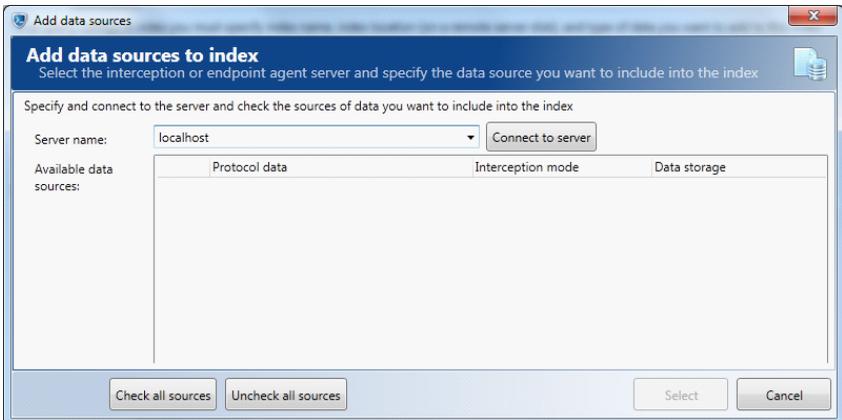
5. After creating a new folder, select it from the list of available folders by clicking **Select** in the **Select folder** window. The newly created index will be saved into this folder.
6. Click **Add data source** in the **Sources of intercepted data to be included into the index** section and choose one of the two available options from the drop-down menu.



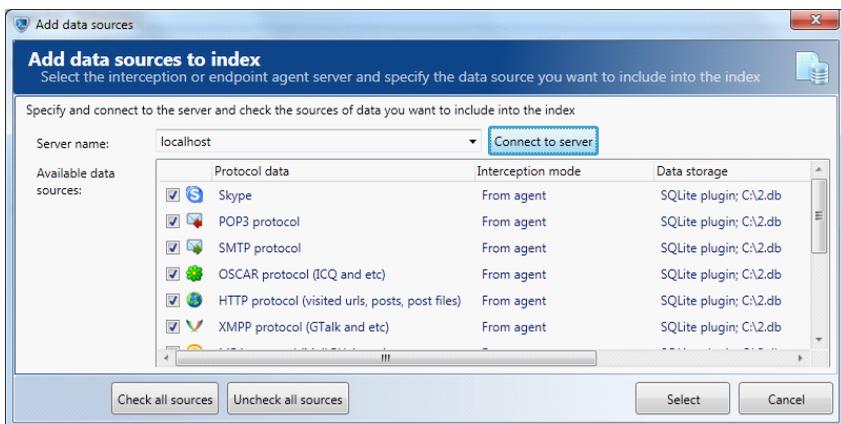
Select the sources of data to be included into the index:

- If you wish to include data transferred over network protocols (POP3, SMTP, Oscar, Skype, HTTP, etc.) and intercepted by **SecureTower** servers, select option **From Falcongaze SecureTower servers (network protocols)** and proceed to the next paragraph.
- If you wish to include data sent to external devices (USB drives, CD/DVD etc.) and intercepted by DeviceLock application, select option **From DeviceLock devices database (USB drives, CD/DVD etc.)** and proceed to paragraphs 9-12.
- If you wish to include data that was previously intercepted by **SecureTower** and is stored in a database, select option **From Falcongaze SecureTower database (network protocols)** and proceed to paragraphs 13-15.

7. In the **Add data sources** window, specify the name of the physical server on which the software interception server component is installed and click **Connect to server**.



In case of a successful connection to the server, the list of available protocols to be added into the index will be displayed in the **Available data sources** window.



8. Select necessary protocols from the list by checking boxes next to the required protocols. To include all the protocols into the index, click **Check all sources**; to exclude all the protocols, click **Uncheck all sources**.



Having checked the necessary protocols, click **Select**. To discard adding the selected protocols into the index, click **Cancel**.

Note: The selected protocols will be displayed in the **Sources of intercepted data to be included into the index** window. To exclude some protocol from this list, click the required protocol and click **Remove data source**.

9. In case you have selected the option **From DeviceLock devices database (USB drives, CD/DVD etc.)**, a dialog box will open in which you can configure a connection to the database which is used to store data captured by DeviceLock.

First you have to specify the name of the physical server where your database is stored (i.e. the MS SQL Server database containing the intercepted devices data). Enter the name of the server in the **Server name** text field or choose one from the drop-down menu opened by clicking the arrow icon in the right corner of the text box.



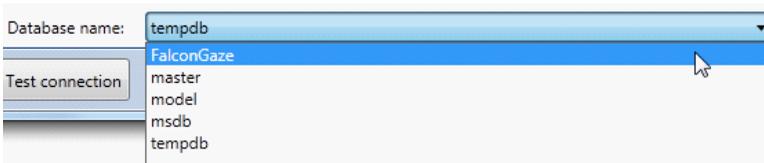
10. Next, select the authentication parameters of the server. Refer to section [Setting up a connection to an MS SQL Server database](#) for details.

- Use Windows authentication
- Use MS SQL Server authentication

User name:

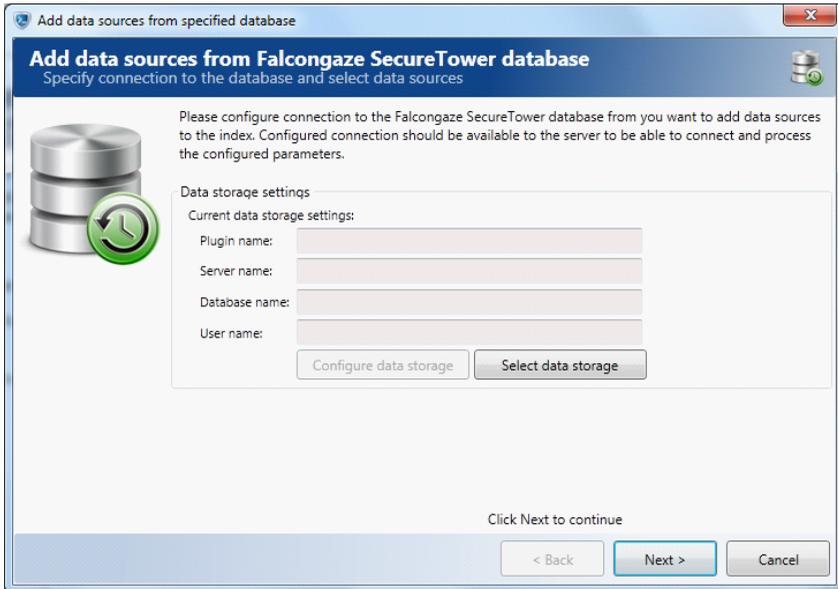
Password:

11. In the **Database name** list box select the name of the database used to store intercepted device data.

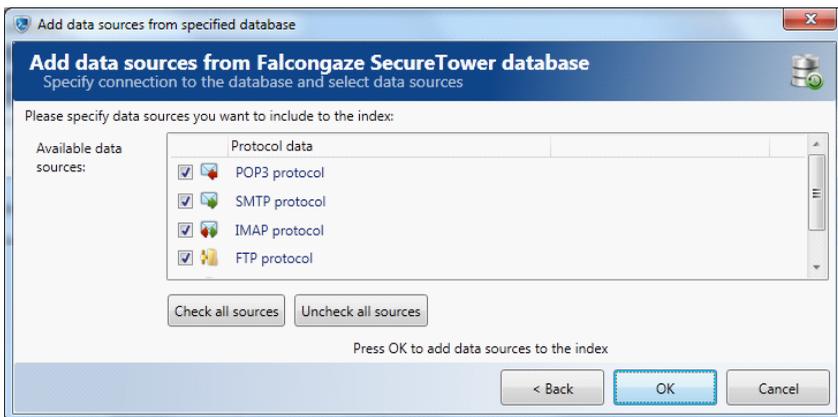


12. Click **OK**.

13. If you have selected the **From Falcongaze SecureTower database (network protocols)** option, a wizard window will open to guide you through the process of adding a data source.



14. Click **Select data storage** to specify parameters of connection to the database (for detailed instructions on configuring database connection parameters refer to paragraph **0 Interception server general parameters: database settings**). Click **Next**.



15. In the next window you will see a list of data types (i.e. protocols they were intercepted over – mail, messengers, etc.). Check the data types (protocols) you wish to add to the index and click **OK**.

16. To configure **Scheduler** parameters, refer to section [Configuring the scheduler](#).

17. To disable the index, uncheck the option **Index available for search operations**. If disabled, the index will stop updating and the data contained in it will be unavailable for search and processing by the system.

After you have specified all necessary index settings, click **Create**. The created index will be displayed in the list of indexes in the **Data Indexing** settings window. To cancel creating the index, click **Cancel**.

Index name	Documents	Index size	Last update date
 POP3	95386	745 MB	21.06.2010 11:52:06
 SMTP	23784	126 MB	21.06.2010 11:52:01
 ICQ	11496	85,3 MB	21.06.2010 11:53:01
 IMAP	0	1,56 MB	21.06.2010 11:53:01
 MSN	23	1,73 MB	21.06.2010 11:52:01
 HTTP	844221	2,34 GB	21.06.2010 11:47:57
 Skype	6070	41,0 MB	21.06.2010 11:53:01

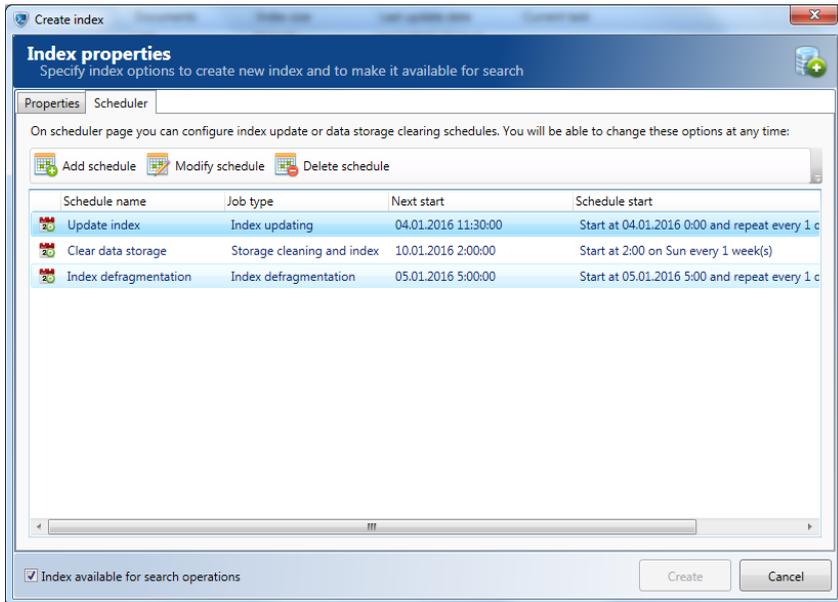
Note 1: To immediately get the index updated, click **Update index** in the **Commands** section of the **Data Indexing** settings window.

Note 2: Before starting an assisted update of a newly created index, it is important to first click **Apply changes** in the bottom right corner of the program's main window in order to apply the new index configuration. Otherwise, a dialogue box requesting applying changes will appear.

18. Click **Yes** to continue. To cancel the action, click **No**.

6.2.2 Configuring the scheduler

To set up automatic index update, defragmentation and database cleanup with index rebuilding, click the **Scheduler** tab in the index properties window.

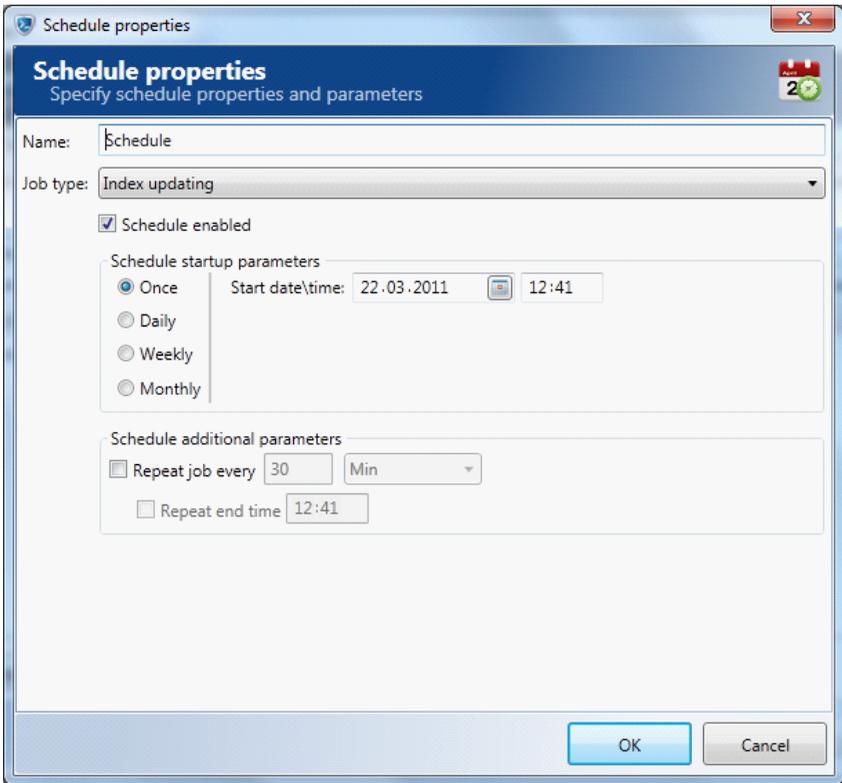


When a new index is created, three schedule records are added by default, configured to update the index every 30 minutes, empty the database once a week and defragment the index daily. These can be modified as needed, or new schedules can be created according to the instructions given in the paragraphs below.

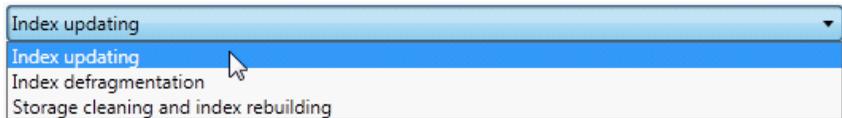
Note: *The cleanup scheduler is deleted automatically by the system upon selecting and adding the data source directly from a SecureTower database. This action provides prevention of unsuspecting data deleting from archive databases.*

Creating a new schedule

To create a new schedule, click **Add schedule**.



1. In the schedule properties window, specify the name for the new schedule in the **Name** field.
2. Click the drop-down arrow next **Job type** field and click the necessary task type in the list.



- **Index updating.** The more frequently an index is updated, the more up-to-date information is provided in the search results. However, it is not recommended to set up too frequent updates of indexes built for massive and rarely updated data arrays, as it can adversely affect system performance. Frequent index updates are appropriate for relatively small and dynamically changing data volumes (for example, IM conversations).
- **Index defragmentation.** When an indexed document (data) changes, the next time the index is updated, such document is marked as outdated and is indexed again. As a result, an index may contain references to multiple data instances that are no longer up-to-date. This increases the size of the index and slows down its

updates. When an index is defragmented, all these outdated data are removed from it, which reduces its volume, increases its update speed and data retrieval speed. This option is especially useful for indexes built for dynamically changing data, such as IM conversations. In case you select this job type, you are to specify an additional parameter – the percentage of outdated documents in the index which will trigger automatic defragmentation process. This percentage is specified in the **Start defragmentation if index defragmentation is more than** text box.

Job type: Index defragmentation

Job parameters

Start defragmentation if index defragmentation more than %

- **Storage cleaning and index rebuilding.** This job type can be used to configure the frequency of database cleanup (only the data the selected index is built for will be deleted) with subsequent index rebuilding. It is not recommended to perform this operation when network and hardware are loaded heavily, as it may take considerable time. In case you select this option, you are to specify an additional parameter – the maximum period any intercepted data can be stored in the database. This period is specified in days after the phrase “Delete information from storage older than...”.

Job type: Storage cleaning and index rebuilding

Job parameters

Delete information from storage older than day(s)

- To enable/disable the schedule select/clear the **Schedule enabled** check box.
- In the **Schedule startup parameters** section you are to specify the date and time the schedule will be started, and the frequency of performing the corresponding job:
 - **Once.** In case you select this option, the schedule will only start once on the date and at the time you specify in the right part of the section.

Schedule startup parameters

Once Start date\time:

Daily
 Weekly
 Monthly

- **Daily.** In case you select this option, specify the date and time the schedule will start for the first time, and the period (number of days) after which the selected job will be repeated, where 1 means the job will be performed every day, 2 –the job will be performed every second day, 3 –every third day, etc.

Schedule startup parameters

Once Start date\time: 22.03.2011 13:20

Daily Recurs every: 1 day(s)

Weekly

Monthly

- **Weekly.** In case you select this option, specify the date and time the schedule will start for the first time, and the period (number of weeks) after which the selected job will be repeated, where 1 means the job will be performed every week, 2 –the job will be performed every second week, 3 – every third week, etc. Also, you are to specify at least one day of the week to perform the job by checking the corresponding day boxes.

Schedule startup parameters

Once Start date\time: 22.03.2011 13:20

Daily Recurs every: 1 week(s) at:

Weekly Mon Tue Wed Thu Fri Sat Sun

Monthly

- **Monthly.** In case you select this option, specify the date and time the schedule will start for the first time.

Schedule startup parameters

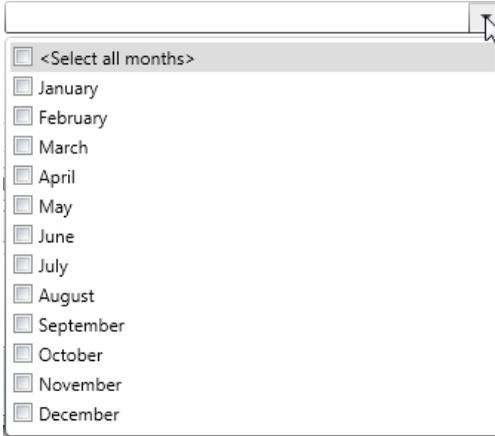
Once Start date\time: 22.03.2011 13:20

Daily Month: [dropdown]

Weekly Days: [dropdown]

Monthly In: [dropdown] [dropdown]

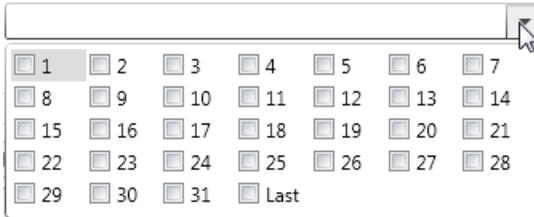
Select at least one month in the drop-down menu **Month**.



A screenshot of a web form showing a drop-down menu. The menu is open, displaying a list of months with checkboxes next to each. The options are: <Select all months>, January, February, March, April, May, June, July, August, September, October, November, and December. A mouse cursor is pointing at the top right corner of the menu.

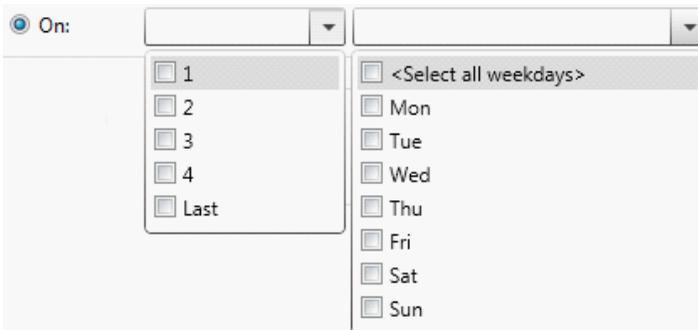
Specific days to start the schedule can be selected in two ways:

- i. switch the radio button into the first position (**Days**) and select the date(s) of the month to start the job (with “**Last**” being the last date on the month).



A screenshot of a web form showing a grid of radio buttons for selecting specific days of the month. The days are arranged in four rows and seven columns. The first row contains days 1 through 7. The second row contains days 8 through 14. The third row contains days 15 through 21. The fourth row contains days 22 through 28. The fifth row contains days 29, 30, 31, and a 'Last' option. A mouse cursor is pointing at the top right corner of the form.

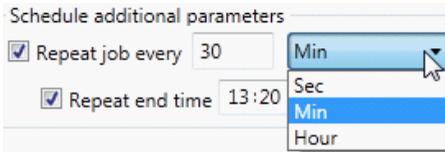
- ii. switch the radio button into the second position (**On**), select a week (or weeks) in the first drop-down menu and a day (or days) in the second one. Thus, selecting, for example, number **3** in the first list and **Thu** in the second one will mean that the job must be repeated on the third Thursday of the selected month(s).



A screenshot of a web form showing two drop-down menus. The first menu is labeled 'On:' and has a radio button selected. The second menu is labeled '<Select all weekdays>' and has a radio button selected. The first menu has options 1, 2, 3, 4, and Last. The second menu has options Mon, Tue, Wed, Thu, Fri, Sat, and Sun.

5. In the **Schedule additional parameters** section you can additionally specify the

frequency of repeating the job in seconds, minutes or hours. Also, you can define the time to stop repeating the job at.



6. After you have specified all necessary parameters, click **OK** to create the schedule. The newly created schedule will appear on the list in the **Scheduler** tab.

Modifying a schedule

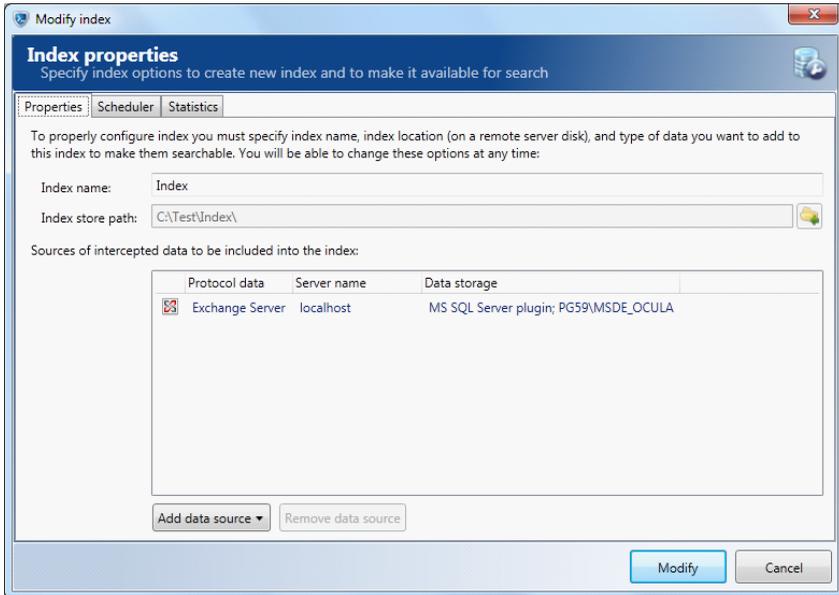
1. To modify an existing schedule, highlight its name by clicking on it in the schedule list and click **Modify schedule**.
2. Make the necessary changes according to the instructions given above in chapter [Creating a schedule](#).
3. Click **OK** to apply your changes.

Deleting a schedule

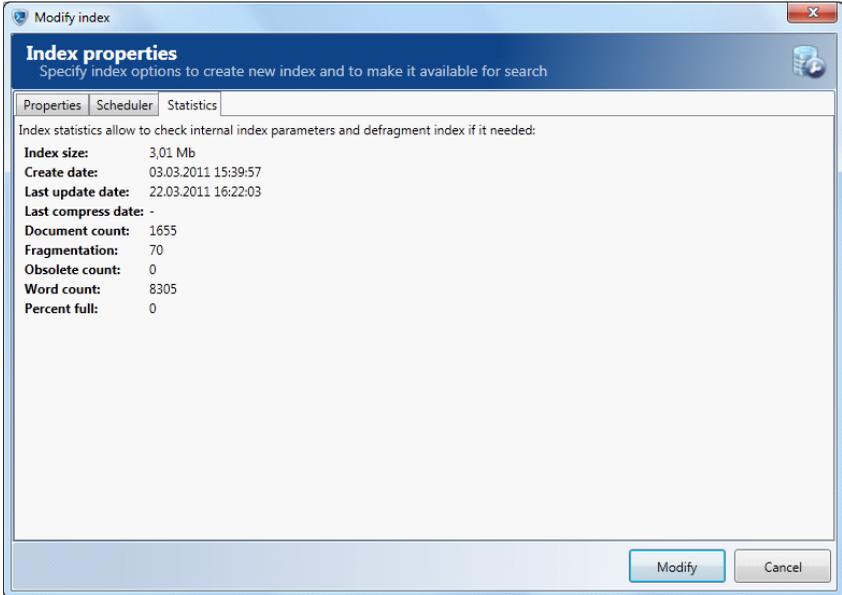
To delete a schedule, highlight its name by clicking on it in the schedule list in **Scheduler** tab of the index properties window and click **Delete schedule**.

6.3 Modifying a search index

1. To modify a certain index, select the necessary index from the list of available indexes in the [Data Indexing](#) settings window and click **Modify index** in the **Data indexing** settings window toolbar.
2. In the **Modify index** window fields, enter the necessary changes: index name, store path, sources of data included into the index, and scheduler parameters. *Detailed guidelines as to the configuration of index parameters are provided in section [Creating a search index](#) of this Guide.*



3. The **Statistics** tab displays detailed information about the current state of the selected index, including index size, date it was created, last update and last compress dates, defragment count, fragmentation percentage, number of obsolete data instances, word count and used share of index capacity. The statistical information help to assess the internal state of the index and deciding whether it needs defragmentation.



4. After you have made the necessary changes, click **Modify**.

6.4 Deleting a search index

1. To delete a certain index, select the required index from the list of available indexes and click **Delete index** on the toolbar.
2. In the action confirmation dialogue box, click **Yes**. The deleted index will disappear from the list of available indexes.

6.5 Updating index

1. To immediately get an updated index, select the required index from the list of available indexes and click **Update index** on the toolbar.
2. In the action confirmation dialogue box, click **Yes**.

Note 1: The presence of the icon below indicates that the index update is currently in

progress:



Note 2: Before starting an assisted update of a newly created index, it is important to first click **Apply changes** in the bottom right corner of the program's main window in order to apply the new index configuration. Otherwise, a dialogue box requesting applying changes will appear.

3. Click **Yes** to continue.

6.6 Clearing a search index

1. To clear the contents of a certain index (which is to delete the documents with indexed data from the index), select the required index from the list of available indexes and click **Clear index** on the toolbar.
2. In the action confirmation dialogue box, click **Yes**. All the parameter fields of the cleared index will have a "0" value.

7 Setting up digital fingerprints

To create and configure digital fingerprint data banks click the **Data indexing** tab on the left sidebar of the program's main window. Then click the **Digital fingerprints** tab in the **Data indexing** window.

7.1 Creating Data Banks

To use the digital fingerprint technology for monitoring sensitive document transmission, you need to create a databank of such documents' digital "snapshots".

SecureTower enables creating two major types of digital fingerprints:

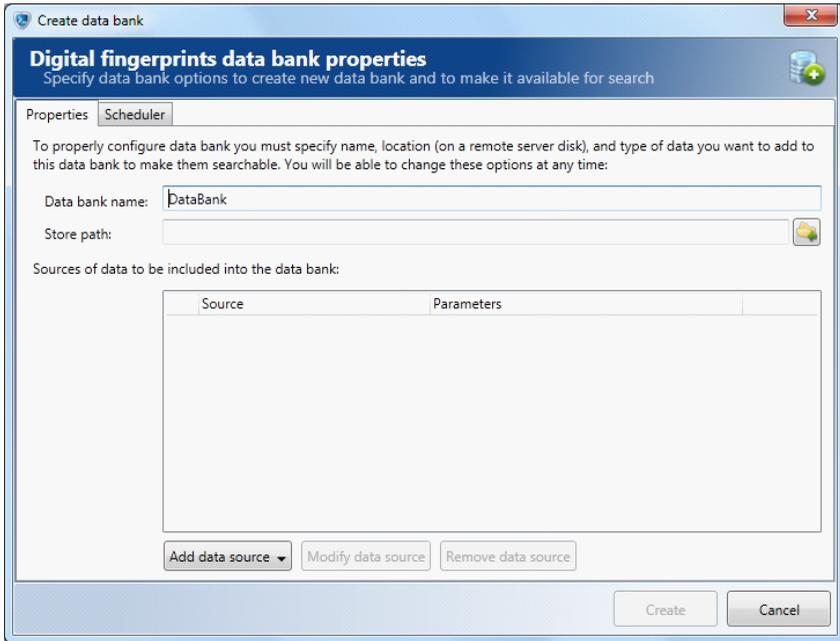
- **by files and folders;**
- **by database entries** (including CSV files).

Provided there is a databank of the classified documents' fingerprints and properly configured security rules (in the **Security Center** of **SecureTower Client Console**), the system compares each intercepted document with the fingerprint databank and notifies a security officer in case it detects the predefined match percentage. The adjustable match percentage is the main criterion to assess the level of confidentiality of a transmitted document.

To create a databank, click **Create digital fingerprints data bank** and follow the recommendations below.

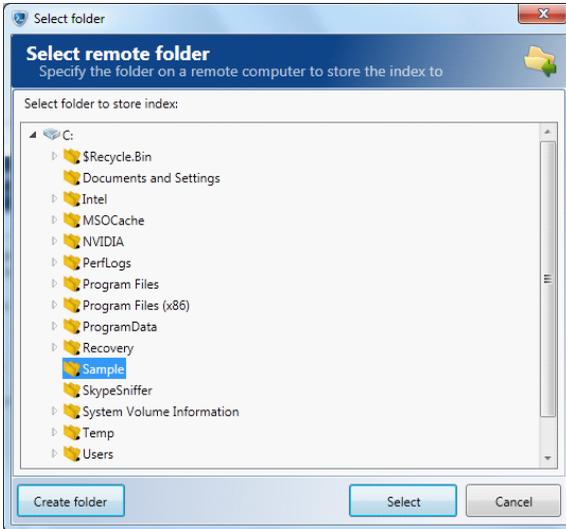
7.1.1 Setting up data bank parameters

1. In the **Properties** tab of the newly opened window enter the name of the new databank into the text field **Data bank name**.

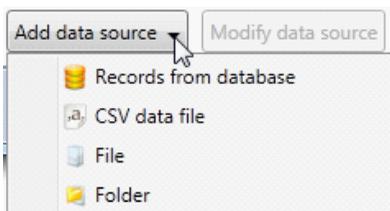


2. Enter the full path to the directory on the remote server, where the new databank will be stored. The directory can also be selected by clicking the button , located to the right of the **Store path** text field. (Select the desired directory in the folder selection window and click **Select**. To create a new folder in the current directory click **Create folder**, specify its name and click **Create**.) To cancel folder selection click **Cancel**.

After you have specified the directory that will be used for databank storage, click **Select**.



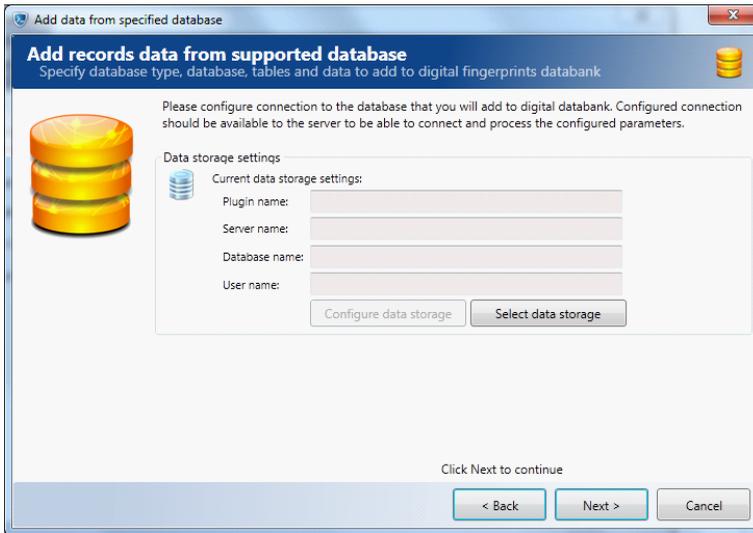
3. Next you are to specify data sources to create digital fingerprints of. To do this, click **Add data source** in the lower part of the databank creation window and select a data source.



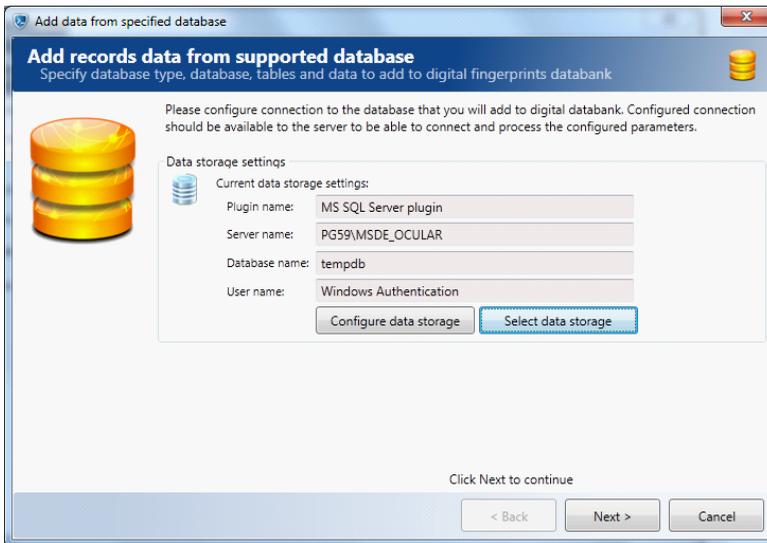
There are four options to select from: records from database, CSV data file, file and folder. One databank can contain several data sources. To create digital fingerprints of database records, choose the option **Records from database** and proceed to [paragraph 4](#). To create a digital fingerprint of a CSV file, choose the option **CSV data file** and proceed with [paragraph 11](#). To create a digital fingerprint of a single classified document, choose the option **File** and proceed with [paragraph 19](#). To create a digital fingerprint of a folder containing confidential data, choose the option **Folder** and proceed with [paragraph 20](#).

4. Creating digital fingerprints of database records.

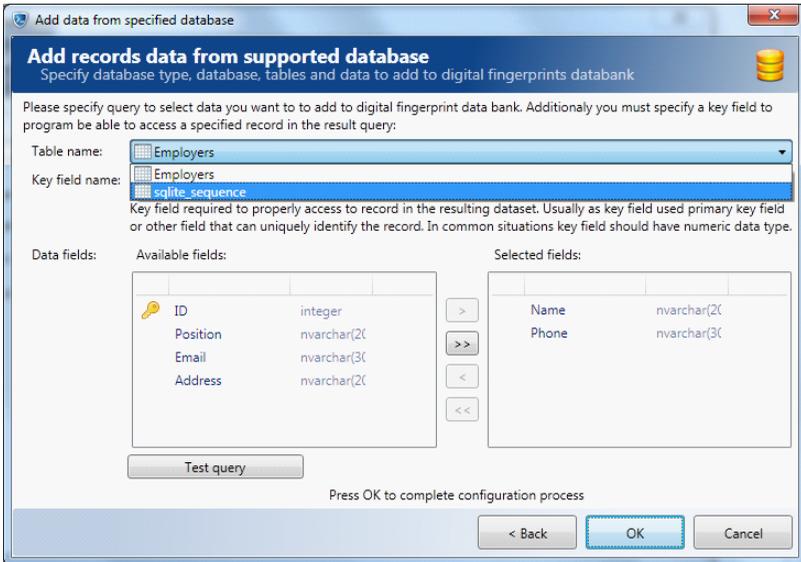
If you have chosen the **Records from database** option, a window will open in which you have to set up your data storage. To specify the database you need to create digital fingerprints for, click **Select data storage** and refer to section [Selecting data storage type](#) for detailed instructions on selecting a database.



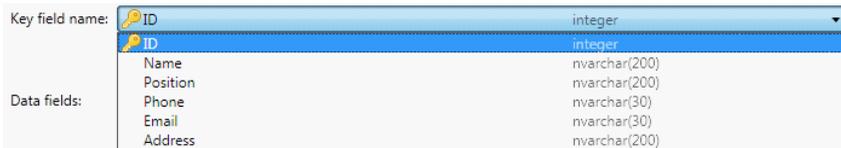
5. Click **Next** to continue



6. Select a table from the database that will be added to the digital fingerprints bank in the **Table name** drop-down menu.



7. Select the key field of the table from the drop-down menu **Key field name**.



8. All available fields of the selected table will be displayed in the **Available fields** box.



9. In this area you have to select the fields containing data the system will search for in the intercepted traffic and send notifications if any matches are detected. The combination of records from the specified table fields in the intercepted data will trigger a security breach alert. For example, if a user sends a client’s name in combination with this client’s telephone number, the **SecureTower** Security Center will send a notification to the security officer.

- To select a table field click on its title, then click button  (to select multiple fields hold down Ctrl on your keyboard and click on the fields’ titles).

- To add all available fields click button . The selected fields will appear in the **Selected fields** box.
- To remove fields from the **Selected fields** box, highlight the field and click button .
- To remove all selected fields click button .

Available fields:		Selected fields:	
 ID	integer	>	Name
Position	nvarchar(20)	>>	Phone
Email	nvarchar(30)	<	
Address	nvarchar(20)	<<	

10. To finish setup click **OK** and proceed with [paragraph 28](#). To cancel changes click **Cancel**.

11. **Creating digital fingerprints of CSV files.** If you have chosen the **CSV data file** option, a window will open in which you are to specify the details of your CSV file.

Add CSV data file

Add CSV data file to digital fingerprints databank
Specify CSV data file and file options

Please select the file that contains CSV data you need to add to digital databank. The file you specify must be accessible for the server. Don't use network mapped drives for network shares. Use UNC paths instead. To properly configure data fields specify correct field separator and additional options.

 File name: 

Field separator:

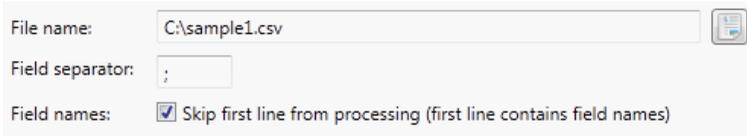
Field names: Skip first line from processing (first line contains field names)

Click Next to continue

12. Enter the full path to the CSV file into the text field **File name**. Alternatively, you can click button , located to the right of the text field, selects the CSV file in the file opening window and click **Open**.

13. Enter the symbol used in the selected CSV file to separate data fields into the text box **Field separator** (for example, comma, semicolon etc.).

14. To skip the first line of the CSV file from processing, check the corresponding check box (the first line is skipped by default as it contains field names).



15. Click **Next**.

16. In the next window you have to select the fields containing data the system will search for in the intercepted traffic and send notifications if any matches are detected. The combination of records from the specified fields of the CSV file in the intercepted data will trigger a security breach alert. For example, if a user sends a client's name in combination with this client's telephone number, **SecureTower** Security Center will send a notification to the security officer.

- To select a field of the CSV file click on its title, then click button  (to select multiple fields hold down Ctrl on your keyboard and click on the fields' titles).
- To add all available fields click button . The selected fields will appear in the **Selected fields** box.
- To remove fields from the **Selected fields** box, highlight the field and click button .
- To remove all selected fields click button .



17. The **Next record** and **Previous record** buttons are used for browsing through the records contained in the selected CSV file.

Available fields:

Name - Andrew Carlson (already added)
Phone - +16178183649 (already added)
Email - andrew@gmail.com

Selected fields:

Name - Andrew Carlson
Phone - +16178183649

< Previous record Next record >

18. To finish the CSV file selection process click **OK** and proceed with [paragraph 28](#). To discard changes click **Cancel**.

19. **Creating digital fingerprints of separate files.** If you have chosen the **File** option, a window will open in which you are to select the file you wish to create a digital fingerprint of. Select the necessary file in the file opening window, click **Open** and proceed with [paragraph 28](#). To cancel file selection click **Cancel**.

20. **Creating digital fingerprints of folders.** If you have chosen the **Folder** option, a window will open in which you are to specify the details of the folder name and additional parameters.

Add folder

Add folder to digital fingerprints databank
Specify folder, options and file types

Folder name:

⚠ The folder you specify must be accessible for the server. Don't use network mapped drives for network shares. Use UNC paths instead.

Include subfolders

File types: All supported file types (doc, html, txt and etc)
 Specified below file types (comma separated list):

OK Cancel

21. Enter the full path to the folder into the **Folder name** text field or click button , located to the right of the text field, select the folder containing classified data and click **OK**.

Note: The specified folder must be accessible from the physical server on which the software server component of **SecureTower** is installed. Please. Note that it should be accessible for the user account under which **SecureTower** Data Processing Server is started (see **Services** section of Administrator Console – **Data Processing server – Service startup parameters**).

22. To make digital fingerprints of all documents contained in all subfolders of the selected folder, check the corresponding check box.

Include subfolders

23. In the **File types** section choose one of the two available options: **All supported file types** or **Specified below file types**.

File types: All supported file types (doc, html, txt and etc)
 Specified below file types (comma separated list):

24. In case you choose **All file types**, digital fingerprints will be created for all files in the specified folder that are supported by **SecureTower** (doc, html, txt etc.).

25. In case you need to create digital fingerprints for certain file types only, select the option **Specified below file types** and enter the desired file types separated by commas into the text box in the lower part of the window.

Specified below file types (comma separated list):

txt, doc

26. Click **OK**.

27. To configure scheduler parameters, refer to section [Configuring the scheduler](#).

28. After you have specified all the necessary parameters, click **Create** in the data bank setup window.

29. The newly created data bank will be displayed in the list of data banks on the main application window.

Digital Fingerprints
On this page you can create, configure and delete digital fingerprints data banks

Create data bank
 Modify data bank
 Delete data bank
 Update data bank
 Clear data bank

Data bank name	Documents	Data bank size	Last update date
DataBank	3	8,29 KB	10.02.2011 16:09:30

30. To apply the settings you have specified for the newly created data bank and start updating it click **Apply changes** in the lower right corner of the main application window and then **Update data bank**, located over the data banks list.

Note 1: For instant update of the databank you can click **Update data bank** in the digital fingerprints setup window.

Note 2: Before starting a forced update of a newly created databank you have to click **Apply changes** in the lower right corner of the main application window to save your settings. Otherwise, a dialog box will pop up suggesting applying the changes. Click **Yes** to continue or **No** to cancel saving the new settings.

7.1.2 Configuring the scheduler

To set up automatic update of the databank, click the **Scheduler** tab in the data bank creation window.

Note: When a new data bank is created, a schedule record is added by default and configured so as to update the data bank every 30 minutes. The schedule can be modified as needed, or new schedules can be created.

Scheduler configuration for digital fingerprint data banks is similar to that for intercepted data indexes (refer to section [Configuring the scheduler](#) for details).

7.2 Other operations with data banks

Modifying a data bank

To change any parameters of a data bank, select it in the data bank list and click **Modify data bank** in the upper toolbar. A data bank properties window will open in which you can change all necessary parameters (refer to section [Creating Data Banks](#) for details).

Click **Modify** to apply changes. The **Statistics** tab of the data bank properties window displays the detailed information about the selected data bank. The statistics include: index (data bank) size, date it was created, last update and last compress date, document count, fragmentation percentage, number of obsolete data instances, word count and used share of data bank capacity. These parameters enables assessing the internal state of the data bank and deciding whether it needs defragmentation.

Deleting a data bank

To delete a data bank, select it in the data bank list and click **Delete data bank** in the upper toolbar.

Confirm your intention to delete the data bank by clicking **OK** in the dialog box.

Forced update of data bank

In addition to automatic data bank updates configured in the **Scheduler** tab, there is an option to update a data bank manually. To do this, select the data bank you wish to update in the list and click **Update data bank** in the upper toolbar.

Confirm your intention to start forced data bank update by clicking **OK** in the dialog box.

Clearing a data bank

When a data bank is cleared, all digital fingerprints of confidential data it contains are deleted. In case you need to empty a data bank, select it in the data bank list and click **Clear data bank** in the upper toolbar.

Confirm your intention to clear the data bank by clicking **OK** in the dialog box.

8 Configuring files hash banks

Checksum calculation is used by **SecureTower** to find coincidences between files on user computers and files which hashes are stored in system. Hashes are calculated by system for sensitive files which should be controlled in terms of information security. To store hashes the data banks are used.

SecureTower enables user to configure a data bank for two types of objects:

- **folder;**
- **file.**

Note: *To receive notifications about coincidence, add corresponding security rule in Security Center of **SecureTower** Client Console. The agent will scan file systems of specified computers and generate alerts if the files coincidences is found.*

To create and configure data banks:

1. Click the **Data indexing** tab on the left sidebar of the program's main window.
2. Click the **Files hash banks** tab of the **Data indexing** window.
3. Select files or folders that are significant for information security and which copies presence on the network workstations should be monitored. See the recommendations from [Creating Data Banks](#) for hash data bank configuring.

 **Attention:** *To monitor coincidences between user files and files from data banks, the [file system control](#) and [indexing of workstation](#) must be configured as well.*

9 Setting up system events and notifications

System events and notifications service is provided by Health Monitor Server and used for monitoring and control of the system server components performance. The service delivers notifications when any server events is occur.

Administrator Console make it possible to inspect server events (such as server start or errors occurring), as well as set up delivery of notifications to a specified e-mail address in case of a certain type of event (information, warning or error events).

To view and configure the system events and notifications service, select the **Events & Notifications** tab in the left sidebar of the program's main window.

9.1 System events

To access system events, click the **System events** tab in the **Events & Notifications** window. The total number of fixed events is displayed next to the tab header.

In the **System Events** window, the list of events is provided with the following parameters: event level (information, warning or error), event time and event message text.

Date	Level	Events on computer	Type	Machine name
21.10.2015 15:02	✘	License issue refused	License server	pg6.pg.local
21.10.2015 15:01	✘	License issue refused	License server	pg6.pg.local
21.10.2015 15:01	✘	License issue refused	License server	pg6.pg.local
21.10.2015 15:00	✘	License issue refused	License server	pg6.pg.local
21.10.2015 15:00	✘	License issue refused	License server	pg6.pg.local
21.10.2015 15:00	ⓘ	Active Directory structure cache was changed	Users server	pg6.pg.local

Event full description

Users server (pg6.pg.local)

Active Directory structure cache was changed. - 21.10.2015 15:00:03

Description: Active Directory structure cache was changed and all system components was notified about changes.

Original message: Active Directory cache structure changed...

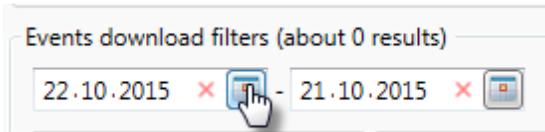
Configure display mode:

1. To view a full event description select an event in the list and click the corresponding row. The event full description will be displayed in the corresponding section under the list of events.
2. To arrange the entries (alphabetically or vice versa –for letter symbols, in the ascending or descending order –for numeric values) in the list by the particular attribute, click the corresponding column header. The icon on the column header represents the currently applied order:  - descending;  - ascending.
3. To sort the events displayed in the list, use the available set of filters as described in the [Filtering](#) section.
4. To export or print the comprehensive list of events follow the recommendation given in the [Export](#) section.

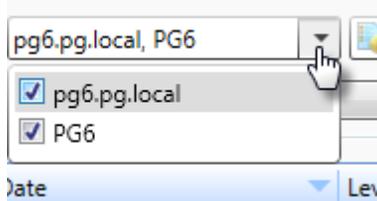
Filtering

To filter system events in the list:

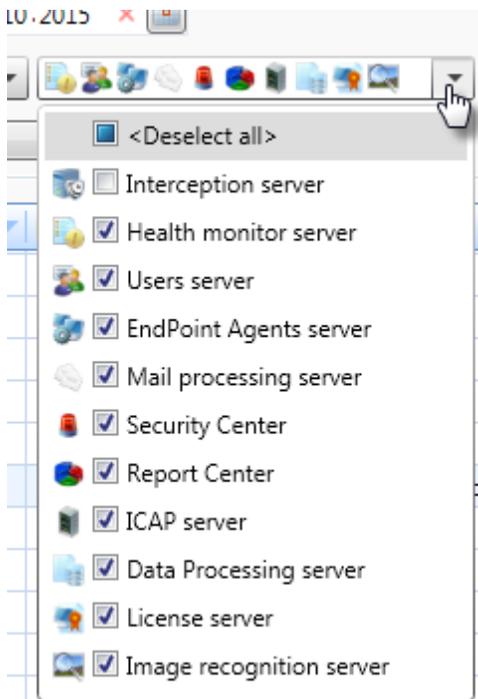
1. Click **Filter** on the window toolbar.
2. To display the events only for particular date interval, click the calendar icons next to the fields with start and end of interval and select the necessary dates.



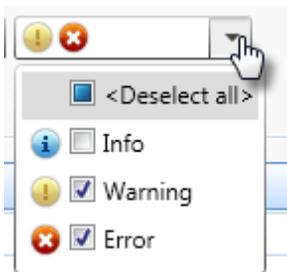
3. To select computers which server events should be displayed in the list, click drop-down arrow of the corresponding field and clear to exclude or select to include to the list the necessary computer name check box.



4. To select server components which events should be figured in the list, click drop-down arrow of the corresponding field and clear to exclude or select to include to the list the necessary server check box. Click **Deselect all** to clear all the check boxes.



5. To select the level of events that should be displayed, click drop-down arrow of the corresponding field and clear to exclude or select to include to the list the necessary level check box.



6. Click **Apply filters** to finish and display the resulting list of events or click **Reset to default** to cancel all changes.

Exporting

To export list of events as well as to print or send by email click **Export** on the toolbar.

9.2 System notifications

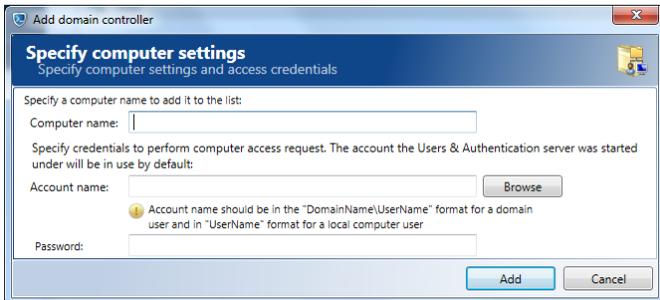
To configure custom settings of notifications or familiarize with default settings, select the **Event notifications** tab in the **Events & Notifications** window.

Selecting computers for monitoring

One can specify the list of computers to detect the **SecureTower** server events on it. If any server event occurs the system will made a record to the system events log and send a corresponding notification to email in accordance with created rules.

To add a workstation to the list of monitored computers, in the **Computers** section:

1. On the section toolbar, click **Add computer**.



2. In the **Computer name** text field type the name of the workstation which server events must be monitored and the email notification about the events must be send as well.
3. If the system account under which the Users&Authentication server is started has no access to the specified computer, in the corresponding text field, type the account

name with access rights or click **Browse** and select the necessary one from the Active Directory structure. Specify the password for the account name in the corresponding text field. For more details on selecting user account, see [Selecting a user account to start up](#).

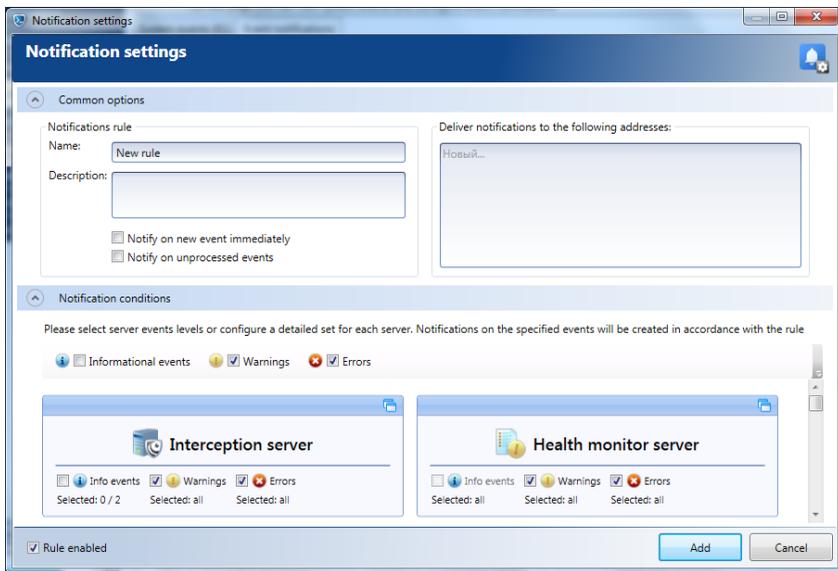
4. Click **Add** to finish.

Use the corresponding buttons on the section toolbar to modify computer settings or delete it from the list.

Configuring email notifications

To configure rules and conditions of notifying, in the **Notification conditions** section:

1. Click **Add rule**.



2. In the **Common options** section of the **Notification settings** window, type a rule name and description in the corresponding text fields.

3. If it's necessary to send a notification when any new event is occur, select the **Notify on new event immediately** option. Herewith, if the event repeats more than one time during an hour, only the first one will be classified as new. Notifications about all following identical events will be send in the end of the hour. Otherwise, if the option is unchecked the notification about every event will be send.

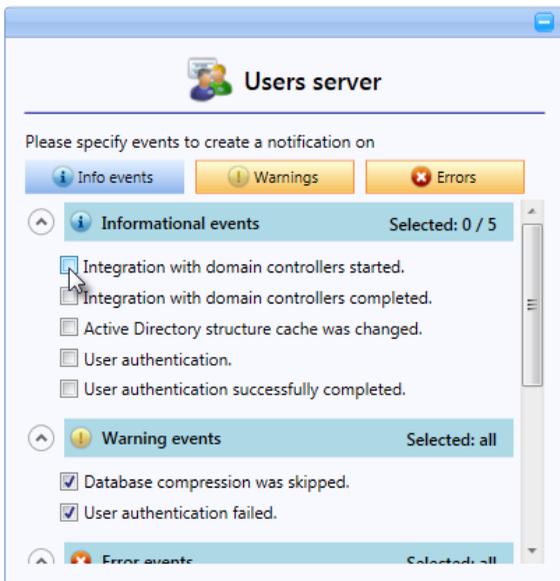
4. If it is necessary to send notification about event that happened while service failure, select the **Notify on unprocessed events** option. Herewith, the notifications about events which occurred during the time of failure will be send after service recovery.

5. Type the email address to which the notifications on the rule will be send.

6. In the **Notification conditions** section, select check boxes according to the event level it's required to be notified about.
7. To set a level of events and select the particular server events for a particular server, click the detailed choice button  on the server dashboard.

Click the necessary level button to select all events with corresponding level.

To select a particular event, select the corresponding check box.



8. Click **Add** to finish rule configuring.

Use the corresponding buttons on the section toolbar to delete a rule from the list or to change it settings.

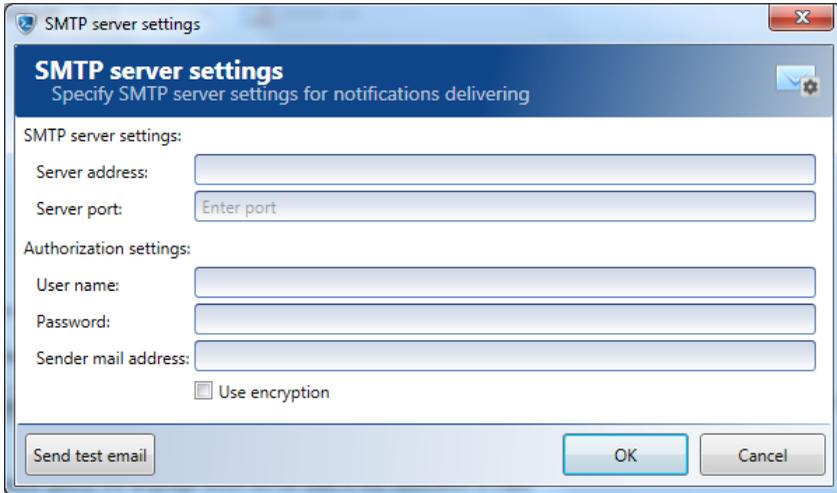
9.3 General settings

To configure SMTP server, language of notifications and auto cleanup of database, click the **Server settings** tab in the **Events& Notifications** window.

Configuring SMTP server

1. To configure SMTP server for notifications delivering:
2. Click the **SMTP server settings** button.
3. In the **Server address** text box of **SMTP server settings**, enter the IP address or name of the server that will be used for sending e-mail messages with system notifications. For example, to enable message delivery with the help of a local mail client, the IP address

or name of a local mail server should be entered. Specify the port of the server in the **Server port** text box.



4. If SMTP server connection authorization is used, specify the user name and password of the e-mail box that will be used for sending system notifications.

Note: *User name and password should be specified only if the SMTP server requires authorization. Otherwise, these fields can be left blank, provided that the server is accessed under the local domain account (Active Directory) and the system notification service has the necessary rights to access the mail server. The latter can be done in the Windows Services section: specify the user name that the system notification service will be running under and assign the required mail server access rights.*

5. In the **Sender mail address** text box, enter the e-mail address that will be used for sending system notifications. If using encrypted connection is necessary, check the **Use encryption** option.
6. To check, if the notification settings are configured properly, click **Send test email**. In case of a successful test completion, a test message will be delivered to the specified e-mail address.

Selecting a notification language

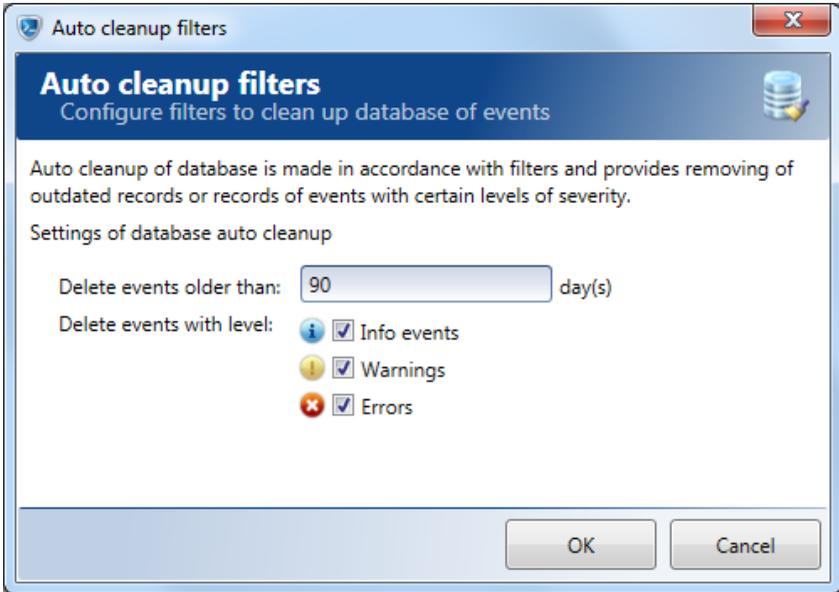
To set a language that will be used for notifications, click the button with preset language and click the necessary one in the list.

Scheduling automatic database cleanups

To enable automatic database cleanup and to configure a schedule of cleanup:

1. Select the **Enable database auto cleanup** check box.

2. Click **Settings of database auto cleanup**.



3. Enter the period of storage of entries about events in the corresponding text box. After expiration of the specified period starting from entries creation, the entries will be deleted from the database.
4. Select check boxes related to events levels that must be filtered. Only the events with selected levels will be deleted from the database after expiration date.
5. To save settings, click **OK**.

10 Setting up user identification service

The program applies a user card system in which each local network user is assigned with an **identification card** containing personal and contact user information (name and last name, job title, e-mail addresses, ICQ UINs, user accounts in IM programs, user names in social networks, etc.). The user database is developed and maintained by an administrator with the help of Administrator Console.

Besides, user cards provide group membership information. As well as user cards, the **user groups** are created with Administrator Console tools and each of group is assigned with certain user rights. Groups can be created by analogy to the organization structure of a company and may represent its structure departments. The program also provides built-in user groups (“Administrators” and “Users”).

To create, view and modify user cards and user groups, select the **User & Authentications** tab in the left sidebar of the program’s main window.

10.1 General settings

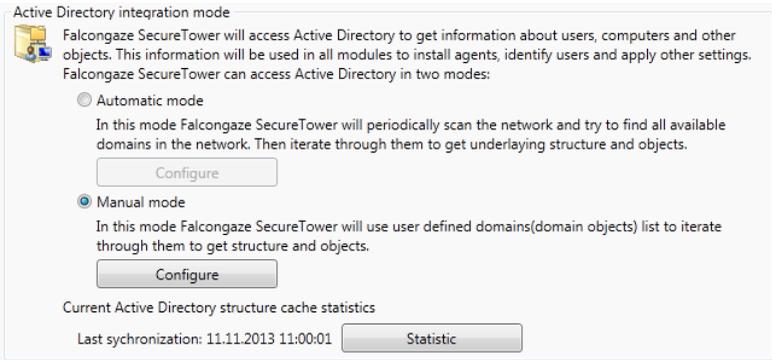
To set up system user authentication and synchronization, select corresponding tab of the **Users & Authentication** window.

 **Attention:** *While operation with user data applied due to Active Directory integration (user synchronization, automatic assignment of user contact information, a new user card creation for unknown user) only the data from the cache of Active Directory are considered. If any changes within Active Directory structure were made in the period between cache updating and such operation, the operation will be performed without taking this changes into account. To take the non-fixed in cache changes of AD structure into account, [update Active Directory structure manually](#) before implementation the operations with user data .*

10.1.1 Active Directory and domains integration

Active Directory integration

SecureTower provides automatic and manual modes of integration with Active Directory structure.

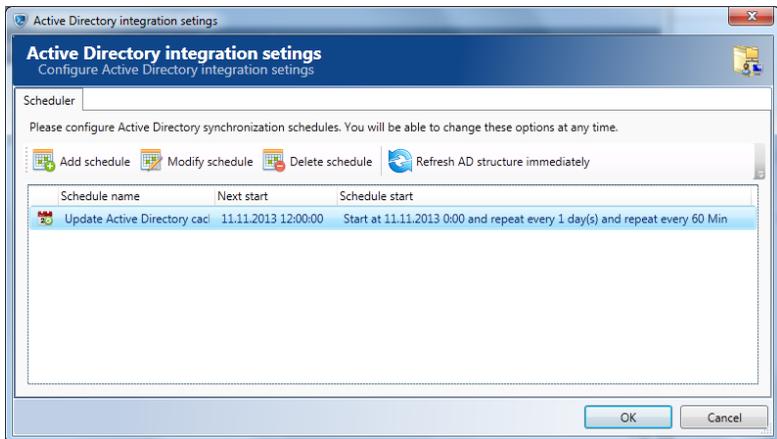


The integration feature enables choice of AD objects (for example, domain, sub-domain, organizational unit) to synchronize user information with. The function is useful for domain controller load decreasing and to speed up system feedback upon AD structure modifying for complex networks.

To choose and configure an integration mode select a necessary option.

Automatic mode

1. Select the **Automatic mode** option to perform integration with all available AD domain automatically. An automatic synchronization of user information will be performed in accordance with settings that are specified in the **Automatic Active Directory user synchronization** section.
2. Click **Configure** to specify preferences of synchronization schedule.



3. To update user information immediately, click **Refresh AD structure immediately** on the command bar.

4. To specify customer schedule properties, click **Add schedule** to add a new one.
5. In the newly opened window, specify the name for the new schedule in the **Name** field.
6. To enable/disable the schedule select/clear the **Schedule enabled** box.
7. In the **Schedule startup parameters** section you are to specify the date and time the schedule will be started, and the frequency of performing the corresponding job.

Select the necessary option and specify conditions for it:

- **Once**. In case you select this option, the schedule will only start once on the date and at the time you specify in the right part of the section.

Schedule startup parameters

Once Start date\time: 22.03.2011 13:20

Daily

Weekly

Monthly

- **Daily**. In case you select this option, specify the date and time the schedule will start for the first time, and the period (number of days) after which the synchronization will be repeated, where 1 means the job will be performed every day, 2 – the job will be performed every second day, 3 – every third day, etc.

Schedule startup parameters

Once Start date\time: 22.03.2011 13:20

Daily Recurs every: 1 day(s)

Weekly

Monthly

- **Weekly**. In case you select this option, specify the date and time the schedule will start for the first time, and the period (number of weeks) after which the synchronization will be repeated, where 1 means the job will be performed every week, 2 – the job will be performed every second week, 3 – every third week, etc. Also, you are to specify at least one day of the week to perform the job by checking the corresponding day boxes.

Schedule startup parameters

Once Start date\time: 22.03.2011 13:20

Daily

Weekly Recurs every: 1 week(s) at:

Mon Tue Wed Thu Fri Sat Sun

Monthly

- **Monthly.** In case you select this option, specify the date and time the schedule will start for the first time.

Schedule startup parameters

Once Start date\time: 22.03.2011 13:20

Daily Month: [dropdown]

Weekly Days: [dropdown]

Monthly In: [dropdown] [dropdown]

Select at least one month in the **Month** list box .

[dropdown arrow]

<Select all months>

January

February

March

April

May

June

July

August

September

October

November

December

Specific days to start the schedule can be selected in two ways:

- i. switch the radio button into the first position (**Days**) and select the date(s) of the month to start the job (with “**Last**” being the last date on the month).

[dropdown arrow]

1 2 3 4 5 6 7

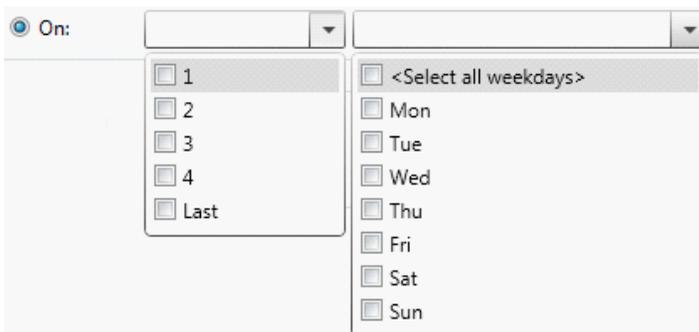
8 9 10 11 12 13 14

15 16 17 18 19 20 21

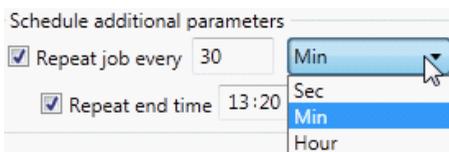
22 23 24 25 26 27 28

29 30 31 Last

- ii. switch the radio button into the second position (**On**), select a week (or weeks) in the first drop-down menu and a day (or days) in the second one. Thus, selecting, for example, number **3** in the first list and **Thu** in the second one will mean that the job must be repeated on the third Thursday of the selected month(s).



8. In the Schedule additional parameters section you can additionally specify the frequency of repeating the job in seconds, minutes or hours. Also, you can define the time to stop repeating the job at.

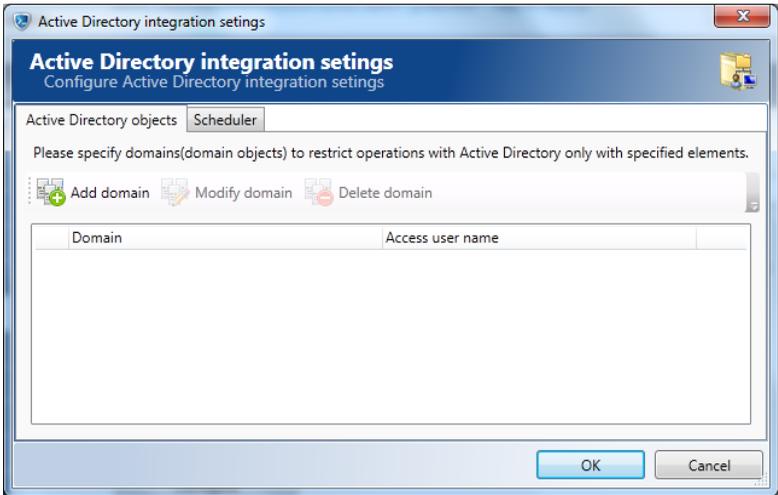


9. After you have specified all necessary parameters, click **OK** to create the schedule. The newly created schedule will appear in the list.

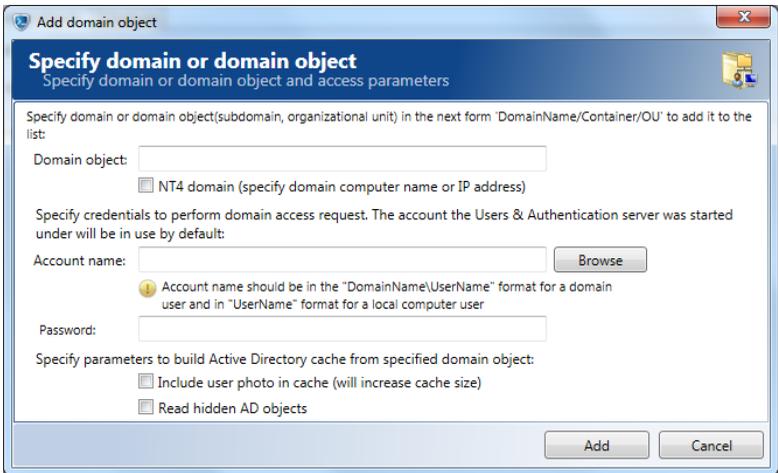
Note: *Configuring scheduler is similar to configuring a schedule for operations with data indexes (for details, see [Configuring the scheduler](#)).*

Manual mode

1. Select the **Manual mode** option to perform integration with specified AD domain objects only. Synchronization will be performed in mode that is specified in the **Automatic Active Directory user synchronization** section.
2. Click **Configure** to specify domain properties and preferences of synchronization schedule.



3. To add a new domain click **Add domain** in the **AD objects** tab of the **AD integration settings** window.



4. Specify domain or domain object name in the form: DomainName/ Container/Organizational Unit in the **Domain object** field.

5. To perform integration with domain under Windows NT 4.0 Server, select the **NT4 domain** check box.

Note: The system supports LDAP connection to Samba 4 file server and connection to Windows NT 4.0 Server as well as operating in system under Windows Server 2008/2012.

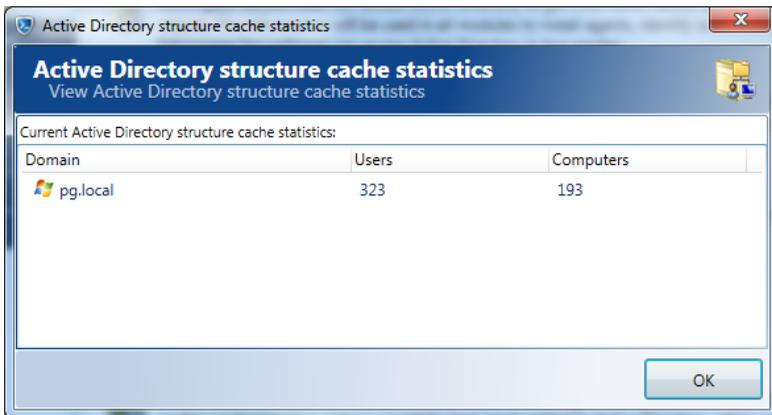
6. To perform domain access request the system will use the account the

Users&Authentication server was started under. If this account doesn't have corresponding access rights it is necessary to specify another credentials with domain access rights. Type in the **Account name** field an account name manually or click **Browse** to select the one from AD structure (for more information, see [Selecting a server startup account](#)).

7. Specify the account password in the corresponding field.
8. Select the corresponding check box to import users photos from AD while integration, if necessary.
9. Select the **Read hidden AD objects** check box to import AD objects with *ShowInAdvancedViewOnly* view properties enabled. Otherwise data for hidden objects will be skipped upon integration.
10. Click **Add** to add domain to the list of objects for synchronization.
11. Click **Scheduler** tab for synchronization schedule configuration as described [above](#).
12. Click **OK** to save integration settings.

Statistics

To view a number of objects included in synchronization process, click **Statistics**.



Automatic Active Directory user synchronization

The program can synchronize users in the program database with Active Directory users. Using the corresponding synchronization options, you can have new user cards automatically created for new users that are added into the Active Directory, the user information to be automatically updated upon any changes are introduced into the user profiles in AD, or users removed from Active Directory to

be deleted from **SecureTower** database.

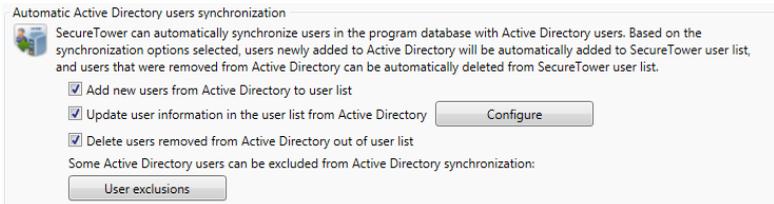
To set up these features, click the **Active Directory and Domain integration** tab in the **Users & Authentication** window and select (or clear) the following options if necessary:

- **Add new users from Active Directory to user list**
- **Update user information in the user list from Active Directory**
- **Delete users removed from Active Directory out of user list**

Note: *Automatic update of user information will only work for this users who have the one AD account linked to user cards.*

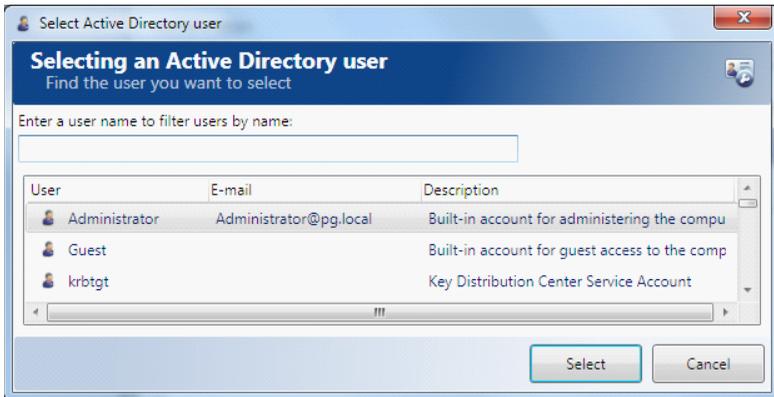
When setting up automatic synchronization of Active Directory users data with system database, you can specify excluded users whose data changes will be ignored during this process.

Update process for system users information can be configured as well.

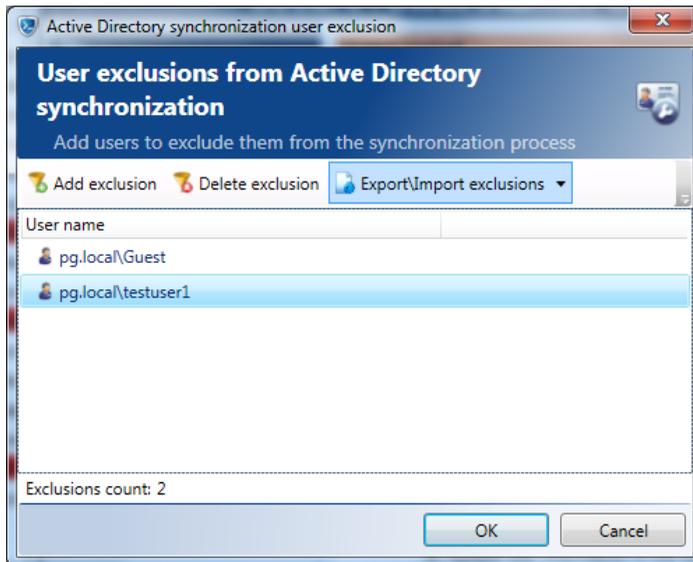


To exclude a user from synchronization process:

1. Click **User exclusions**.
2. In the opened window, click **Add exclusion**.
3. In the **Enter a user name to filter users by name** text box, type the name of the user you need to exclude from synchronization, or select the one from the list below.



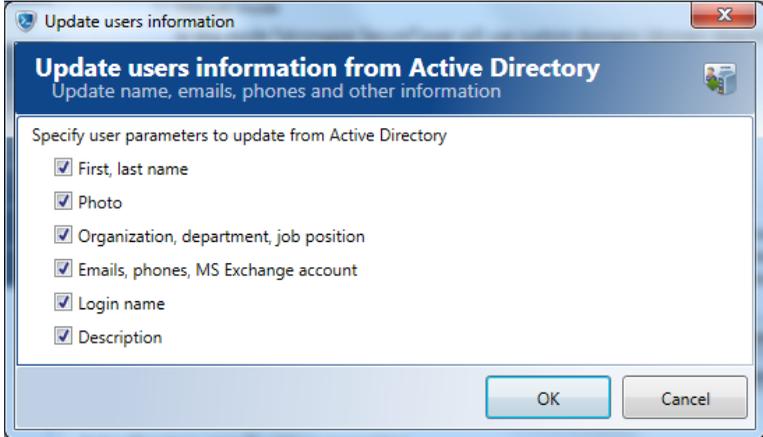
4. Click **Select**. The selected user will be added to the list of user exclusions .
5. To remove any user from the list, click the necessary user in the list and click **Delete exclusion**.



6. To save the list of existed exclusions to output file or to import previously created list of exclusions from the external file, click **Export\Import exclusions**, click the necessary command in submenu and continue with the Export\Import dialog window.
7. To save exclusions and finish, click **OK**. To discard the changes, click **Cancel**.

Configuring user info

To specify users personal data parameters which is necessary to update during synchronization, click **Configure**.



Select/clear the parameters to configure the update process. When finished, click **OK**.

Domain controllers integration

Domain controller is a server on a Microsoft Windows or Windows NT network that is responsible for allowing host access to Windows domain resources. The domain controller stores user account information, authenticates users and enforces security policy for a Windows domain.

Active Directory users IP address recognition

 Falcongaze SecureTower will connect to the Domain Controllers to get information about Active Directory user login on computers to recognize the user IP addresses. This information will be automatically added to the user cards to provide correct user linking to the intercepted information.

Enable IP address recognition

Some Active Directory users can be excluded from Domain Controllers login information processing:

Some IP addresses can be excluded from Domain Controllers login information processing:

This option allows you to create new user card if new contact information not belonging to any existing user is found. It can be helpful to automatically track new users that appear in the network

Create new user card for unknown user

This option allows you to exclude certain users from contact information auto assigning process.

SecureTower makes it possible to get information about AD users logging on workstations by appealing to domain controllers. Login information contains an IP address that will be added automatically to user card to provide correct linking of intercepted information to user account.

To start with domain controllers integration configuring in the **Domain controllers integration** section select the **Enable IP address recognition** option and click **Configure** and proceed as was described above for manual mode of domain integration.

Click **User exclusions** to exclude particular users from login information processing. Follow directions given above for automatic AD user synchronization.

Click **IP addresses exclusions** to exclude particular IP from login information processing.

In the manager window, click **Add exclusion** and follow the steps below:

1. Select the necessary IP address/range option (**Single IP address** or **IP address range**):

- If you choose the **Single IP address** option, type a specific IP address which you want to exclude.
- If you choose the **IP address range** option, type an IP range.

2. Type a description if necessary in the corresponding field.
3. Click **Add** to add the IP data to the list of exclusions .
4. To remove any IP from the list of exclusions, click the necessary one in the list and click **Delete exclusion**.
5. To save the list of existed exclusions to output file or to import previously created list of exclusions from the external file, click **Export\Import exclusions**, click the necessary command in submenu and continue with the Export\import dialog window.
7. To save the exclusions settings and finish, click **OK**.

Automatic assignment

The system provides an automatic assignment of user data and a new user card creation, when a new contact information which not belongs to existing user is found. To enable automatic assignment, select the **Create new user card for unknown user** check box.

When setting up automatic assignment, one may specify excluded users that will not be involved in the assignment processes. To include a user account into exclusions, click **User exclusions** and follow the recommendations that were given [above](#).

⚠ Attention: *While operation with user data obtained from Active Directory, only the data from cache of Active Directory are considered. If any changes within Active Directory structure were made in the period between cache updating and such operation, the operation will be performed without taking this changes into account. To take the non-fixed in cache changes of AD structure into account, [update Active Directory structure manually](#) before implementing operations with user data.*

10.1.2 Setting user authentication mode

When working with **SecureTower** either of two available authentication modes - based on Windows Active Directory user accounts or **SecureTower's** internal user authentication can be used. In the first case, user is authenticated in Client Console using the Windows Active Directory account he is currently working under. In the second case, the user will have to enter the name and password set for him in the system (refer to [User Network identification](#) for details).



The screenshot shows the 'Authentication' settings window. At the top, it states: 'SecureTower provides authentication based on Windows accounts and SecureTower internal accounts. Based on the authentication mode selected, the user will need to use either an Active Directory account or a internal user account to get access to the system functions.' Below this, there is a checked checkbox for 'Authentication enabled'. Under 'Authentication mode:', there are two radio buttons: 'SecureTower internal accounts authentication' (which is selected) and 'Windows Active Directory authentication'. Under 'Authentication options:', there are two unchecked checkboxes: 'Disable login with empty password' and 'Allow to disable users'. A note below these options states: 'Authentication module disables a user account for a several minutes if an incorrect password is entered 3 times'.

To enable user authentication, select the relevant check box. Then you are to choose one of the two options – **SecureTower internal accounts authentication** or **Windows Active Directory authentication**.

Note: *If **SecureTower internal accounts authentication** is checked, a user will have to enter the name and password on every login. The password can be changed by user after login. To change the password, on the **Tools** menu, click **Change login password** (this option is accessible with internal authentication only - [User Network identification](#)).*

If the **SecureTower internal accounts authentication** mode is checked, the following options can be set:

- **Disable login with empty password** can be set to prohibit users to login in with an empty password and to increase the security level.
- **Allow to disable users** can be set to lock a user account out for a several minutes when an incorrect password is entered 3 times.

 **Warning!** *Before you enable an authentication system, make sure that the user who will work with **SecureTower Administrator Console** is included into the **Administrators group** (or another group that has access rights to Administration Console), because after you enable user authentication and click **Apply changes** in the lower right corner of the window, access to Administration Console will be restricted to only the users who have the corresponding rights.*

Protecting the system from unauthorized changes in settings

To prevent unauthorized changes in the system settings the two-factor authentication mode is provided. When enabling, this mode obligates the console user, who made some

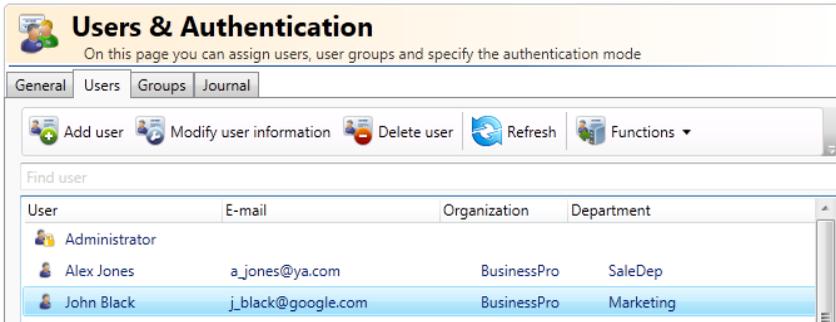
changes in the system configuration, to enter an additional secret password every time when he click **Apply changes**.

To enable two-factor authentication:

1. Select the relevant check box in the **User & Authentication** window.
2. To set the secret password, click **Set password**.
3. Enter the secret password and confirm it in the corresponding text box.
4. Click **OK**.
5. To activate the mode, click **Apply changes** in the bottom right corner of the console window.

10.2 User management

To create, view and modify user cards, select the **Users** tab in the **User identification** service window. One can add and delete user cards, edit user information and import users from Active Directory.



User information (if there are any user cards) is presented in form of a table with a list of user cards, and the data can be sorted by user names and other user information viewing and searching convenience. By clicking the corresponding column header, one can get ascending or descending sorting of users by the values in this column (alphabetically or vice versa). To search for a specific user in the list, enter the symbols that the name contains into the **Find user** text field. As you type, the list will display only those user names containing the entered symbols.

10.2.1 Creating a user card

To create a new user card, click **Add user** in the ribbon toolbar of the **Users** tab.

The **Add user** window contains the following tabs: **General**, **Network identification**, **Contact identification** and **Groups**. User information can be filled out tab by tab. When you finish entering the necessary data into a user card, click **Add** to save the changes.

10.2.1.1 General user information

In this tab one can enter the name, middle and last name of a user, the name of the organization for which they work, department, job title, contact phone number, address, employment period (dates of employment and discharge) in the corresponding fields. Besides, you can specify additional information in the **Comments text** field.

To the right of the user name field, there is the ID field which contains a unique user identification number. The ID is assigned by the system automatically after a new user card is created.

Adding a user picture

1. To provide a user with a certain *image*, click **Set image** in the right part of the tab.



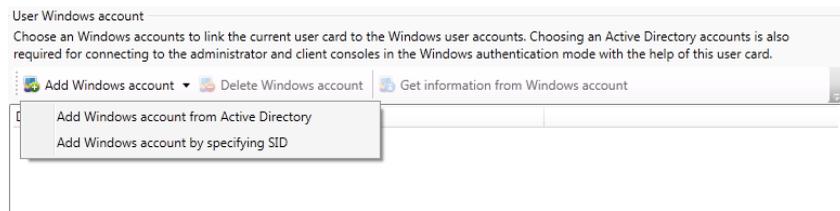
2. In the **Open file** dialogue box, specify the folder in which the necessary file is located, select it and click **Open**. The added file will be displayed in the top right corner of the **General** tab.

10.2.1.2 User Network identification

In this tab one can familiarise with the history of IP addresses usage by the current user, as well as select an Active Directory account to link it to the current user, and set user name and password for internal authentication mode.

Selecting an Active Directory account

In order to link one or several Windows accounts to the current user, click **Add Windows account** and then click the necessary type of account:



- To add account from AD, click the corresponding command, and then follow the recommendations from [Selecting a user account to start up](#) chapter.
- To add account by SID, click the corresponding command and enter user SID in the

opened dialog window. Click **Select** to save a choice.

The list of all accounts linked to the current user is displayed in the field below toolbars with the indication of the corresponded domain and account name. After you have selected an account to link to the user, you can import additional user data (contact information, department and position, and other information available for the selected account), by clicking **Get information from Windows account**. All imported data will be added to the user card automatically. To remove an account from the list, highlight the account and click **Delete Windows account**.

Internal account information

In case the internal authentication mode is used, you have to specify a name and password (both are case sensitive) that the user will have to enter to access **SecureTower Client Console**.

Internal account information

Specify internal account information to be able to use this user card for connection to the administrator and client consoles within the internal authentication mode.

Login name: jonh

Password:

Re-enter password:

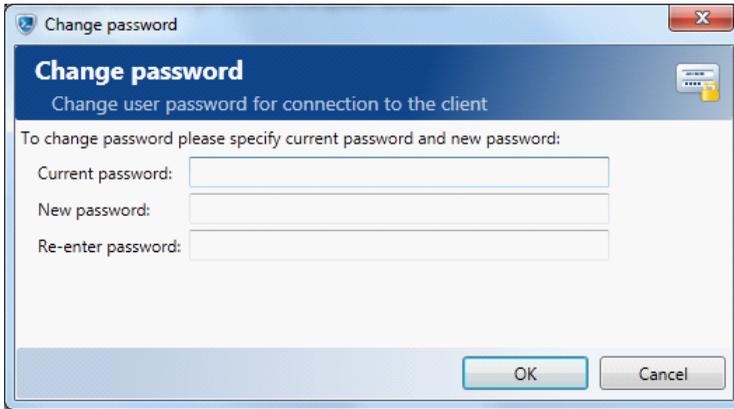
User must change the password on next logon in internal authentication mode

When the user launches **SecureTower Search Client**, he will have to enter the name and password that you have specified. To require the user to change password on next logon, check the corresponding option.

The password can be changed by the user after he has successfully logged in. To change the password, select the **Tools** menu and click on **Change login password** (this option is accessible with internal authentication only). Enter current and new password in corresponding fields. Click **OK** to confirm or **Cancel** to cancel the action.

To oblige the user to change a specified password on next logon, it is necessary to check the appropriate option **User must change the password on next logon in internal authentication mode**.

Note: If the **User must change the password on next logon** option is checked and the internal authentication mode is activated, the **Change password** window will appear after logging in.



The user will have to enter current and new passwords in corresponding fields (case sensitive).

Disabling logging

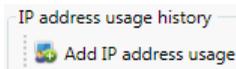
By default all users who have an account in the system are permitted to log in. This can be undesirable in certain situations.

A user account can be locked out while authentication process to prevent the user from logging in. Select the relevant check box in the **User login state** section to prohibit the user to log in. Disabling can be also set for any user who has entered an incorrect password 3 times by means of authentication module.

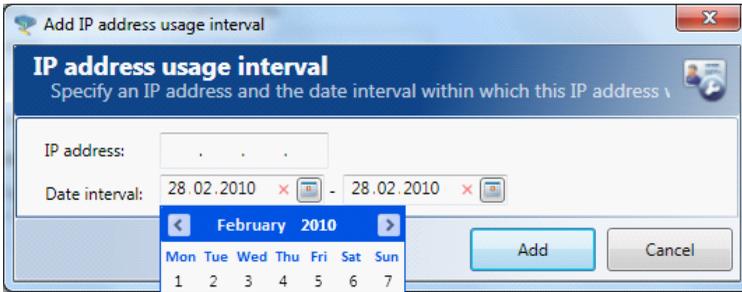
Adding IP address history

IP address usage history reflects what IP addresses were used by this user and within which time interval.

1. To *enter a record* on a certain IP address usage manually, click **Add IP address usage**.



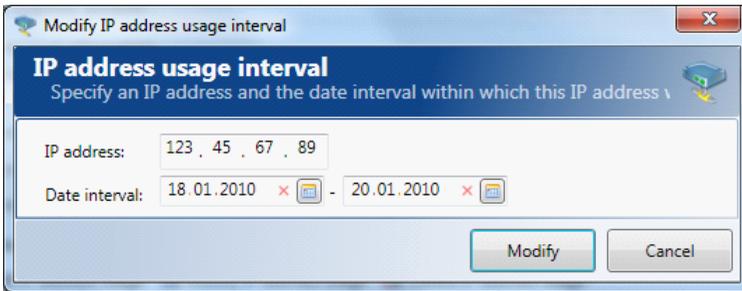
2. In the dialogue box opened, specify the necessary IP address and time interval within which it was used by the current user. Time interval can be either typed or selected in the drop-down menu opened by clicking the calendar icon. Then click **Add**.



Modifying an IP address history

To modify a record on a certain IP address usage, select the necessary record in the list of IP address usage records and click **Modify IP address usage**.

1. In the new dialogue box, make the necessary changes.
2. To apply the changes, click **Modify**.



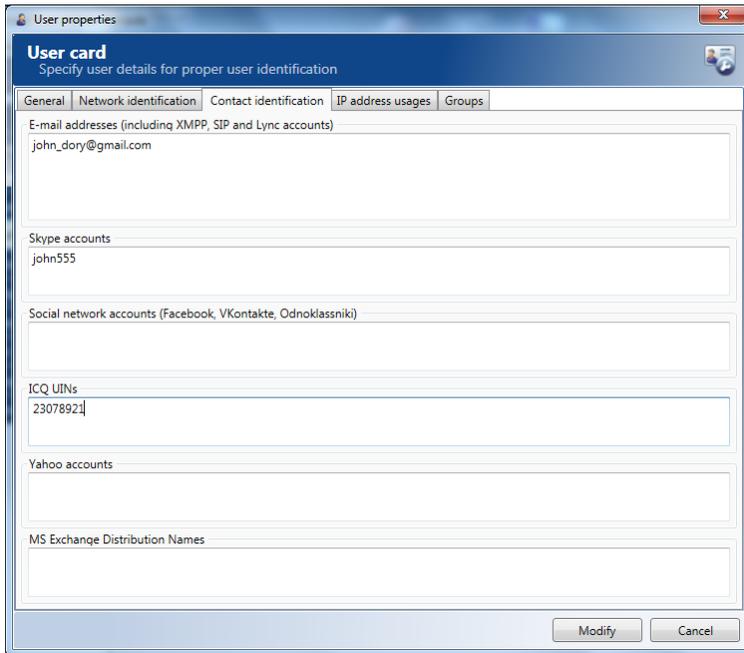
Deleting an IP address history

To *delete a record* on a certain IP address usage:

3. Select the necessary record in the list of IP address usage records and click **Delete IP address usage**.
4. In the action confirmation dialogue box, click **Yes**.

10.2.1.3 User contact identification

In this tab you can enter e-mail addresses and account names of the current user in instant messengers (ICQ, Skype, Yahoo), MS Exchange account, social network accounts, etc.



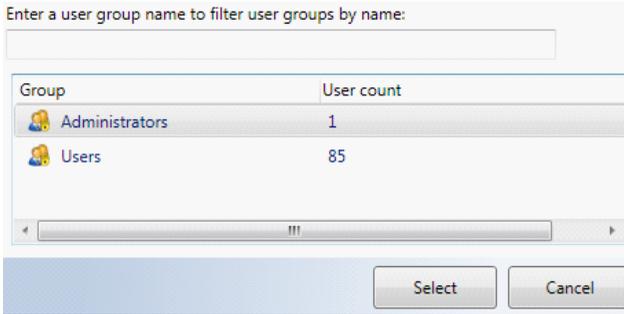
10.2.1.4 User groups

In this tab you can include/exclude a user into/from a certain group.

Including a user into a group

To include a user into some user group:

1. Click **Add group membership**.
2. In the opened dialogue window, enter the name of the required user group in the text box or select the necessary group in the list of user groups.
3. Then click **Select**. The group into which the user was included will be displayed in the **Groups** tab.



Excluding a user from a group

1. To remove some user's group membership:
2. Select the necessary group and click **Remove group membership**.
3. Click **Yes** in the action confirmation dialogue window.

The group from which the user was removed will not be displayed in the **Groups** tab.

10.2.2 Modifying a user card

To view or modify user card information:

1. Select the necessary user in the list of user cards and double-click his name or click **Modify user information** in the ribbon toolbar of the **Users&Authentication** window(see [Creating a user card](#) for details).
2. When finish modifying the user card, click **Modify** to apply the changes.

Modify user

User card
Specify user details for proper user identification

General | **Network identification** | Contact identification | Groups

First name: John
Last name: Smith
Middle name:
Organization: Business Solutions, Ltd.
Department: Sales Department
Job position: Marketing Responsible
Phones: +123456789012
Address:
Comments:

Set image

Apply Cancel

10.2.3 Deleting a user card

To delete a certain user card:

1. Select the necessary user in the user card list and double-click their name or click **Delete user** in the **Commands** section.
2. In the action confirmation dialogue box, click **Yes**.

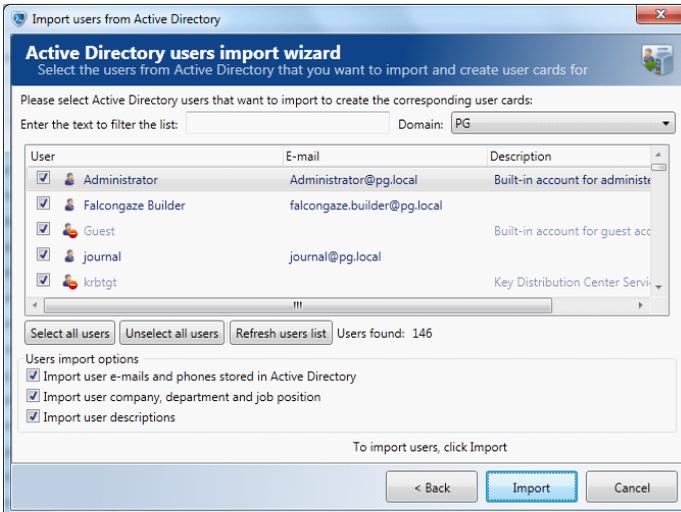
10.2.4 Importing users from Active Directory

To import users from the Active Directory domain:

1. Select **Import users from Active Directory** option in the **Functions** menu.
2. In the Import users from Active Directory wizard window, click **Next**.



3. In the users import window, select the domain from which you wish to import, and the users that should be imported by checking the corresponding boxes. To import all the users, click **Select all users**; to uncheck all the users, click **Deselect all users**. To update the list of users, click **Refresh user list**.



Note: For searching convenience, you can filter the list of users in the selected domain by

typing the corresponding symbols in the text field in the upper part of the window. As you type, the system will display only those users that have the entered combination in their names. Additionally, for viewing convenience, the user data presented in the list can be sorted by the following parameters:

- User name
- E-mail address
- Description.

By clicking the column header, one can get ascending or descending sorting of users by the values in this column (alphabetically or vice versa).

User	E-mail	Description
------	--------	-------------

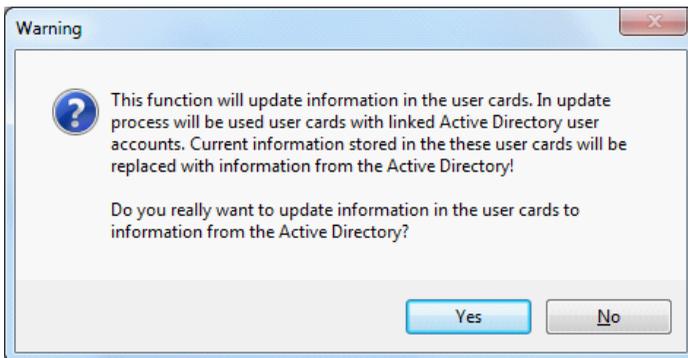
4. In the **Users import options** section, check the necessary options. To import e-mail addresses and phone numbers of the specified users, check the **Import user e-mails and phones stored in Active Directory** option. To import such data as company name, department and position, check the corresponding box. To import additional user information that is stored in AD, click **Import user descriptions**.
5. To start importing, click **Import**. Upon finishing importing, click **OK**. The imported user will be displayed in the list of user cards.

Note: To view or add information on the imported user, click their name in the list of user cards and click **Modify user information**. Detailed guidelines as to entering data into a user card are provided in section [Creating a user card](#) of this Guide.

10.2.5 Updating user information from Active Directory

To update user information contained in the user cards:

1. Select option **Update user information from Active Directory** in the **Functions** menu in the **Users** tab.



2. In the dialog window click **Yes** to confirm update.

Note: The function of user information update will work only for the users with one AD account linked to them in their user cards.

After you start this process, the user ID information (first name, last name, department, position, etc.) will be replaced with data contained in the Active Directory. User's new contact information in the AD (e-mail addresses, user accounts in messengers) will be added to the existing data (the contact information that is already recorded in the user card will not be deleted).

10.3 Managing user groups and access rights

To create, review, modify user groups and define group access rights, select the **Groups** tab in the **Users & Authentication** server window.



User groups are displayed in a table, and for searching and viewing convenience, they can be sorted by group name and by the number of users included into the group. By clicking the name of the corresponding column, you can sort the groups in the ascending or descending order of the values in this column (for a group name – alphabetically or vice versa; for a user count – in the ascending or descending order). To search for a specific group in the list, enter the symbols that the group name contains into the **Find group** text field. As you type, the list will display only those groups containing the entered symbols.

10.3.1 Creating a user group

To create a new user group follow the steps below:

1. Click **Add group** in the ribbon toolbar.
2. In the **New group** window, specify the name of the group that should be created in the **Group name** text field.

Group name: ID:

The ID field on the right contains a unique identification number of the group. The ID is assigned automatically by the system when a new group is created.

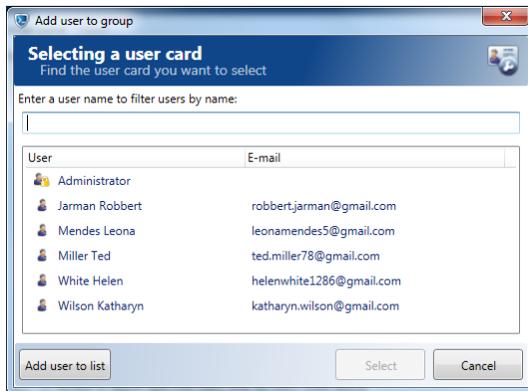
3. In the **Rights** section you can assign access rights to the group. The following options are available to configure group rights:
 - **Allow connecting to the client console** – the main option which grants access to Client Console. If this option is disabled, the group members will see a message notifying them that they do not have privileges to access **SecureTower** Client Console whenever they start the application. Enabling this option activates all other “dependent” options. Disabling this option also disables all dependent options even if the corresponding boxes were checked.
 - **Allow access to search functions** – if this box is unchecked, the Search module of Client Console is disabled (including simple and advanced search functions). This means the

group members will not be able to perform search in the interception database. Upon activating search access the following child options become available. Upon deactivating search access the child options became disabled regardless their status. To specify the particular kind of search for access proceed with the child options settings. To specify users which intercepted information is available for advanced search click **Configure** on the right of this option and specify the user list for advanced search.

Configuring of the advanced search is based on user list which include users excluded from the common settings. Set an exclusion mode by clicking a necessary radio button in the **Exclusion mode** section. Only one mode can be applied to the all items in the list:

- a. If the **Access to search in intercepted data of all users except listed above** mode is selected, the list will include the users which intercepted data is unavailable for search operations. Search in intercepted data of all other controlled users will be allowed.
- b. If the **Access to search only in intercepted data of listed user** mode is selected, the list will include the users which intercepted data is available for search operations. Search in intercepted data of all other controlled users will be prohibited.

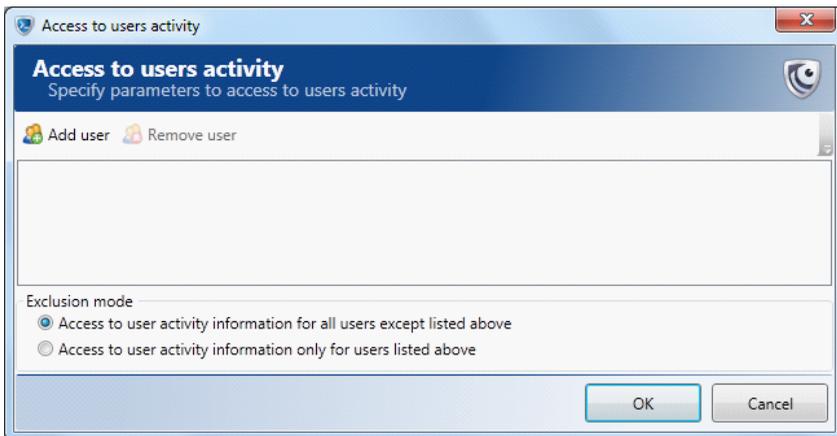
To create the list click **Add to list** and then click the necessary option in the drop-down list.



Select the necessary users (groups) in the list of users (groups) controlled by **SecureTower**:

- a. To add a user (group) from the list and finish, click the necessary user row and click **Select**.
 - b. To add a user (group) and continue the selection, click **Add user to list**.
 - c. To select and add a set of users (groups) simultaneously, select the first row of the set, press and hold Shift and click the last row of the set. Click **Select**.
 - d. To select and add a number of separate users (groups) press and hold Ctrl and click the necessary rows. Click **Select**.
- **Allow access to user activity** –if this box is unchecked, the User Activities module of Client Console is disabled, i.e. the information on users’ network activities will not be

available for the members of this group. When this option is enabled, the group members gain access to information on network activities of all users controlled by **SecureTower**. If you need to restrict access for the group members to allow them to view network activity statistics of certain users only, click **Configure** and specify the users they will be able to view network stats of.



A window will open in which you are to compile a list of users and select one of the two possible restriction modes: **Access to user activity information for all users except listed** (in this case the group members will have access to network usage statistics of all users controlled by **SecureTower**, except those you list in this window) or **Access to user activity information only for users listed above** (in this case the group members will only have access to network usage statistics of the users you list in this window).

- **Allow editing user cards** – if this box is unchecked, when opening user cards in Client Console, the group members will see the corresponding notification in the lower part of the card. In this case saving any changes to user cards made by the group members will be impossible.
- **Allow viewing Security Center rules** – if this box is unchecked, the Security Center module of **SecureTower** Client Console will be inactive, i.e. the group members will not have access to viewing and editing security rules. When this option is enabled, the following dependent option becomes active and can also be enabled/disabled. When this option is disabled, the dependent option is also disabled even if its box was checked.
- **Allow editing Security Center rules** – if this box is unchecked, when entering the Security Center of Client Console, the group members will see the following notification in the upper part of the window: “You do not have the necessary rights to edit security rules. Contact your system administrator to obtain editing rights”. In this case, the group members will only have a right to view the existing security rules and breach incidents, but will not be able to create new rules or rule groups and edit the parameters of the existing rules.
- **Allow access to Report Center** – if this box is unchecked, the **Report Center** module is disabled, i.e. reports on users’ network and computer activities will not be available for the members of this group. When this option is enabled, the group members gain

access to **Report Center** functional.

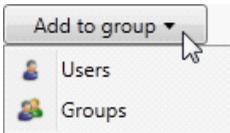
- **Allow editing Report Center reports** – if this box is unchecked, when entering the **Report Center** of Client Console, the group members will see the following notification in the ribbon toolbar of the Report Center window: “You do not have the appropriate permissions required to modify groups and reports. Contact your system administrator to obtain this permission”. In this case, the group members will only have a right to view the existing reports, but will not be able to create a new report or reports groups and edit the parameters of existing reports.
- **Allow viewing Report Center reports** – if this box is unchecked, the **Report Center** module of **SecureTower** Client Console will be inactive, i.e. the group members will not have access to viewing and editing reports. When this option is enabled, following dependent options become active and can also be enabled/disabled. When this option is disabled, the dependent option is also disabled even if its check box was checked. To grant viewing permissions for any reports type check corresponding check boxes. If you need to restrict access for the group members to allow them to view the selected type of report for certain users only, check corresponding type and click **Configure** to specify the users they will be able to view this report type of.
- **Allow access to audio/video monitoring** – if this box is unchecked, the audio/video monitoring module of **SecureTower** Client Console will be inactive, i.e. the group members will not have access to module functionality. If you need to restrict access for the group members to allow them to monitor the audio or video stream of the selected users only, check corresponding type and click **Configure** to specify the users.
- **Allow connecting to the admin console** – if this box is unchecked, the members of the group will not have access to **SecureTower** Administrator Console. To grant access rights to Administrator Console select this check box. Herewith, the members of the group will be permitted to view current settings without configuration permissions. In this case the corresponding message will notify a user about restricted access to the server settings.



- To allow the members of the group to configure any of the servers, select the corresponding option check box in the list of permissions .

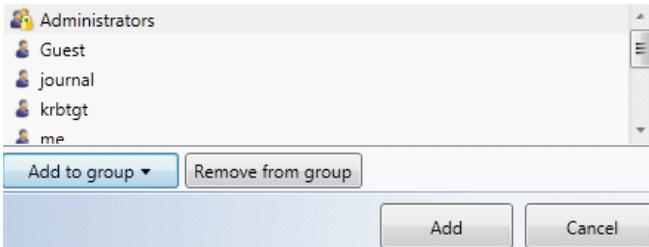
Note: In case one user is included in several user groups at once, and these groups associated with different access rights, the rights defined for all of these groups will be merged and applied to such user. The merger of group access rights is performed with the use of logical “or”, which means if one of the groups has a certain right and another one does not, as a result of access rights merger the corresponding option will be deemed enabled, and the user will be granted the respective right.

- In the **Members** section, users and sub-groups included into the group are displayed. To add a new user (sub-group) to the group, choose an option in the **Add to group** drop-down menu.



In the opened dialogue window, enter the name of the required user (group) in the corresponding text box or select the necessary item in the list. After highlighting the item, click **Select** (for details on item choice, see [above](#)).

- To remove some user (or sub-group) from the group, click the name of the user (sub-group) in the list and then **Remove from group**. In the action confirmation dialogue window, click **Yes**.
- To save the settings of the newly created user group, click **Add**.



10.3.2 Modifying a user group

To modify a certain user group:

1. Select the necessary user group in the list of groups, and then click **Modify group**.
2. In the **Modify group** window, enter the necessary changes in accordance with clauses 2-6 of section [Creating a user group](#) of this Guide, and click **Modify** to save the settings that were entered.



10.3.3 Deleting a user group

To modify a certain user group:

1. Select the necessary user group in the list of groups and click **Delete group**.
2. In the action confirmation dialogue window, click **Yes**.

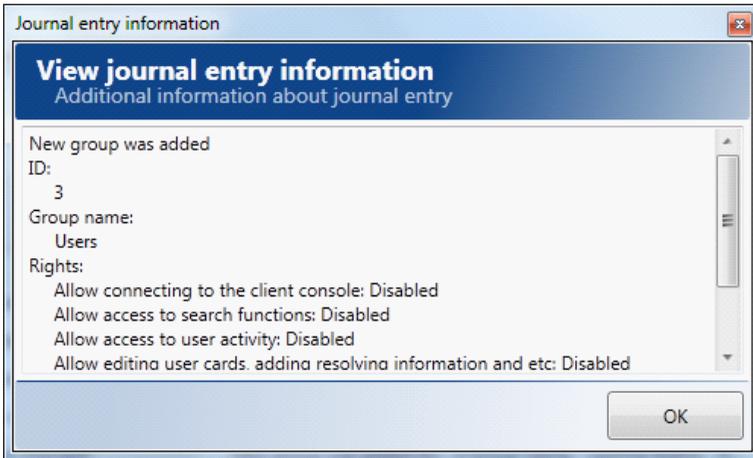
10.4 Authentication journal review

In case you use user authentication (see section [Setting user authentication mode](#)), the system will keep a log of all authentication attempts. To view this log, click the **Journal** tab.

The journal provides information on all successful and failed authentication attempts (including the time and date of the event, the ID and name of the user and the action performed) and on any user or group credentials changed.

Date	User	Action	Additional information
10/10/2011 1:02:16 PM	(82) Alex Jones	Login to admin console successfull	
10/10/2011 12:31:52 PM	(82) Alex Jones	Login to admin console successfull	
10/10/2011 12:19:29 PM	(82) Alex Jones	Login to admin console successfull	
10/10/2011 11:29:48 AM	(82) Alex Jones	User information was changed	User information was changed ID: 82 User
10/10/2011 11:11:52 AM	(82) Alex Jones	Group information was changed	New group was added ID: 3 Group name:
10/10/2011 10:12:16 AM	(82) Alex Jones	Login to admin console successfull	
10/10/2011 10:10:14 AM	(82) Alex Jones	Login to client successfull	
10/10/2011 10:09:24 AM	(82) Alex Jones	Login to client unsuccessfull: access not allowed	

The **Additional information** button in the toolbar is available for records about changed user or group information. Click this button to view additional information on such records.

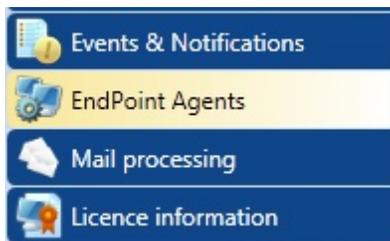


To refresh the journal records, click **Refresh** in the toolbar.

11 Configuring Endpoint Agents

Endpoint agents are used for tracking of data exchanged by Skype, Microsoft Lync users and information transferred over encrypted channels (SSL traffic) or to control usage of USB devices/ network shares and local/network printers. Administrator Console enables centralized installation and configuring of such agents.

To start the Endpoint agents' installation and configuring, select the **EndPoint Agents** tab in the left sidebar of the program's main window.



In the **Endpoint agent control center** window, you can choose an endpoint agent installation strategy, configure connection to the database where the information received from agents will be stored. Also you can monitor the performance and status of all the agents installed in the network and configure other agent settings.

Note: *SecureTower maintains parallel operation of several users with Administrator Console. However, it is necessary to keep in mind that the changes competition rule are applied in the case of the EndPoint Agent configuring: if any changes of the server settings was made and applied by one of the competitive users during parallel operation, the other users will be notified with the corresponding message upon attempting to apply their changes during the same running session lately.*

There are three possible way of the changes processing:

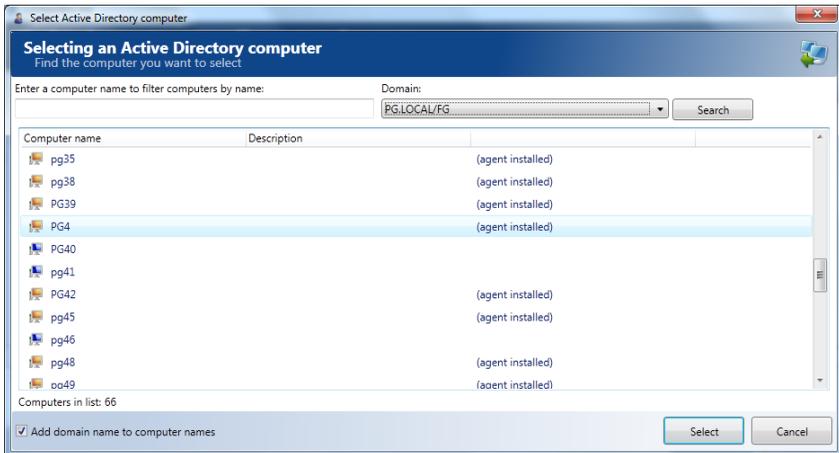
- Choose **Yes** to apply your settings changes. The current actual settings will be replaced with yours.
- Choose **No** to abort your configuring process and leave the current actual settings without changes. Herewith the actual current settings, that was applied by another user during parallel operation previously will be displayed in the console.
- Choose **Cancel** to proceed with configuring your version of EndPoint Agent settings. In this case the settings previously applied by competitive user will be actual and keep on function.

11.1 Installing endpoint agents on workstations

There are three strategy that can be used to install the system endpoint agents on workstations in the network:

- [centralized installation by SecureTower EndPoint Agent Server](#) (centralized from Administrator Console);
- [remote installation by Group Policy](#);
- [manual installation](#).

If the agent is installed on a computer, the computer name is highlighted in color and displayed with the relevant note in the list of Active Directory computers.



Agent installation specific feature

Upon the first installation of endpoint agents, those sessions that were started before the installation will not be intercepted. This occurs due to the fact that interception of a session starts upon that TCP session startup. To prevent data loss, when installation of agents is complete, restart the applications that data is necessary to intercept.

11.1.1 Centralized installation

Upon centralized installation the agents will be installed automatically without any user interaction or assistance. You can monitor agent installation progress, as well as track the status and performance of the agents installed further with tools of agents schema .

Detailed information on monitoring agent performance and status is described in section [Monitoring endpoint agents status](#).

To install endpoint agents on your network computers for Skype, Lync, USB, Network shares, Cloud storages, SIP, Viber and SSL traffic control:

1. Select the **Endpoint agents options** tab in **Endpoint agent control center**.
2. In the **Endpoint agents installation strategy** section, click the radio button corresponded to the strategy based on which agents will be installed on network computers:
 - **Install agents on specified computers only;**
 - **Install agents on all Active Directory computers.**

Endpoint agents installation strategy

 SecureTower provides remote agents installation based on the selected installation strategy. To start distributing remote endpoint agents, please, select the installation strategy below:

Install agents on specified computers only
 Use this strategy if it necessary to install endpoint agents on the particular computers only. According to this strategy SecureTower will install endpoint agents and monitor their status only on the computers which were specified by user.

Install agents on all Active Directory computers (only the objects from Active Directory cache are taking into account)
 Use this strategy if it necessary to install endpoint agents on all the computers from Active Directory cache created by SecureTower (cache settings can be configured in the Active Directory&Domains section of the User& Authentication tab). According to this strategy SecureTower will install endpoint agents and monitor their status automatically on all Active Directory cache computers. If endpoint agents mustn't be installed on the particular computers, specify it in the exclusions list.

The installation strategy can be applied both to the particular computers or to the Active Directory objects which include network computers accounts.

⚠ Attention: *All the operations concerning Active Directory structure are based on data stored in the AD cache at the current moment. If any changes in AD structure were made between AD update and operations in question, this operation will be processed excluding AD changes. To take the non-fixed in cache changes of AD structure into account, [update Active Directory structure manually](#) before implementing the operations with user data.*

Installing agents on particular computers

If agents should be installed only on the certain workstations in your network:

1. Click the **Install agents on specified computers only** radio baton. With this option enabled, the Endpoint agent control server is checking the presence or status of agents on specified computers only, and in case when some agents are not present, failed or were removed by users, it will automatically install the agents on the corresponding workstations.
2. Click **Computers to install agents on** to specify the list of the particular workstations or AD objects for agent installation and follow the recommendations given in [The list of objects to install agents on](#).

Install agents on all available computers in network

If it is important to have agents installed on all or on the majority of network computers which information were stored in the AD cache:

1. Click the **Install agents on all Active Directory computers** radio baton. If this strategy is selected, the Endpoint agent control server is checking the presence or status of agents on all the computers detected in your network, except for the ones specified in the

exclusion list. In case some agents failed or were removed by users, or new workstations are added to the AD cache, it will automatically install the agents on the corresponding workstations.

2. Click **Computers to exclude from agents installation** to specify the list of workstations which should be ignored while agent installation and follow the recommendations given in [The list of excluded computers](#).

Note: To apply the settings and to start installing the agents on the specified computers immediately, click **Apply changes** in the bottom right corner of the program's main window.

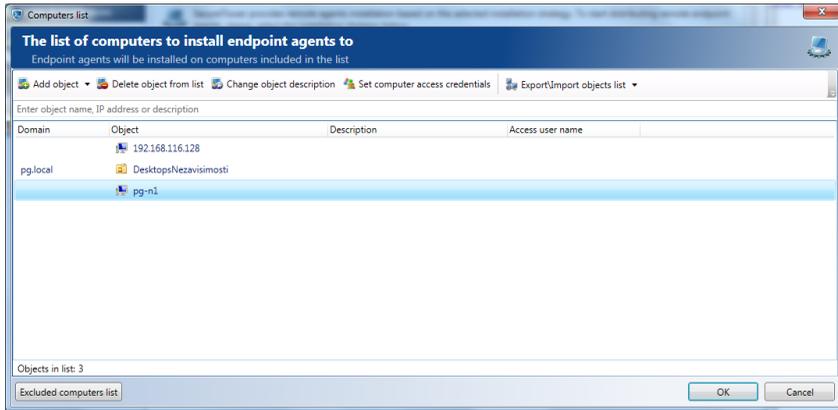
11.1.1.1 The list of objects to install agents on

When agent installation on the particular computers is necessary the list of AD objects or computers names for installation can be set.

Adding an object to the installation list

1. In the **Computer list** window, click **Add object**.
 2. Select one of the offered choice way:
 - Click **From Active Directory** if necessary to add AD objects. In the newly opened window specify a domain name in the drop-down **Domain** list (there are only local network domain) and click **Search**. To search for a specific object in the list, enter the name of it in the filtering text field. As you type, the list will display only the objects that have the entered symbols in their name. Finish the list configuring:
 - a) To select more than one object without closing a window, select the necessary item in the list and click **Add objects to list** (in the bottom left window corner) - the object will be added to the list. Repeat the action with other items. To finish, click **Select**.
 - b) To add object to the installation list and close the window select the necessary item in the list and click **Select**.
- or**
- Point to **Computer name** and click one of the preferable command to specify computer names for installation:
 - a) Click **From Active Directory** if necessary to add AD computers.
 - b) Click **From non controlled by server agents list** to install agent on uncontrolled workstations.
 - c) Click **Manually** to specify the particular known name. Type names of computers you need to be included to the list in the **Computer names** text field. Type a description of the computers in the corresponding field if necessary.

3. The newly added objects will be displayed in the list of computers to install agents on. The computers presented in the list can be sorted by computer name (alphabetically or vice versa –for letter symbols, in the ascending or descending order–for numeric values) by clicking the header of the **Computer name** column. For other operation with object list, see [Managing list of objects](#).



Note: Upon removing a workstation from the list, the agent installed on it will also be *deinstalled*.

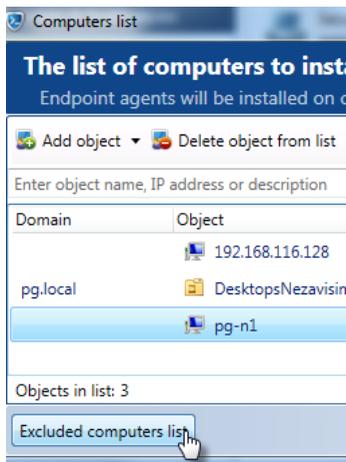
Excluding single computers from the installation

In some cases there is necessity to exclude a computer (that is a part of an object from the list) from installation policy.

If the objects that were selected for installation include computers which should be excluded from installation policy, one should specify the list of exclusions.

To specify the list of exclusions:

1. Click the **Excluded computers list** button in the bottom left corner of the **Computer list** window.



2. Select the necessary computer names in the list (to select multiple fields hold down Ctrl or Shift on your keyboard and click the names) and click **OK**.
3. For other operation with object list, see [Managing list of objects](#).
4. Click **OK** to finish with exclusion list configuring.

11.1.1.2 The list of excluded computers

If the strategy of agents installation on all accessible workstations in the network is selected, the list of workstations on which agents should not be installed can be set.

To specify the list of workstations or AD objects excluded from installation, click **Computers to exclude from agents installation** in the **Endpoint agents options** window.

Adding an object to the list of exclusions

1. In the computer list window, click **Add object**.
2. Select one of the offered way in the drop-down list:
 - Click **From Active Directory** if necessary to add AD objects. In the newly opened window specify a domain name in the drop-down **Domain** list (there are only local network domain). To finish the list configuring, click **Search** - the results will be displayed in the window. To search for a specific object in the list, enter the name of it in the filtering text field. As you type, the list will display only the objects that have the entered symbols in their name:
 - a) To select more than one object without closing a window, select the necessary item in the list and click **Add objects to list** (in the bottom left window corner) - the object will be added to the list. Repeat the action with other items. To finish, click **Select**.
 - b) To add object to the list and close the window select the necessary item in the list and click **Select**.

or

- Point to **Computer name** and click one of the preferable command to find and select the particular computers:
 - a) Click **From Active Directory** to add AD computers.
 - b) Click **From controlled by server agents list** to select objects with already installed agent to uninstall agent and exclude it from further installation.
 - c) Click **Manually** to specify the particular known name. Type names of computers you need to be included to the list in the **Computer names** text field. Type a description of the computers in the corresponding field if necessary.

The newly added computers will be displayed in the list of computers that will be ignored while agent installation. The computers presented in the list can be arranged by computer name (alphabetically or vice versa – for letter symbols, in the ascending or descending order – for numeric values) by clicking the header of the **Computer name** column. For other operation with object list, see [Managing list of objects](#).

Note: Upon removing a workstation from the list, the agent will be installed on it automatically.

11.1.1.3 Assigning access credentials

Access to all controlled computers by default is implemented under the username that is used for Endpoint agents control server (for more information, see [Service startup parameters](#)). If it is necessary to access a computer under a username other than default, specify the username manually.

One can specify credentials required for access to the computer while configuring agent installation as well as with the [Agents schema](#) tool.

To specify access credentials for the particular computer while configuring agent installation, in the list of computers for installation:

1. Click the name of the computer in the list.
2. Click **Set computer access credentials** on the command bar or click the corresponding command on the computer context menu.
3. Type an account name with the sufficient access rights in the corresponding field or click **Browse** to select the account from AD structure or from the list of local machine users (for more information, see [Selecting a user account to start up](#)).
4. Type the password for specified account name in the corresponding text box.
5. Click **OK** to finish.

11.1.1.4 Agents deinstallation

Endpoint agents that were installed on computers of your network with Endpoint agent control center are deinstalled by the same way.

1. Click the **Agents schema** tab in **Endpoint agent control center**.
2. In the **Agents schema** window, one can see the list of agents. Right-click the specific workstation where agent is installed on and select the **Remove agent and exclude computer from schema** option from the context menu.

3. Click **Apply Changes**. The system will try to connect to this computer and remove the agent from it. In case the computer name was entered incorrectly or the computer cannot be accessed for any other reason, the system will keep trying to connect to this computer until it succeeds and uninstalls the agent.

To uninstall agents from several computers simultaneously, click the **Endpoint agents options** tab and follow the recommendations given below:

- If the **Install agents on specified computers only** strategy is used, it is enough to delete computer names from the list of computers that were specified for agent installation (see [The list of objects to install agents on](#)).
- If the **Install agents on all Active Directory computers** strategy is used, just add the computer name to the list of excluded from agents installation (to find the computer name, select [From controlled by server agents list](#) in the **Add objects** menu).

11.1.1.5 Managing list of objects

Removing a computer from the list

To remove some workstations from the list of objects, click **Delete objects from list**. In the action confirmation dialogue window, click **Yes**.

Exporting\Importing the list of objects

To save the list of computers into a XML file or to import the list from a file, click the corresponding option on the **Export\Import list of computers** menu. This feature may be useful when exporting system settings for quick configuring an endpoint agent control server in another segment of the network. When you click this button, you have to specify the name of the file and the directory to save it into.

Changing computer description

The description of a computer can be changed from the computer context menu or by double-clicking the computer name in the list or by clicking the corresponding button on the window command bar.

11.1.2 Remote agent installation by Group Policy

Creating MSI file

1. Endpoint agent control server database should be configured first before installing. The MSI file for agent installation will be created then automatically (*the guidelines on configuring the database are provided in [Selecting data storage type](#)*).

2. The MSI file (**FgstAgentSetup.msi**) and the transform file (**FgstAgentSetup.mst**) for agent installation by means of Group Policy at one of these two paths: **C:\Program Files\FalconGaze SecureTower\EPA Control Server\Agent** or the **Start** menu.

Creating a distribution point

To assign an endpoint agent distribution point on the publishing server must be created. To do this, follow these steps:

1. Log on to the server as an administrator.
2. Create a shared network folder (for example, **C:\Agent_install**) where you will put the files **FgstAgentSetup.msi** and **FgstAgentSetup.mst** that you want to distribute.
3. Set permissions on the share to let users and computers read and run these distribution files.
4. Copy the distribution files to the distribution point.

Creating a Group Policy Objects

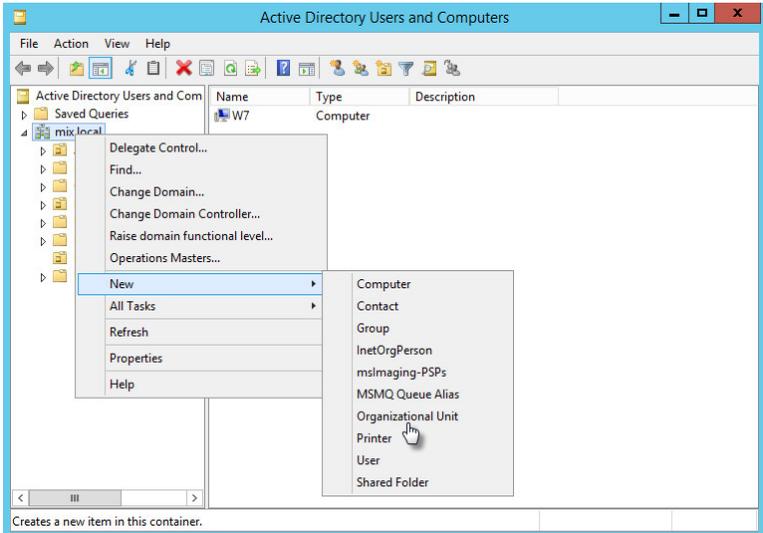
A Group Policy object (GPO) is usually applied only to members of an organizational unit (OU) to which the GPO is linked.

Note: *To manage domain Group Policy across an enterprise, you must first install Group Policy Management Console (GPMC).*

To create a Group Policy Object (GPO) to distribute the software, follow these steps:

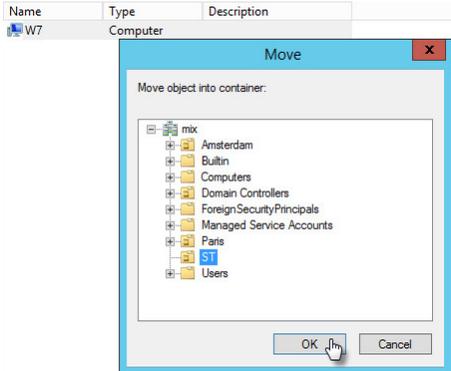
1. Log on as a domain administrator, and then start Active Directory Users and Computers.

In the console tree, right-click the domain node in which you want to add an organizational unit. Point to **New**, and then click **Organizational Unit**.

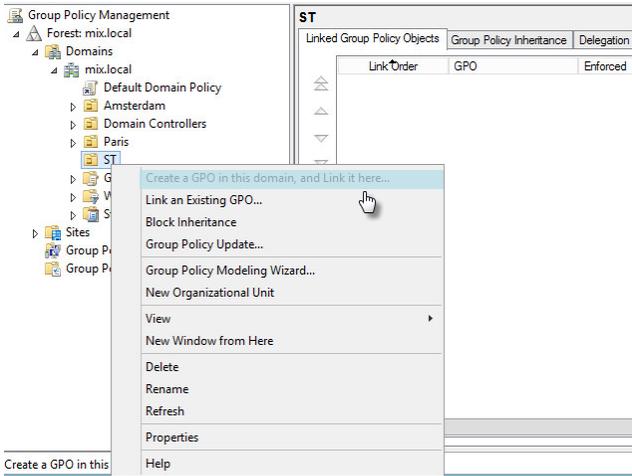


Type the name of the organizational unit (for example, **ST**) and click **OK**.

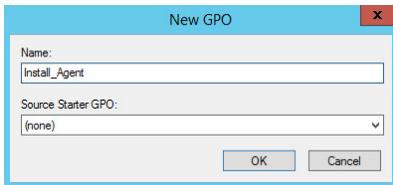
Right-click the **Computers** folder. Select the necessary computers from the list, drag and drop the computers into the created organization unit or click **Move** and select the one in the list.



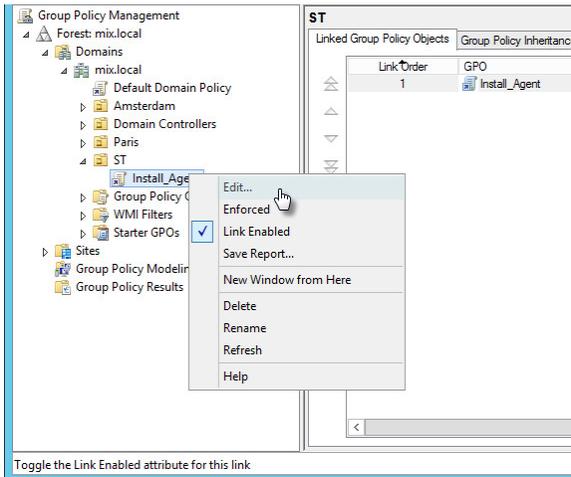
4. click *Group Policy Management Console* and create a new GPO for created OU (use the appropriated command on the popup menu).



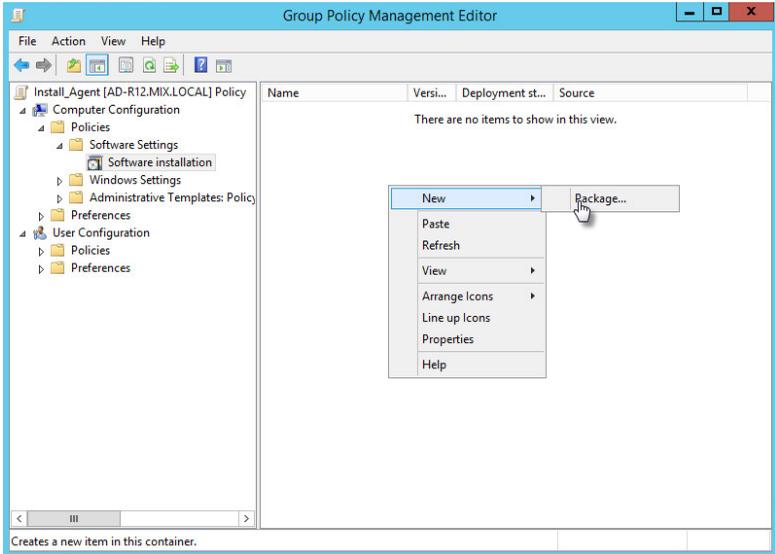
5. Specify the name of the GPO and click **OK**.



6. Open the popup menu of the created GPO and click **Edit**.

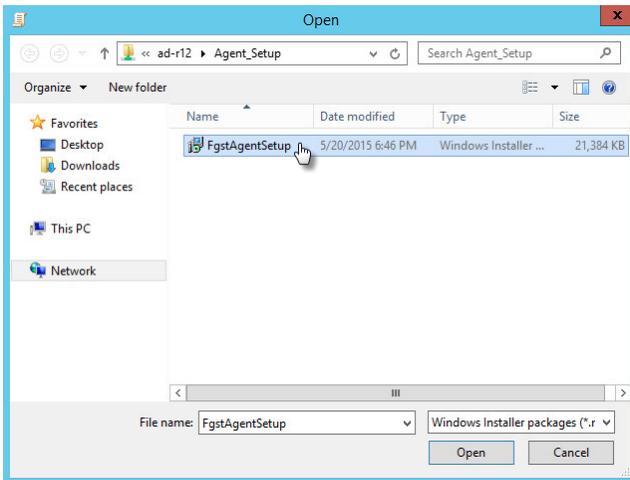


7. Navigate to **Computer Configuration - Policies-Software settings-Software installation** and right-click on the view area. On the popup menu point to **New** and click **Package**.



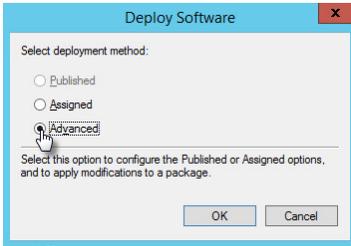
8. Select the MSI package in the folder that was created upon [distribution point creation](#).

Note: Specify the full network path to the folder to provide remote computers with access.



Click **Open**.

9. Click to select the **Advanced** radio button and continue configuring.



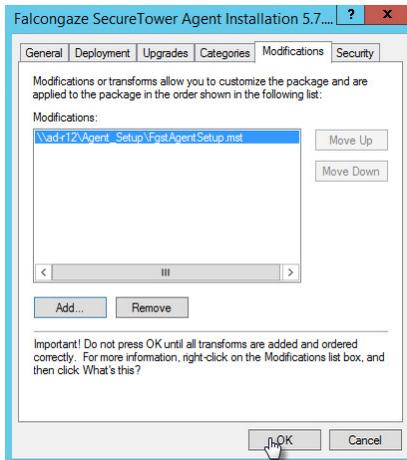
Click **OK**.

10. Click the **Modifications** tab of the setting window. Click **Add**.

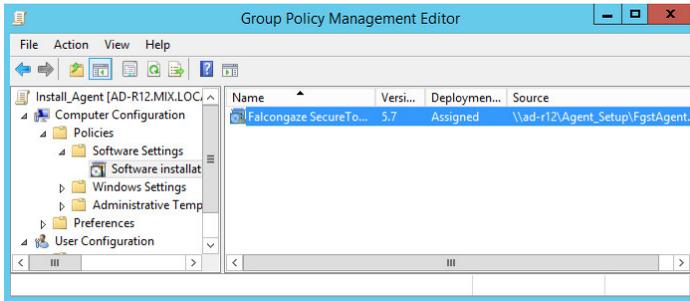
Note: The Add button will be unavailable if the Assigned option is checked on the previous step. Besides this it will be unavailable after configuring completion. Therefore all modifications must be added exactly on this step.

Select MST file (**FgstAgentSetup.mst**) and click **Open**.

Note: Specify the full network path to the folder to provide remote computers with access.



Click **OK**.



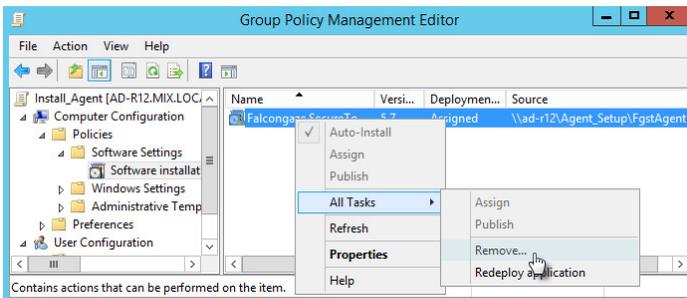
The installation package is ready to be installed.

Computers that were included into created OU will receive information about modifications in GPO and the corresponding OU will be assigned after the first restart. To implement a new task computer restart is necessary (agent installation implements after restart before user logging), thus the task notification will be created to install new agent application after the next restart. Therefore the agent will be installed just after the second restart.

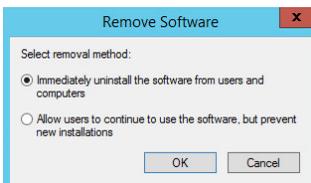
To force the installation the command line tool **gpupdate /force** can be used on the corresponding workstations. In this case policies will be updated immediately and the agent installation will be performed after the next restart.

GPO - based agents uninstalling

To delete agents from the controlled workstation select the installation package, right-click and point to **All Tasks** on the popup menu, click **Remove**.



There are two possible way of agents uninstalling:



Click an appropriated radio button and click **OK**.

Agents updates and recovery

To update agents or recover after agents files corruption or to correct any mistake in settings delete agents as described above and repeat installation.

11.1.3 Manual agent installation

SecureTower EndPoint Agents can be installed manually (for example, by means of copying from a storage device) by running *FgstAgentSetup.exe* available at *C:\Program Files\FalconGaze SecureTower\EPA Control Server\Agent* by default.

There are two possible ways of installation: with Installation Wizard interface or from command line.

Installation Wizard

1. Run **FgstAgentSetup.exe** on workstation.
2. When starting the Installation Wizard, you are to specify the network path to the EndPoint Agent Control Server and the server port number that will be used for connection establishing (default port - 10500). Click **Start**. Installation progress will be displayed in the wizard window.
3. Click **Close** after installation completion.

Note: If the server address isn't specified the agent installation will be aborted and the corresponding error message box will appear then.

If the wrong server address is specified or connection to server is lost due to any reason the agent installation will be aborted and the corresponding error message box will appear. It's strongly recommended to continue with installation after a connection problem is fixed:

- Click **No** to cancel the action.
 - Click **Yes** to continue. The agent will be successfully installed on the target workstation but will work incorrectly. The cyclic attempt of connection to server will take place to receive the agent settings. Note that no data will be intercepted until the connection is unavailable.
-

Installation from command line

Executed file of agent installation can be started from command line using the command-line options listed below:

- **/SVC** - Setup will work in service mode.
- **/SILENT** - starts auto-installation / deinstallation. When Setup is silent the wizard and the background window are not displayed but the installation progress window is. In cases of reboot necessity for correct installation, you will be prompted with the corresponding dialog box. To disable reboot use **/NORESTART**.
- **/VERYSILENT** - starts auto-installation / update in stealth mode. If the system reboot is needed for correct installation, it will be performed automatically. To disable autoreboot use **/NORESTART**.
- **/SUPPRESSMSGBOXES** - suppresses message boxes. Only has an effect when combined with 'SILENT' and 'VERYSILENT'.
- **/LOG="filename"** - creates a log file in the user's TEMP directory detailing file installation and [Run] actions taken during the installation process. Allows user to specify a fixed path/filename to use for the log file. If a file with the specified name already exists it will be overwritten. If the file cannot be created, Setup will abort with an error message.
- **/LANG=language** - Specifies the language to use. Available languages: en or ru.
- **/COMPONENTS="comma separated list of component names"** - Overrides the default component settings. Using this command line parameter causes Setup to automatically select a custom type. If no custom type is defined, this parameter is ignored. If a component name is prefixed with "*" character, any child components will be selected as well (except for those that include the dontinheritcheck flag). If a component name is prefixed with "!" character, the component will be deselected. This parameter does not change the state of components that include the fixed flag.

Example 1: /COMPONENTS="help,plugins" - Deselect all components, then select the "help" and "plugins" components.

*Example 2: /COMPONENTS="*parent,!parent\child" - Deselect all components, then select a parent component and all of its children with the exception of one.*

Available components:

console_client – client console

console_admin – administrator console

server – SecureTower servers

server\mailprocsrv - Mail Processing Server

server\intercept - Interception Server

server\intercept\event - Event and Notifications Server

server\epa - EndPoint Agents Control Server

server\icapserver - Icap Server

server\search - Data Processing Server
server\search\secsrv - Security Center
server\search\srv_rcnz - Recognition Server
server\search\clnt_rcnz - Recognition Client

- **/TYPE=type name** - Overrides the default setup type. If the specified type exists and isn't a custom type, then any /COMPONENTS parameter will be ignored..

Available types :

type_full – all components setup
type_custom – only selected components setup
type_admin – admin console
type_client – client console
type_server_intercept – interception server
type_server_mailproc – mail processing server
type_server_epa – endpoint agents control server
type_server_dataprocessing – data processing server
type_icap – ICAP server
type_server_recognize – recognition server
type_client_recognize – recognition client

- **/uninstall** delete endpoint agent from workstation.
- **/server SERVERADDR:PORT** - endpoint agents control server address.
- **/checksrv** - installation/ update connection test.

Example 3: FgstAgentSetup.exe /svc /checksrv /server FGST:10500. Setup will be in service mode (without user interface). Server address is "FGST:10500". Connection test and checking for updates will be performed upon setup.

Updates and recovery

To update agent version or to recover agent files if the agent settings become incorrect, start The Agent Setup Wizard:

1. Start installation file (**FgstAgentSetup.exe**) on the workstation you need to maintain.
2. Select **Update Falcongaze SecureTower Agent to version** mode and click **Next**.
3. Specify the up to date server address and click **Start**.
4. Click **Close** when process is finished.

Deleting manually

1. To delete an agent start the The Agent Setup Wizard(**FgstAgentSetup.exe**) on the workstation you need to maintain.
2. Select **Delete Falcongaze SecureTower Agent...** option and click **Next**.
3. Click **Close** when process is finished.

11.2 Server information

To familiarize with general server settings and configure them, click the **Settings of server and data storage** tab in the **Endpoint agent control center** window.

The relevant section provides information about the server name and port number used by the Endpoint agent control server to receive data from agents. Enter the appropriate data in the **Server name**, **Backup name** and **Server port** text boxes if these parameters are different from default settings.

Select the **Use ICMP for initial verification of the workstation status** check box, if you want to ping the computer in the network for the first time and if the support of this protocol is enabled in your LAN. However, clear the check box if there is a need to reduce network load.

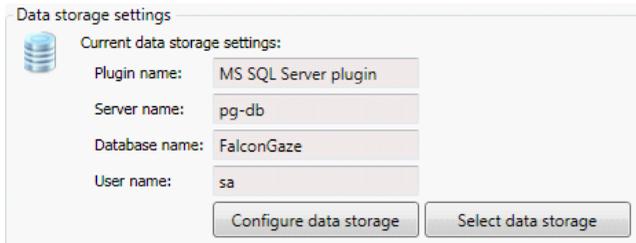
In the **Server address** field the address of User&Authentication server is represented. To change address, type the necessary one in this field.

To set up periodicity with which the server will check the Active Directory structure, use **Scheduler** (see [Active Directory and domains integration](#) for details). In case of detection of new objects in the Active Directory structure an appropriate strategy of agents installation will be applied to them.

Note: *In case of Server port number changing (for example, in case of version updating), it is necessary to consider that connection with the agents that have been earlier set manually or through group policies, will be stopped through the previous port number. For restoration of data acquisition from such agents it is necessary to carry out their updating manually. Updating of the agents installed with **Endpoint agent control center** will be made automatically.*

11.3 Configuring the database

To configure the database where the information provided by agents to the server will be saved, click the **Settings of server and data storage** tab in the **Endpoint agent control center** window, and in the **Data storage settings** section click **Select data storage**. *The guidelines on configuring the database are provided in [Selecting data storage type](#) chapter.*



Data storage settings

Current data storage settings:

Plugin name: MS SQL Server plugin

Server name: pg-db

Database name: FalconGaze

User name: sa

Configure data storage Select data storage

11.4 Agent settings profile

SecureTower enables configuring personal profiles of agents for the certain user accounts, computers, groups of Active Directory (including domains, containers and organizational units) and the certain computers which is out of Active Directory domain group.

To configure advanced settings of endpoint agents, click the **Agent settings profiles** tab in the **Endpoint agents control center** window.

In the **Agent settings profiles** tab the information about existed profiles is presented. Fields of the table contain the profiles name (the **Profile Description** column) and objects information which the appropriate profile is applied to (the **Applied to** field).

System enables configuring profiles and changing a priority of its application as well (for more details see [Priority of agent profile](#)). To manage profile list, use the appropriate command on the command bar of the tab (for more information, see [Managing profile list](#)).

Default profile is applied to all computers and users of the network by default depending on the selected strategy of agents installation.

To view and set parameters of an existing profile, left-click the corresponding profile name in the list. The settings of the profile can be accessed in the bottom part of the window.

To configure and apply specialized agent settings for data interception from particular computers or net users, it is necessary to create a new profile (see [Creating new agent settings profile](#)).

Note: *Default profile isn't available for deleting and priority changing. However, profile settings (except the name and objects of application) can be configured according to the current working tasks. To reset **Default profile** to presets, click **Reset settings to default** in the **Endpoint agent settings profile** window.*

11.4.1 Creating agent settings profile

To create a new profile:

1. Click **Create profile** on the command bar of the **Agent settings profiles** window.
2. Configure profile parameters switching between tabs in the section of profile settings:
 - [Settings profile information](#)
 - [Network traffic interception](#)
 - [Storage devices control](#)
 - [Devices control](#)
 - [Printers interception](#)
 - [Skype interception](#)
 - [Viber interception](#)
 - [SIP interception](#)
 - [Lync interception](#)
 - [Browser interception](#)
 - [Desktop activity](#)
 - [Audio/video Monitoring](#)
 - [Network shares control](#)
 - [File system control](#)
 - [Data blocking](#)
 - [Other](#)

Note: Clear the **Settings profile enabled** check box if you do not want to use the profile at present, but you are going to use it further. This option is also available from the profile context menu in the profile list.

3. When finish configuring, click **Apply changes** in the bottom right corner of the console window to save and apply the settings.

11.4.1.1 Settings profile information

To configure a profile general parameters, click the **Settings profile information** tab in the section of profile settings:

1. To specify a new profile name type a unique name in the **Profile description** field.
2. To activate created profile unconditionally, select the **Settings profile enabled** check box.

Note: If activated, the profile will be applied to its objects when there is no other condition specified. If there is at least one condition of activation specified, the profile will be applied only if the condition is satisfied. In other cases, despite the activation status, the profile will be disabled.

3. To specify activation conditions, select the necessary option check box in the corresponded section:
 - If it is necessary to apply profile when the connection is lost for more than n minutes, select the relevant option and type the time value.
 - If the profile must be enabled when a VPN connection is detected on the controlled workstation, select the **VPN connection is active** option.
 - If the other conditions must be applied, select the **User-defined condition** option and click the **Edit Lua script** button to create or edit the condition script. Type a script in the text box or click **Insert from file** and upload already created one from a file. Click **OK** to save.
-

Example. The Lua script created to change the status of the profile every 15 sec.:

```
condition_state = false;
OnLoad = function ()
    timer.set_for("Timer", 15 * 1000);
end
OnTimerEvent = function(str)
    condition_state = not condition_state;
    setting.set_condition_res(condition_state);
    return true;
end
```

4. If the endpoint control server is unavailable by its general name, select the **Redirect to the reserved server name** option. The data from agent will be sent to the server using reserved name regardless of availability of the server by the general name (see [Server information](#)).
5. To create a list of new profile objects, click **Add objects** and click the necessary sub menu:
 - If the objects are included into domain group, continue as described in the [The list of objects to install agents on](#) chapter.
 - If a workstation with agent isn't included into AD structure the SID can be specified to identify the profile object manually. To add object by SID, click **Add objects**, and then click **Custom user SID**. Specify the SID and description (optionally) in the newly opened window.

The list of all profile objects with domain and object names is displayed in the **Applied to** field.

Note: The profile name applied to the computer and SIDs of local users can be found in the field **Computer network statistics of the Agents schema** tab (for more information, see [Monitoring endpoint agents status](#)).

11.4.1.2 Network traffic interception

To configure network traffic interception options, click the **Network traffic interception** tab in the section of profile settings:

1. To select an interception mode, in the **Interception mode** list:

- Click **No interception allowed** if you do not want to intercept any traffic;
- Click **All network traffic (encrypted and non-encrypted)** if you need to intercept entire network traffic **by endpoint agents**. This option is useful if you did not install the interception server that is responsible for centralized interception of traffic. Otherwise, enabling this option may result in the traffic duplication;
- Click **SSL encrypted network traffic only**, if you need to intercept only the encrypted traffic (recommended option if you installed the interception server that is responsible for intercepting non-encrypted traffic only);
- Click **Non-encrypted network traffic only**, if you need to intercept only non-encrypted traffic (not recommended if you installed the interception server because this may result in traffic duplication).



In case you select either **All network traffic** or **SSL encrypted traffic only**, the agent will substitute SSL certificates to capture encrypted traffic.

2. To configure SSL interception, click the corresponding button. For more information, see the [Configuring SSL interception](#) chapter.

3. To intercept traffic through intermediary proxy-servers, select the **Proxy preprocessor enabled** check box.

Preprocessor for HTTPS and SOCKS v4/4a/5 proxies. The filter classifies the transmitted content and detects proxy type automatically (SOCKS v4/4a, SOCKS5, HTTP CONNECT request to HTTPS proxy)

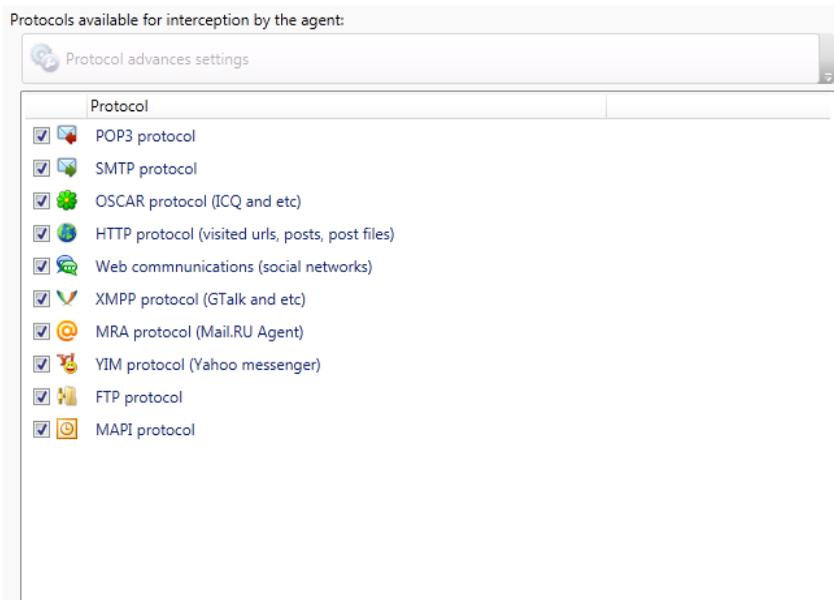
Proxy preprocessor enabled

4. To block network traffic of the particular processes, select **Enable traffic blocking for processes** and click **List of processes to block traffic**. For more information, see [Blocking process traffic](#).

5. To set the mode of process traffic interception, click the **Processes exclusions** button and configure the list of processes as described in [Excluding processes from interception](#).

6. To exclude from interception traffic from particular IP, click IP address exclusions and follow the recommendations of the [IP exclusions](#) chapter.

7. To intercept by agent a particular type of traffic, select the check box of the relevant protocol. For more information, see the [Configuring protocol interception](#) chapter.

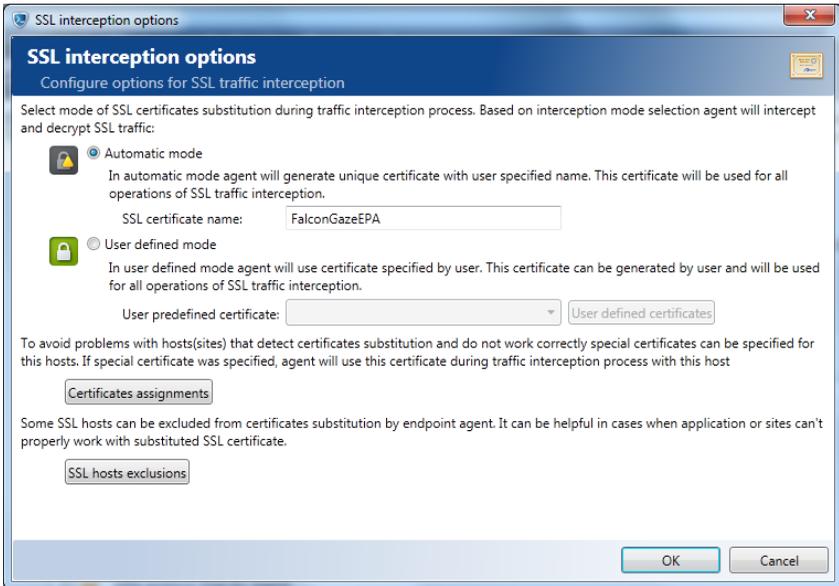


Note: *SecureTower agents execute interception of network traffic with user ID identified in Active Directory (SID), thus the traffic of system processes (service program) is ignored.*

11.4.1.2.1 Configuring SSL interception

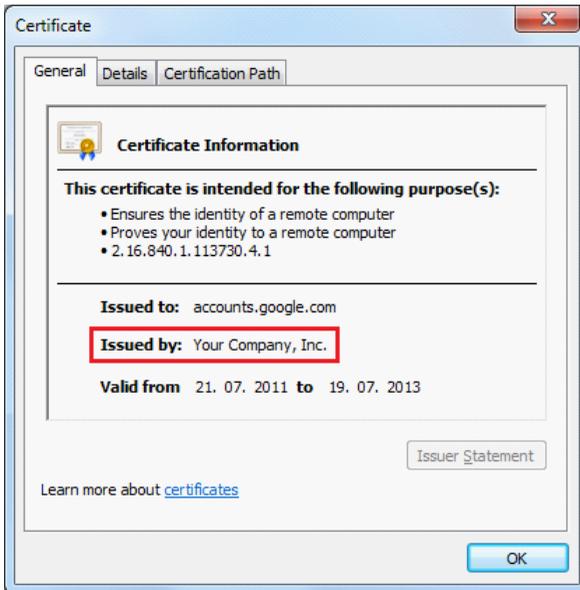
In case of secure connection between a client and a server, agent replaces the original server certificate on another one with a similar name, but issued from a trusted Endpoint agent's Root Certificate.

The root certificate with signer rights can be issued automatically (by the **SecureTower** agent) or manually in user defined mode. The binding of SSL certificates to particular hosts (sites) and particular hosts (sites) exclusion from certificates substitution also are available.



1. To choose modes for SSL certificates substitution, click the corresponding radio button in the **SSL interception options** window:

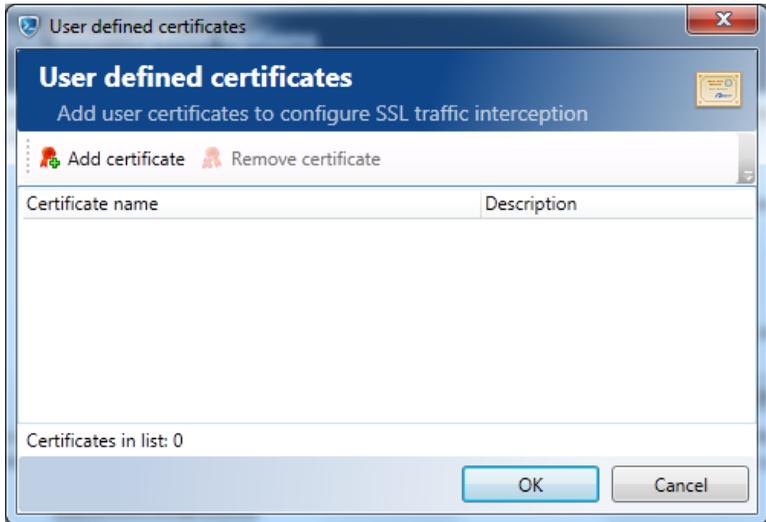
- Click the **Automatic mode** radio button to use the SSL root certificate that was created by the agent automatically upon installation on the user workstation. This agent root certificate will be stored in the data base of trusted Certificate Authorities and will be used for further issue of SSL certificates with **Falcongaze SecureTower** signature by default. The name you enter here will be displayed in the SSL certificate information in your web browser.



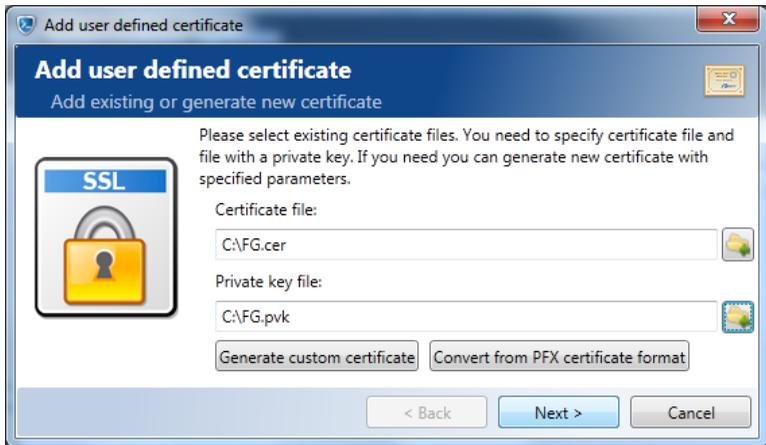
To change the default signature enter the necessary issuer name in the **SSL certificate name** field.

- Click the **User defined mode** radio button to use the SSL root certificate that was specified or created previously by user.

To specify user certificate select its name from the **User predefined certificate** drop-down list or add new certificate and private key files to system data base by using the **User defined certificate** button.

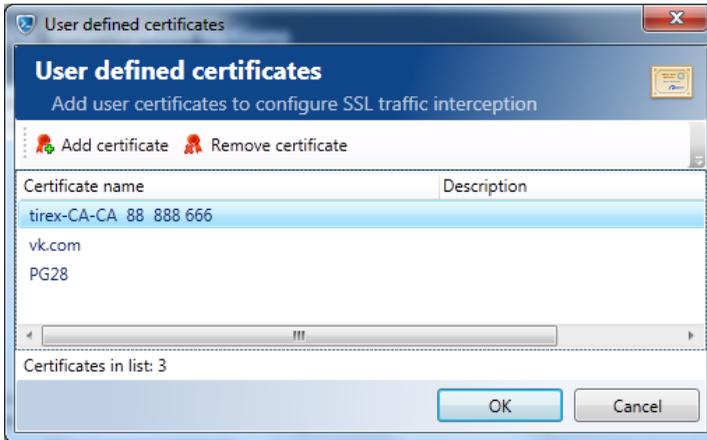


To add new files, click **Add certificate** in the **User defined certificates** window and add existing certificate and private key files by specifying the path.



Click **Next** to proceed.

Enter a unique issuer name and description (optionally) in a newly opened window and click **Finish** to add this certificate to the system data base of user certificates.



Click **OK** to add certificate to the data base of reliable certificate issuers.

Certificate generating

To generate custom certificate click **Generate custom certificate**.

Enter a name, valid duration and path to newly generated certificate file (*.cer) and private key file (*.pvk).

Click **Generate** and follow recommendations given [above](#).

Certificate converting

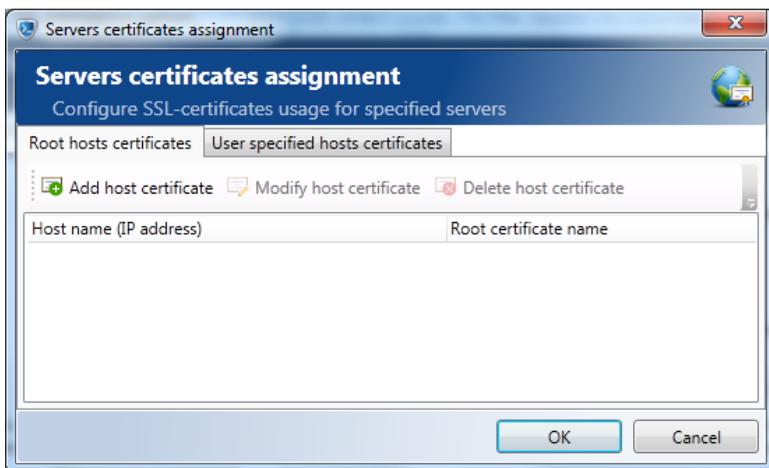
To convert certificate use **Convert from PFX certificate format**.

Enter the password and the path to the PFX file and paths to a certificate file (*.cer) and a private key file (*.pvk) to convert the PFX file to.

Click **Convert** to finish converting and follow recommendations given [above](#).

A predefined certificate can be used to intercept traffic from particular hosts (sites).

2. To bind a certificate to a host use **Certificate assignments**:

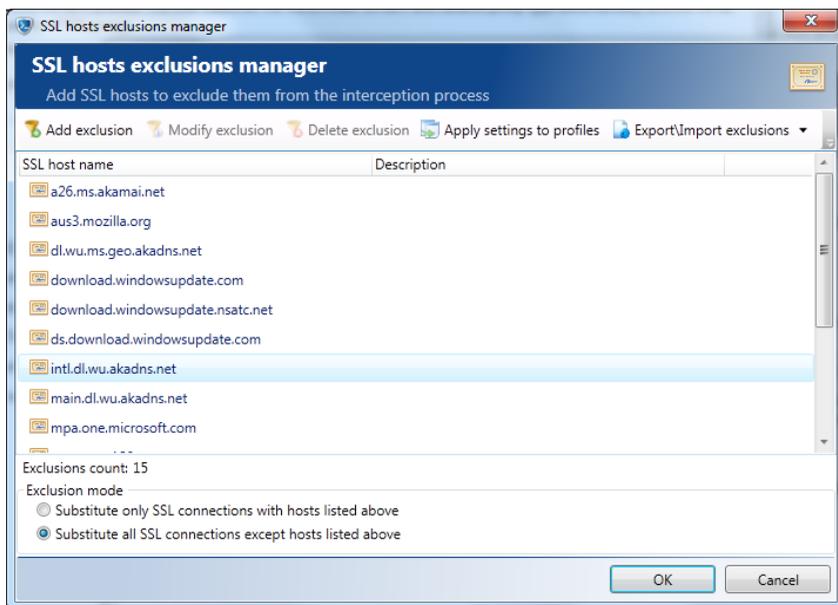


- To bind the root certificate to the host click **Add host certificate** in the **Root hosts certificate** tab.
 1. Enter host name(or IP address), which the SSL certificates will be issued to and to which the root certificate will be bound.
 2. Select one from the root certificate preset drop-down list or add new root certificate and private key files by using **User defined certificate**.
- To bind any predefined SSL certificate to the host, click **User specified hosts certificates** tab and click **Add host certificate**. User predefined SSL certificates will be used by agent to intercept SSL traffic.
 1. Enter host name(or IP address), which the SSL certificates will be bound to.
 2. Select one from the already bound SSL certificate drop-down list or bound a new one by using **User defined certificate** (follow recommendations given [above](#) for user root certificate).

Note: Using IP- address instead host name is acceptable only for cases when it is impossible to reveal the host name.

3. Substitution of original certificate can sometimes make the SSL connection to server impossible. It is necessary to exclude such problem server from interception by setting deny on substitution processes for this server. This action will recover connection but the agent cannot intercept SSL traffic for this web-site or program.

To exclude problem server from substitution, click **SSL hosts exclusions**.



There are 15 hosts in preset exclusions. It is possible to add, modify or delete any by using corresponding buttons in the **SSL hosts exclusions manager** window.

To add a new one use the corresponding button and enter host name (register-sensitive), for example, accounts.google.com. It is possible to use mask entering (*.microsoft.*).

For other operation with exclusions follow the recommendations from [Managing interception exclusions](#) chapter.

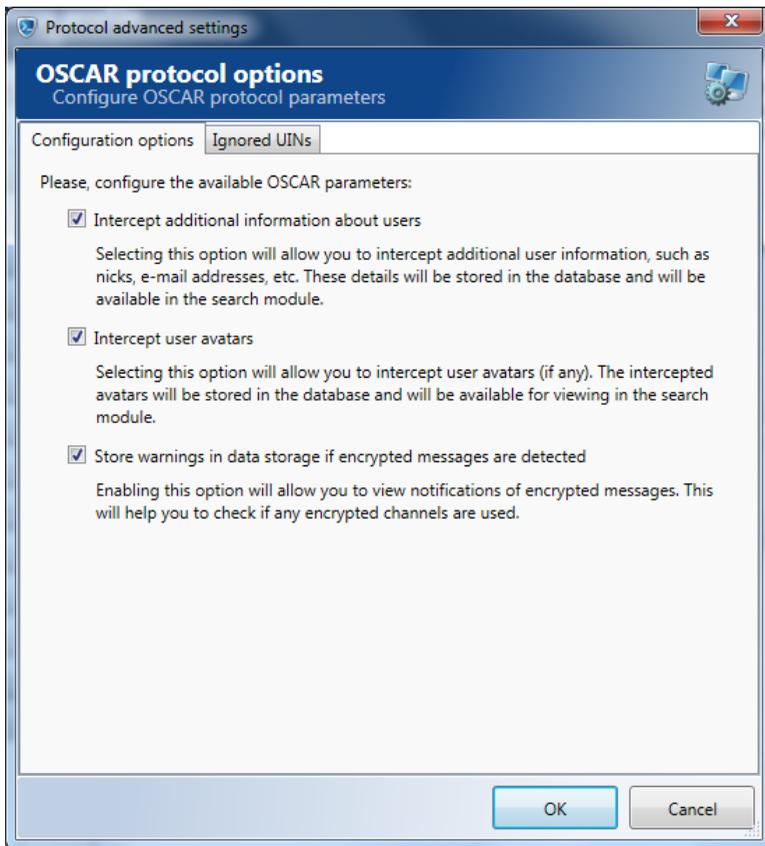
11.4.1.2.2 Configuring protocol interception

To configure a protocol interception, select the protocol check box in the list, and then click **Protocol advanced settings**. For more information, see corresponding article of [Setting up supported protocols for centralized traffic interception](#) chapter. Advanced settings of OSCAR, HTTP(S) and Web communications interception are described below.

Note: *Interception of data transferred over encrypted MAPI is provided using [integration with MS Outlook](#), enabling MAPI protocol interception is only applicable for decrypted MAPI. Interception of data transferred over IMAP and OSCAR files is implemented by means of interception server only. To intercept the data in question the both type of interception must be used. Herewith, interception of MAPI over HTTP traffic is supported by agents means as well as MAPI over RPC over HTTP and MAPI over RPC.*

Oscar advanced settings

Agents enables interception of IM conversations transferred over OSCAR protocol.



The following advanced option are available:

- **Intercept additional information about users** - enables interception of account names, emails, etc. All data will be stored in database and accessible for analysis.
- **Intercept user avatar** - IM user avatar will be intercepted and stored if this option is active.
- **Store warnings in data storage if encrypted messages are detected** - notification about encrypted data transferring can be delivered to addressee if this option is checked.

HTTP settings for SSL traffic interception

When SSL connection is established HTTPS traffic can be intercepted as well. To process HTTPS traffic with filter tool configure advanced settings of HTTP.

To configure filtering, click the **Filters** tab in the **HTTP protocol options** window and check the **Enable filters** option. Use combination with SSL condition and other one to create a filter for HTTPS traffic.

Filtering as well as other advanced settings for HTTP can be configured as described for centralized interception of HTTP (see [HTTP settings](#)).

Web communications advanced settings

Interception of communications in the most popular social networks enables monitoring and storing both local and remote user posts in the social network chats, forums. Moreover the interception and monitoring of mail transferred with the certain web-mail services is implemented in the system.

To specify the social network to control, select the corresponding check box in the **Social networks tab** of the **Web communications protocol options** window.

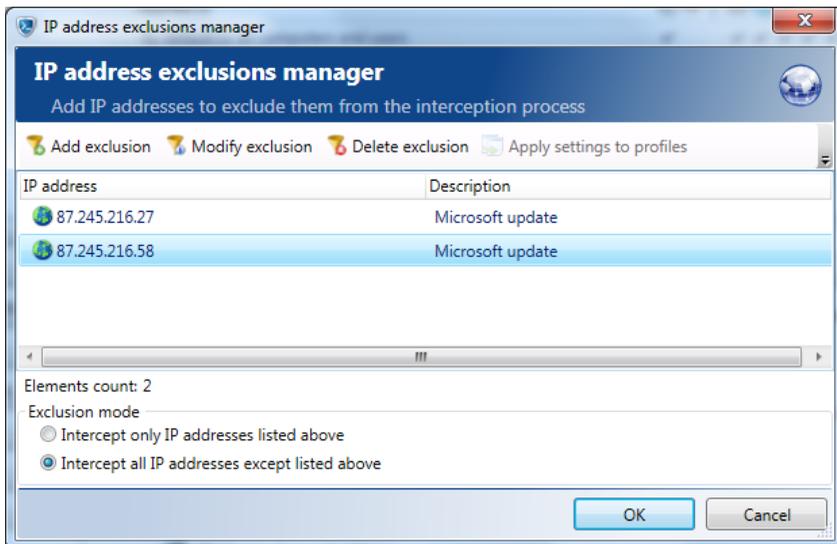
To specify the web-mail services for which mail sending and receiving are need to be monitored, click the **Web mail** tab and select the corresponding check box. The most popular services are available: gmail, yandex, mail.ru, rambler, hotmail, yahoo.

To specify the web messengers, that must be intercepted by the agent, click the corresponding tab, and then select the necessary check boxes.

11.4.1.2.3 IP exclusions

To exclude a certain IP address or range of IP addresses from interception:

1. Click **IP address exclusions** in the **Network traffic interception** tab.
2. In the IP addresses exclusions manager window, you will see two exclusion modes: **white list** and **black list** of IP addresses. You can only select one type of exclusion mode to apply to the list of addresses that you enter in the **IP address** window.
 - Once you mark the IP addresses as included in to the **white list**, these IP addresses only will be intercepted; all other IP addresses will be ignored.
 - If you mark the IP addresses as included into the **black list**, all IP addresses other than these will be intercepted; only the IP addresses listed in the **IP address** window will be ignored.



3. To add IP addresses that you want to include into the black or white list, click **Add exclusion**.
4. Click the necessary type of exclusion: single or range.
5. Enter the required IP address or range of IP (if selected) in the **Exclusions** text box.
6. Type the port number or range in the corresponding text boxes (if necessary).
7. Click **Add**.
8. For other operation with exclusions follow the recommendations from [Managing interception exclusions](#).
9. To save the settings, click **OK**.

11.4.1.2.4 Blocking process traffic

Network traffic of processes is blocked on basis of process attributes analysis. If an attribute is added to the list for blocking, network traffic of all processes with this attribute will be blocked by agent.

To add attribute to the list:

1. Click **Add attribute** on the command bar of the blocking manager window.
2. Select a type from the **Attribute type** drop-down list.
3. Enter the necessary value of the attribute in the **Attribute** text box (such as "inifum.exe" or "iexplore.exe" for the File name type) or click the process selection button  next to the text box to select attribute from the list of processes started on the network computers.

Note: The attribute of following type must be specified as regular expression: Product name, Copyright, Original name.

The process selection window displays all processes running on the selected computer.

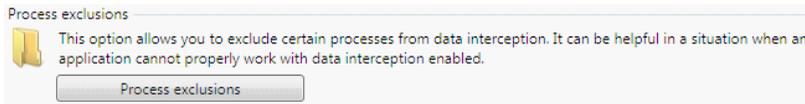
To view a list of processes run on another computer, select it from the **Computer** drop-down menu and click **Refresh processes list**. To facilitate search for a specific process in the list type the characters contained in the name of the process into the filtering text box. Highlight the desired process in the list and click **Select**.

4. When finish configuring the list enter the comment in the **Description** text box if necessary, and then click **Add**.
5. For other operation with the list follow the recommendations from [Managing interception exclusions](#).
6. To save the settings, click **OK**.

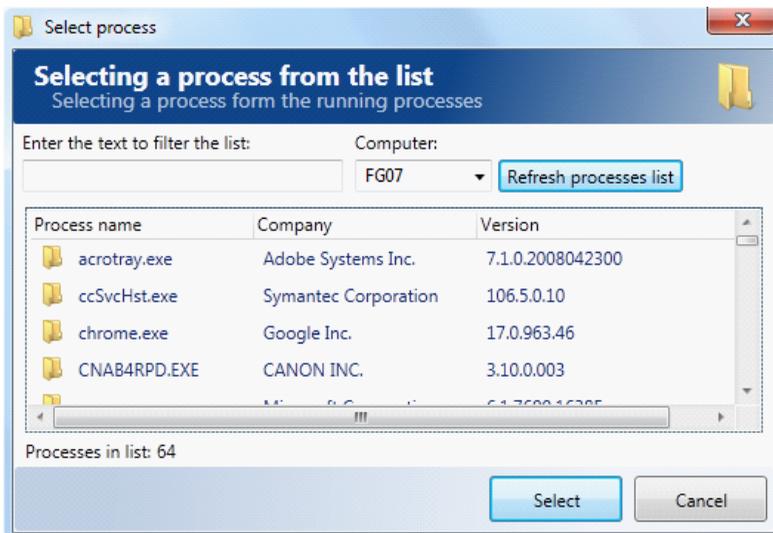
11.4.1.2.5 Excluding processes from interception

To manage a certain process interception, in the **Network traffic interception** tab:

1. Click **Process exclusions**.



2. In the Processes exclusions manager window, you will see two exclusion modes: **white list** and **black list** of processes. You can only select one type of exclusion mode to apply to the list of processes that you enter in the **process name** window.
 - Once you mark the processes as included in to the **white list**, these processes only will be intercepted; all other processes will be ignored.
 - If you mark the processes as included into the **black list**, all processes other than these will be intercepted; only the processes listed in the **Process name** window will be ignored.
3. To add processes that you want to include into the black or white list, click **Add**.
4. Enter the name in the text box of the dialog window, or click  next to the text box.



The process selection window displays all processes running on the selected computer.

To view a list of processes run on another computer, select it from the **Computer** drop-down menu and click **Refresh processes list**. To facilitate search for a specific process in the list type the characters contained in the name of the process into the filtering text box. Highlight the desired process in the list and click **Select**.

5. In the exclusions dialog box, click **Add**. The process will be added to the list of exclusions.
6. For other operation with exclusions follow the recommendations from [Managing interception exclusions](#).
7. To save the settings, click **OK**.

Note: SecureTower processes are excluded from interception by default.

11.4.1.3 Control of storage devices

The system enables control of data storage devices (USB flash drive, hard disk drive, optical and floppy disc, devices, recognized as removable storage) that are used at workstations. To set up parameters of devices audit, control and interception, click the **External device control** tab in the section of profile settings and click the **Settings** button related to storage devices.

A set of flexible control options allows to configure audit, shadow copy, access and writing policies for mass storage devices with specified parameters. The file operations control considering files extensions is provided as well. Devices parameters and file extensions are specified by system administrator upon exclusions configuring for a particular control procedure.

File operations audit

The system enables audit of file operations with storage devices, fixation of copying to storage devices is performed. The full file name, file size as well as the name of the process that has started the recording process are intercepted and saved by the agent. The files content isn't intercepted and stored. Audit of files operations is provided regardless of other control procedures settings.

To enable the audit function, select the **Audit file operations** check box.

The system enables user to set a specific audit mode for storage devices with different parameters and for files with different extensions:

- To specify exclusions from audit for particular devices, click **Audit exclusions** (navigate to the bottom of the window). Follow the guidelines from [Excluding according to devices parameters](#) section to configure an audit mode.
- To specify exclusions from audit for files with the particular extensions, click **File extensions** in the corresponding section (navigate to the bottom of the window). Follow the guidelines from [Excluding according to files extensions](#) section to configure an audit mode.

Note: *Audit and interception are provided for files with non-zero size by default, select the corresponding check box to control zero-size files as well.*

Control procedures

To configure control procedures, select the **Enable storage devices control** check box.

SecureTower enables interception of data transferred to storage devices and restriction of access and writing to devices.

Interception of information is carried out by **SecureTower** agent by shadow copying of the data transferred to storage devices. Thus the copy of the intercepted data is stored in the shadow copy storage located on the local user computer, and then is transferred to the Endpoint agent control server to save the data to the database. By default, the size of shadow copy storage is 1000 MB. When exceeding this threshold the description of the intercepted files is transferred only. Shadow copies of the intercepted information are accessible in **SecureTower** Client Console.

To intercept the information copied to storage devices, select the corresponding option check box in the **Storage devices control** tab and configure the necessary parameters:

- To set a shadow copy policy for devices with the particular parameters, click **Interception exclusions**. Follow the instructions from [Excluding according to devices parameters](#) section.
- To set a shadow copy policy for files with the particular extensions, click **File extensions** in the corresponding section. Follow the instructions from [Excluding according to files extensions](#) section.

Note: *If the shadow copy option is active, interception and storage of all data transferred to all storage devices are performed by default.*

When interception of the file copied to storage device is taken place file size is considered. By default, files with size smaller than 100 MB are copied to shadow copy storage entirely. A shadow copy of the fragment consisted of the first 100 MB of data is made for files bigger than 100 MB.

To optimize the interception process, set parameters of shadow copies saving. It can be useful for reduction of the shadow storage size:

- Type wanted size in the **Shadow copy file size limit** text box(MB);
- Type wanted size in the **Shadow copy storage size limit** text box(MB).

To configure access control select the **Control access to storage device** check box:

- To set an access control policy for devices with the particular parameters, click **Access exclusions**. Follow the instructions from [Excluding according to devices parameters](#) section.

To configure control of copying to storage devices, select the **Control writing to storage device** check box and configure the necessary settings:

- To prohibit or allow network users to copy data to devices with the particular parameters, click **Writing access exclusions**. Follow the instruction from [Excluding according to devices parameters](#) section.
- To prohibit or allow network users to copy files with the particular extensions to devices, click **File extensions** in the corresponding section. Follow the instructions from [Excluding according to files extensions](#) section.

Note: *If the control options is active, access and writing are enabled for all files extensions and all storage devices by default.*

Excluding according to devices parameters

Storage devices parameters can be specified in the **Devices exclusions manager** window.

Note: *After completion of agents installation information about devices which are connected at present and devices parameters are displayed in the **Agents schema** tab of the **Endpoint agent control center** (see [Monitoring endpoint agent status](#) for more details).*

1. Click the necessary exclusion mode radio button to select the mode. There are two exclusions modes in exclusions manager window: a **white list** and a **black list** of devices. You can select only one type of exclusions modes to apply to the list of storage devices:
 - Once you mark the list of devices as included into the **white list**, control procedure will be applied to devices only with these parameters; all other devices will be ignored.
 - If you mark the list of devices as included into the **black list**, control procedure will be applied to all devices with parameters other than specified in the list; only the devices with parameters listed in the list will be ignored.

Note: *The second exclusion mode is selected by default.*

2. To add a storage device parameter in exclusions, click **Add exclusion** and from the drop-down list select one of the options:

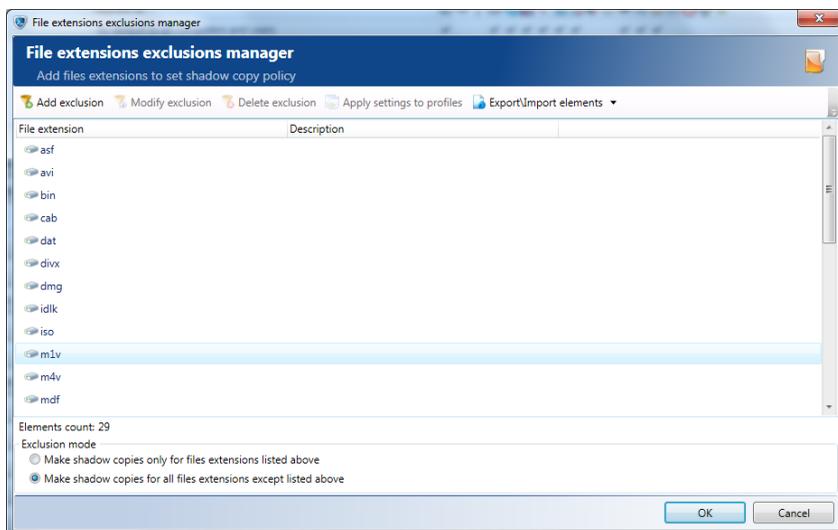
- To add exclusions for current connected drives, select corresponding option. To choose a computer with connected storage devices, in the **Computer name** list click the name of your choice. In the **Exclusions** list click the exclusion type of your choice. To add exclusion, click **Add**.
- To add exclusions for arbitrary storage devices select corresponding option, in the **Exclusions type** list click the exclusion type of your choice. In the **Devices types** list click the necessary device type. Type the value of exclusion in the text field. To add exclusion, click **Add**.

The list of specified exclusions will be displayed in the manager window. The quantity of the listed exceptions is displayed in the **Exclusions count** field. .

3. For other operation with exclusions follow the recommendations given in [Managing interception exclusions](#) chapter.
4. To save exclusions, click **OK** in the **Devices exclusions manager** window.

Excluding according to files extensions

The excluded extensions are displayed in the **File extensions exclusions manager** window in the list form. The default list of excluded files extensions that potentially considered as not a security threat are used in the system.



1. Click the necessary exclusion mode radio button to select the mode. There are two exclusions modes in exclusions manager window: a **white list** and a **black list** of extensions. You can select only one type of exclusions modes to apply to the list:
 - Once you mark the list of extensions as included into the **white list**, only file with these extensions will be under control; all files with other extensions will be ignored.

- If you mark the list of extensions as included into the **black list**, files with other than these extensions will be under control; only the traffic of files with extensions listed in the window will be ignored.

Note: *The second exclusion mode is selected by default.*

2. To add extension in exclusions, click **Add exclusion** and type in the **Exclusions** field the extensions of your choice (start a new one in the new line) and description (optionally).

The list of specified exclusions will be displayed in the manager window. The quantity of the listed exceptions is displayed in the **Exclusions count** field.

3. For other operation with exclusions follow the recommendations given in [Managing interception exclusions](#) chapter.

4. To save exclusions, click **OK** in the **File extensions exclusions manager** window.

Excluding processes from the common control settings

To exclude the certain processes from the allowing policies (the "white list" mode is set) specified previously while configuring audit, shadow copy and access control settings, click the **Processes exclusions** button and configure the exclusions in the **Process exclusions manager** window.

There are two modes in the exclusions manager window: a **white list** and a **black list** of processes. One can select only one type of exclusion mode to apply to the list of processes.

- Once you mark the list as included into the **white list**, checked control type of these processes interactions with storage devices will be prohibited.
- If you mark the list as included into the **black list**, processes with the names other than these will be excluded from the allowing policies (SecureTower control of this processes interactions with storage devices will be prohibited); only for the processes listed in the window the allowing common control settings will stay valid.

1. Click the necessary radio button to set the exclusions mode.

2. To add process name to the list, click **Add** and enter the necessary name in the **Exclusion** text field. To select a process from the list of processes executed on the controlled workstations at the moment click the **Selection** icon  and select the necessary process in the list.

3. Select the necessary control type check box in the **Scope** section:

- Select **Access lockout** if it is necessary to prohibit access to storage devices that are allowed to use for the specified processes .
- Select **Write lockout** if it is necessary to prohibit writing to allowed storage devices for the specified processes.
- Select **No interception** if it is necessary to prohibit shadow copying of data transferred to allowed storage devices by the specified processes.
- Select **No audit** if it is necessary to prohibit audit of file operations with allowed

storage devices for the specified processes.

4. Comment the exclusion if necessary.
5. Click **Add** to finish. The list of the processes with all exclusions settings will be displayed in the manager window. To change the exclusion scope select or clear the necessary exclusion type check box.
6. For other operation with exclusions follow the recommendations given in [Managing interception exclusions](#) chapter.
7. To save exclusions, click **OK**.

11.4.1.4 Control of devices

The system enables control of using external devices via USB-, COM-, LPT-port and to set up control modes for such devices according to their parameters. Audit of devices connections to workstation can be enabled as well.

To start configuring, click the **External device control** tab in the section of profile settings and click the **Settings** button related to devices control.

Note: To configure control of devices, recognized as removable storage in the OS of controlled computer (iPhone, iPad, mobile phone, digital camera with flash memory cards), use tools of [storage devices control](#).

Devices control

To enable devices control, select the corresponding option. All type of connected devices will be found and information about them will be available in the system (for example, in the **Agent schema** tab window).

To set up control modes for devices with specified parameters (to configure black and white list of available for using), click **Access exclusions**.

In exclusions manager window, you will see two exclusion modes: a **white list** and a **black list**. You can select only one type of exclusion mode to apply to the list.

- Once you mark the list of devices as included into the white list, using of devices with these parameters only will be denied; using of other devices will be permitted.
- If you mark the list of devices as included into the **black list**, using of devices with parameters other than these will be denied; only the devices listed in the window will be accessible.

Note: The second exclusion mode is selected by default.

1. To add the parameter to exclusions, click **Add exclusion** and select one of the options:
 - To add exclusions from current connected devices select corresponding option and continue configuring:
 - To choose a computer with connected devices, in the **Computer name** list click the name of your choice. The list of devices connected to PC will appear in the **Exclusions** field.
 - To specify a device type that should be added to exclusions, in the **Device type**

list click the type you want.

- In the **Exclusions** list click the one from offered exclusion parameters, and then click **Add** to finish.

- To add exclusions for arbitrary device select corresponding option. In the **Exclusions type** list click the type of your choice. In the **Devices types** list click the necessary device type. Type the value of exclusion in the text box. To add selected type of exclusion, click **Add**.

The list of selected exclusions will be displayed in the manager window. The quantity of listed exceptions is displayed in the **Exclusions count** field.

2. For other operation with exclusions, follow the recommendations from [Managing interception exclusions](#) chapter.
3. To save exclusions, click **OK** in the **Devices exclusions manager** window.

Devices audit

To enable the audit function select the **Enable devices usage audit** check box.

SecureTower will intercept the history of devices usage. The time of connection and disconnection as well as devices parameters (identifier and name of manufacture, identifier and name of product, serial number) and the current state of devices that connected to the workstations will be available for analysis.

11.4.1.5 Printer interception

The endpoint agent enables interception of documents sent to local or network printers. Captured documents will be displayed in **SecureTower** Client Console.

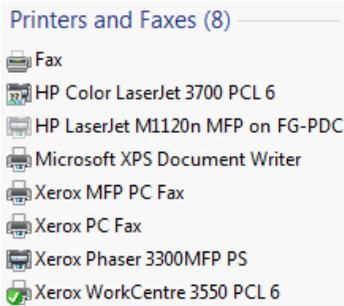
To enable interception of document sent to local and network printers, click **Printers interception** tab in the section of profile settings, and then select the corresponding option.

An intercepted document may be displayed in **SecureTower** Client Console in two variants: text formatted as the original or fully graphic view (as a picture). Subject to the format of the file printed, the application that sent the file, the printer and other factors, captured documents may be available only in graphic format.

- In case of **text view**, by default the system will save and display the document in full, including graphic objects it may contain. If there is no need to save graphic objects, select the **Do not include graphic objects into a text document view** check box. In this case the system will only store and display text data contained in documents, which may be helpful to reduce the size of the database.
- To intercept data from printers in raw format select the relevant check box.
- In case of **fully graphic view**, you can adjust the quality of the image stored in the database and displayed to the user by moving the **Image quality slide bar**. The lower this value is, the less disk space will be needed to store the files and the lower will be the quality of the picture.

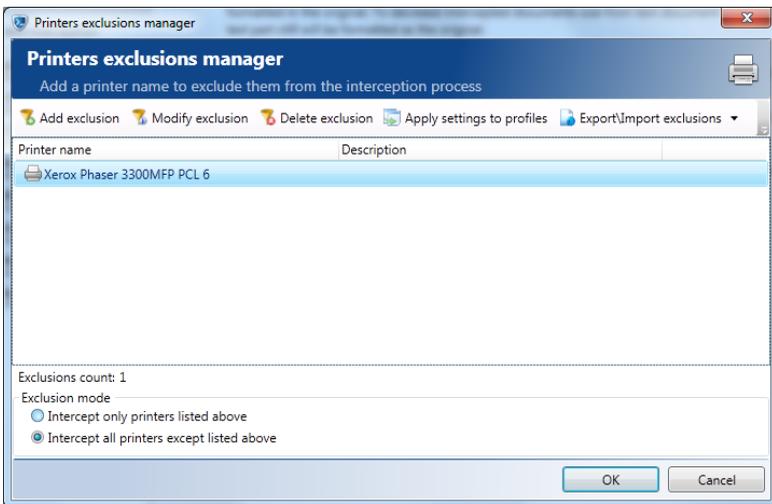
Printer exclusions

1. To disable interception of data sent to specific printers, click **Printer exclusions**.
2. To add a printer to exclusions, click **Add exclusion**.
3. Enter the name of the printer and description (optionally) into the corresponding text fields. You have to specify the full name the printer is registered with in your operating system. For example, the following printers are registered in the system:



In this case you have to specify the exact name of the printer, whether it is a local or network printer (for example, **HP LaserJet M1120n MFP on FG-PDC**).

4. After you have entered the name of the printer, click **Add**. The printer will appear on the exclusion list.



6. For other operation with exclusions follow the recommendations from [Managing interception exclusions](#) section.

Select the exclusion mode:

The radio buttons in the lower part of the exclusion manager window set the exclusion mode:

- **Intercept only printers listed above** (in case this option is selected, the system will only intercept documents sent to printers you have added into the list), or
- **Intercept all printers except listed above** (in case this option is selected, the system will intercept documents sent to any printers except those you have added into the list).

After you have specified all parameters in the exclusion manager, click **OK**.

11.4.1.6 Skype interception

If you need to intercept information transferred over desktop application or via web client Skype (user accounts, messages, files, voice calls), click the **Messengers interception** tab in the section of profile settings and enable it by checking the **Enable Skype interception** check box.

To configure Skype interception, click the **Settings** button next to the Skype control check box:

- enable Skype conversation interception (to intercept text messages between Skype accounts);
- enable interception of files transferred through Skype (to intercept files transmitted over Skype protocol);
- enable Skype calls interception (to intercept voice calls Skype-to-Skype, Skype-to-phone).

To save the settings, click **OK**.

Excluding Skype accounts from interception

1. To exclude certain Skype accounts from interception, click **Exclusions**.

To exclude a Skype account from the interception process, please add it into excluded accounts list:

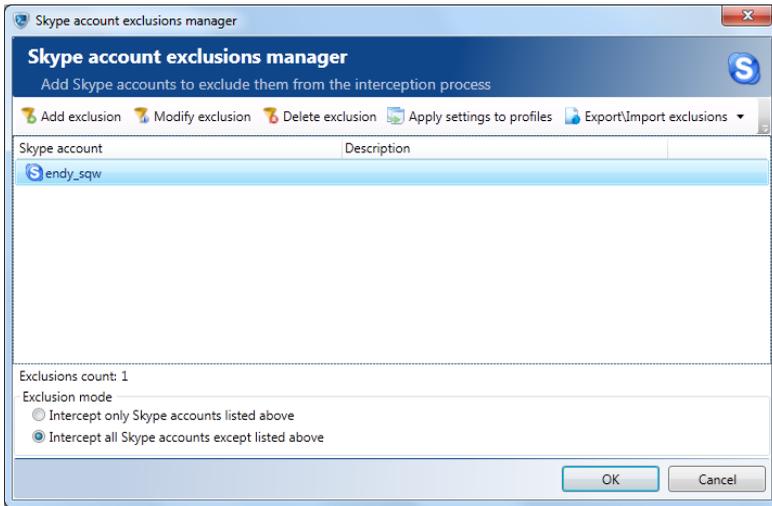
Exclusions

2. In the Skype account exclusions manager window, you will see two exclusion modes: a **white list** and a **black list** of Skype accounts. You can only select one type of exclusion mode to apply to the list of Skype accounts that you enter in the **Skype account** window.

- Once you mark the Skype accounts as included in to the **white list**, conversations with these accounts only will be intercepted; all other

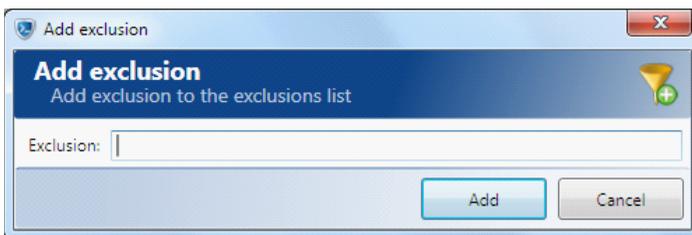
accounts will be ignored.

- If you mark the Skype accounts as included into the **black list**, conversations of all Skype accounts other than these will be intercepted; only the accounts listed in the **Skype account** window will be ignored.



Note: When working with the white and black lists of Skype accounts, please note that if any Skype conversation, including a group chat, involves any Skype user that is black-listed, such a conversation will not be intercepted. The same is valid for the opposite case: if any Skype conversation, including a group chat, involves any Skype user that is white-listed, such a conversation will be intercepted.

3. To add Skype accounts that you want to include into the black or white list, click **Exclusions**.



4. Enter the required Skype account in the **Exclusion** text box. Click **Add**.
5. For other operation with exclusions follow the recommendations from the [Managing interception exclusions](#) section.
6. To save the settings, click **OK**.

11.4.1.7 Viber interception

If you need to intercept information transferred over Viber (user accounts, messages, files, voice calls), click the **Messengers interception** tab in the section of profile settings and enable it by checking the **Enable Viber interception** check box.

To configure Viber interception, click the **Settings** button next to the Viber control check box:

- enable Viber conversation interception (to intercept text messages between Viber accounts);
- enable interception of files transferred through Viber (to intercept files transmitted over Viber protocol);
- enable Viber calls interception (to intercept voice calls Viber-to-Viber, Viber-to-phone).

To save the settings, click **OK**.

Excluding Viber accounts from interception

1. To exclude the certain Viber accounts from interception, click **Exclusions**.
2. In the Viber account exclusions manager window, you will see two exclusion modes: a **white list** and a **black list** of Viber accounts. You can only select one type of exclusion mode to apply to the list of Viber accounts that you enter in the **Viber account** window.
 - Once you mark the Viber accounts as included in to the **white list**, conversations with these accounts only will be intercepted; all other accounts will be ignored.
 - If you mark the Viber accounts as included into the **black list**, conversations of all Viber accounts other than these will be intercepted; only the accounts listed in the **Viber account** window will be ignored.

Note: *When working with the white and black lists of Viber accounts, please note that if any Viber conversation, including a group chat, involves any Viber user that is black-listed, such a conversation will not be intercepted. The same is valid for the opposite case: if any Viber conversation, including a group chat, involves any Viber user that is white-listed, such a conversation will be intercepted.*

3. To add Viber accounts that you want to include into the black or white list, click **Exclusions**.
4. Enter the required Viber account in the **Exclusion** text box. Click **Add**.
5. For other operation with exclusions follow the recommendations from the [Managing interception exclusions](#) section.
6. To save the settings, click **OK**.

11.4.1.8 Telegram interception

If you need to intercept information transferred over Viber (user accounts, messages, files, voice calls), click the **Messengers interception** tab in the section of profile settings and enable it by checking the **Enable Viber interception** check box.

To configure Viber interception, click the **Settings** button next to the Viber control check box:

- enable Viber conversation interception (to intercept text messages between Viber accounts);
- enable interception of files (including voice messages) transferred through Telegram (to intercept files transmitted over Telegram protocol);

To save the settings, click **OK**.

Excluding Telegram accounts from interception

1. To exclude the certain Telegram accounts from interception, click **Exclusions**.
2. In the Telegram account exclusions manager window, you will see two exclusion modes: a **white list** and a **black list** of Telegram accounts. You can only select one type of exclusion mode to apply to the list of Telegram accounts.
 - Once you mark the Telegram accounts as included in to the **white list**, conversations with these accounts only will be intercepted; all other accounts will be ignored.
 - If you mark the Telegram accounts as included into the **black list**, conversations of all Telegram accounts other than these will be intercepted; only the accounts listed in the **Telegram account** window will be ignored.

Note: *When working with the white and black lists of Telegram accounts, please note that if any Telegram conversation, including a group chat, involves any Telegram user that is black-listed, such a conversation will not be intercepted. The same is valid for the opposite case: if any Telegram conversation, including a group chat, involves any Telegram user that is white-listed, such a conversation will be intercepted.*

3. To add Telegram accounts that you want to include into the black or white list, click **Exclusions**.
4. Enter the required Telegram account in the **Exclusion** text box. Click **Add**.
5. For other operation with exclusions follow the recommendations from the [Managing interception exclusions](#) section.
6. To save the settings, click **OK**.

11.4.1.9 SIP interception

If you need to intercept information transferred over SIP (user accounts, messages, voice calls), click the **Messengers interception** tab in the section of profile settings and enable it by checking the **Enable SIP interception** check box.

To configure SIP interception, click the **Settings** button next to the SIP control check box:

- enable SIP conversation interception (to intercept text messages between SIP accounts);
- enable SIP calls interception (to intercept voice calls SIP-to-SIP, SIP-to-phone).

To save the settings, click **OK**.

Note: *If a safe encoded connection between SIP clients is supported within your network, interception of the information transferred on the SIP protocol will not be carried out.*

Excluding SIP accounts from interception

1. To exclude certain SIP accounts from interception, click **SIP account exclusions**.
2. In the SIP account exclusions manager window, you will see two exclusion modes: a **white list** and a **black list** of SIP accounts. You can only select one type of exclusion mode to apply to the list of SIP accounts that you enter in the **SIP account** window.
 - Once you mark the SIP accounts as included in to the **white list**, conversations with these accounts only will be intercepted; all other accounts will be ignored.
 - If you mark the SIP accounts as included into the **black list**, conversations of all SIP accounts other than these will be intercepted; only the accounts listed in the **SIP account** window will be ignored.

Note: *When working with the white and black lists of SIP accounts, please note that if any SIP conversation, including a group chat, involves any SIP user that is black-listed, such a conversation will not be intercepted. The same is valid for the opposite case: if any SIP conversation, including a group chat, involves any SIP user that is white-listed, such a conversation will be intercepted.*

3. To add SIP accounts that you want to include into the black or white list, click **Exclusions**.
4. Enter the required SIP account in the **Exclusion** text box. Click **Add**.
5. For other operation with exclusions follow the recommendations from [Managing interception exclusions](#) section.
6. To save the settings, click **OK**.

11.4.1.10 Lync interception

To intercept information transferred over Viber (user accounts, messages, files, voice calls), click the **Messengers interception** tab in the section of profile settings and enable it by checking the **Enable Lync interception** check box.

To configure Viber interception, click the **Settings** button next to the Viber control check box:

- enable Lync conversation interception (to intercept text messages between Lync accounts);
- enable audit of files transferred through Lync (to record and store data about files transmitted over Lync protocol, not files content);
- enable Lync calls interception (to intercept voice calls Lync-to-Lync, Lync-to-phone).

To save the settings, click **OK**.

Excluding Lync accounts from interception

1. To exclude a Lync accounts from interception, click **Exclusions**.
2. In the Lync account exclusions manager window, you will see two exclusion modes: a **white list** and a **black list** of Lync e accounts. You can only select one type of exclusion mode to apply to the list of Lync accounts that you enter in the **Lync account** window.
 - Once you mark the Lync accounts as included in to the **white list**, conversations with these accounts only will be intercepted; all other accounts will be ignored.
 - If you mark the Lync accounts as included into the **black list**, conversations of all Lync accounts other than these will be intercepted; only the accounts listed in the **Lync account** window will be ignored.

Note: *When working with the white and black lists of Lync accounts, please note that if any Lync conversation, including a group chat, involves any Lync user that is black-listed, such a conversation will not be intercepted. The same is valid for the opposite case: if any Lync conversation, including a group chat, involves any Lync user that is white-listed, such a conversation will be intercepted.*

3. To add Lync accounts that you want to include into the black or white list, click **Exclusions**.
4. Enter the required Lync account in the **Exclusion** text box. Click **Add**.
5. For other operation with exclusions follow the recommendations from [Managing interception exclusions](#) section.
6. To save the settings, click **OK**.

11.4.1.11 Browser interception

To intercept browser navigation, click the **Browsers interception** tab of the **Endpoint agent settings profile** window and enable it by checking the **Enable browsers interception** check box.

Once the option is activated the browsers check box is available for choice.

To enable one or more browsers interception, select the corresponding check boxes.

To exclude data about visiting some particular URL from browsers interception:

1. Click **URL exclusions**.
2. Click **Add exclusion** in the exclusion manager window.
3. Type the URL address (or its mask) in the **Exclusions** text field. The symbols "*" and "?" can be used to specify the address mask.
4. Type description in the corresponding text field if necessary.
5. For more details on operating with exclusions see [Managing interception exclusions section](#).

11.4.1.12 Control of network shares

The system enables control of usage of network shares in a local network. To configure options of network shares audit, control and data interception, click the **Network share interception** tab of the **Endpoint agent settings profile** window.

A set of flexible control options enables configuring audit, shadow copy, access and writing policies for specific network shares. The file operations control considering files extensions is provided as well. Network shares names and files extensions are specified by system administrator upon exclusions configuring for a particular control procedure.

File operations audit

The system enables audit of file operations with network shares, herewith fixation of copying to network shares is performed. The full file name, file size as well as the name of the process that has started the recording are intercepted and saved by the agent. The files content isn't intercepted and stored. Audit of files operations is provided regardless of other control procedures settings.

To enable the audit function select the **Audit file operations** check box.

Set a specific audit mode for particular network shares and for files with different extensions:

- To specify exclusions from audit for the particular network shares click **Audit exclusions** button. Follow the instruction from [Excluding according to network share name](#) section to configure an audit mode.
- To specify exclusions from audit for files with the particular extensions, click **File extensions** in the corresponding section (the bottom group of buttons). Follow the instruction from [Excluding according to files extensions](#) section to configure an

audit mode.

Note: Audit and interception are provided for files with non-zero size by default, select the corresponding check box to control zero-size files as well.

Control procedures

To configure control procedures, select the **Enable network shares control** check box.

SecureTower enables interception of data transferred to network shares as well as access and writing restriction.

Interception of information is carried out by **SecureTower** agent by shadow copying of the data transferred to network shares. Thus the copy of the intercepted data is stored in the shadow copy storage located on the local user computer, and then is transferred to the Endpoint agent control server to save the data to the database. By default, the size of shadow copy storage is 1000 MB. When exceeding this threshold the description of the intercepted files is transferred only. Shadow copies of the intercepted information is accessible in **SecureTower** Client Console.

To intercept the information copied to network shares, select the corresponding option, and then configure the necessary parameters:

- To set a shadow copy policy for the particular network shares, click **Interceptions exclusions**. Follow the instruction from [Excluding according to network share names](#) section.
- To set a shadow copy policy for files with the particular extensions, click **File extensions** in the corresponding section. Follow the instruction from [Excluding according to files extensions](#) section.

Note: If the shadow copy option is active, interception and storage of all data transferred to all network shares are performed by default.

When interception of the file copied to storage device is taken place file size is considered. By default, files with size smaller than 100 MB are copied to shadow copy storage entirely. A shadow copy of the fragment consisted of the first 100 MB of data is made for files bigger than 100MB.

To optimize the interception process, set parameters of shadow copies saving. It can be useful for reduction of the shadow storage size:

- Type wanted size in the **Shadow copy file size limit** text box(MB);
- Type wanted size in the **Shadow copy storage size limit** text box(MB).

To configure access control select the **Control access to network shares** check box:

- To set an access control policy for the particular network shares click **Access exclusions**. Follow the instruction from [Excluding according to network share names](#) section.

To configure control of copying select the **Control writing to network shares** check box and configure the necessary settings:

- To prohibit or allow to copy data to the particular network shares, click **Writing**

access exclusions. Follow the instruction from [Excluding according to network share names](#) section.

- To prohibit or allow to copy files with the particular extensions, click **File extensions** in the corresponding section. Follow the instruction from [Excluding according to files extensions](#) section.

Note: *If the control options is active, access and writing are enabled for all files extensions and all storage devices by default.*

Excluding according to network share name

A specific network share can be specified in the **Network shares exclusions manager** window.

1. Click the necessary exclusion mode radio button to select the mode. There are two exclusions modes in exclusions manager window: a **white list** and a **black list** of folders. You can select only one type of exclusions modes to apply to the list:
 - Once you mark the list of network shares as included into the **white list**, control procedure will be applied only to these network shares; all other will be ignored.
 - If you mark the list as included into the **black list**, control procedure will be applied to all network shares other than specified in the list; only the folders listed in the list will be ignored.

Note: *The second exclusion mode is selected by default.*

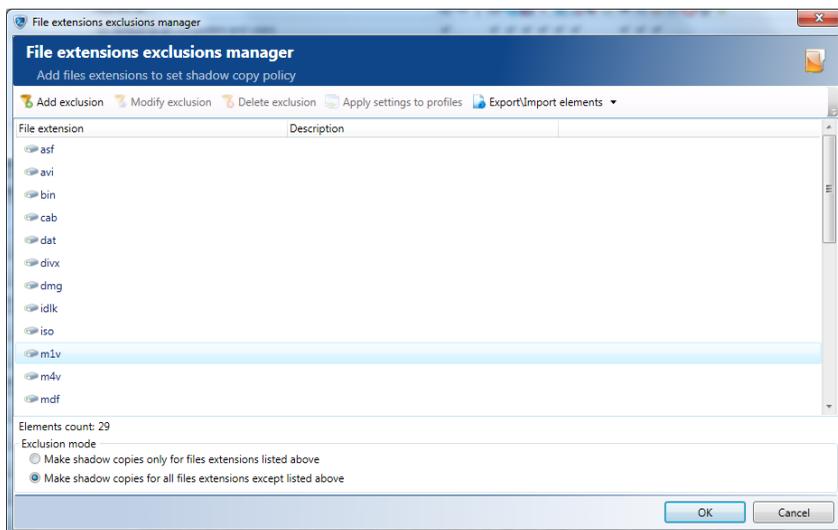
2. To add a network share in exclusions, click **Add exclusion** and type the network name of network share and description (optionally) in the corresponding text fields. To add exclusion, click **Add**.

The list of specified exclusions will be displayed in the manager window. The quantity of the listed exceptions is displayed in the **Exclusions count** field. .

3. For other operation with exclusions follow the recommendations given in [Managing interception exclusions](#) chapter.
4. To save exclusions, click **OK** in the **Devices exclusions manager** window.

Excluding according to files extensions

The excluded extensions are displayed in the **File extensions exclusions manager** window in the list form. The default list of excluded files extensions that potentially considered as not a security threat are used in the system.



1. Click the necessary exclusion mode radio button to select the mode. There are two exclusions modes in exclusions manager window: a **white list** and a **black list** of extensions. You can select only one type of exclusions modes to apply to the list:
 - Once you mark the list of extensions as included into the **white list**, only file with these extensions will be under control; all files with other extensions will be ignored.
 - If you mark the list of extensions as included into the **black list**, files with other than these extensions will be under control; only the traffic of files with extensions listed in the window will be ignored.

Note: *The second exclusion mode is selected by default.*

2. To add extension in exclusions, click **Add exclusion** and type in the **Exclusions** field the extensions of your choice (start a new one in the new line) and description (optionally). The list of selected exclusions will be displayed in the manager window. The quantity of the listed exceptions is displayed in the **Exclusions count** field.
3. For other operation with exclusions follow the recommendations given in [Managing interception exclusions](#) chapter.
4. To save exclusions, click **OK** in the **File extensions exclusions manager** window.

Process exclusions from the common control settings

To exclude the certain processes from the allowing policies (the "white list" mode is set specified previously while configuring audit, shadow copy and access control settings, click the **Processes exclusions** button and configure the exclusions in the **Process exclusions manager** window.

There are two modes in the exclusions manager window: a **white list** and a **black list** of

processes. One can select only one type of exclusion mode to apply to the list of processes names.

- Once you mark the list as included into the **white list**, checked control type of these processes interactions with network shares will be prohibited.
 - If you mark the list as included into the **black list**, processes with the names other than these will be excluded from the allowing policies (SecureTower control of this processes interactions with network shares will be prohibited); only for the processes listed in the window the allowing common control settings will stay valid.
1. Check the necessary radio button to set the exclusions mode.
 2. To add process name to the list click **Add** and type the necessary name in the **Exclusion** text field. To select a process from the running on the controlled workstations at the moment the **Selection** icon  and select the necessary process in the list.
 3. Select the necessary control type check box in the **Scope** section:
 - Select **Access control** if it is necessary to prohibit access to network shares that are allowed to use for the specified processes .
 - Select **Writing control** if it is necessary to prohibit writing to allowed network shares for the specified processes.
 - Select **Shadow copy** if it is necessary to prohibit shadow copying of data transferred to allowed network shares by the specified processes.
 - Select **Audit** if it is necessary to prohibit audit of file operations with allowed network shares for the specified processes.
 4. Comment the exclusion if necessary.
 5. Click **Add** to finish. The list of the processes with all exclusions settings will be displayed in the manager window. To change the exclusion scope select or clear the necessary exclusion type check box.
 6. For other operation with exclusions follow the recommendations given in [Managing interception exclusions](#) chapter.
 7. To save exclusions, click **OK**.

11.4.1.13 Cloud storage control

SecureTower enables control of usage of cloud storages and provide interception of the data transferred in both ways: from a local PC to a cloud storage as well as data copied from a cloud storage to a local PC. SecureTower provides control of both the web interface and the desktop application based interaction with cloud storages.

To set up parameters of file operations with cloud storages audit, access control and interception of information copied from/to cloud storages, click the **Cloud storages control** tab of the **Endpoint agent settings profile** window and select the **Enable cloud storages control** check box.

Cloud storage	Access	Audit	Shadow copy
Dropbox	Full access ▾	All files ▾	All files ▾
OneDrive	Read only ▾	Outgoing files ▾	Outgoing files ▾
Yandex.Disk	Access denied ▾	Incoming files ▾	Disabled ▾

There are a wide range of settings available for cloud storages control configuring:

1. To set the access level of reading, copying or writing operation for users or processes select the necessary status from the drop-down list in the **Access** column.
2. To set the status of file operations audit, check if the access is not denied and select the necessary status from the drop-down list in the **Audit** column. The full file name, file size as well as the name of the process that have started an operation are intercepted and saved by the agent. The files content isn't intercepted and stored.

Note: *Audit function is provided for files with non-zero size by default, select the corresponding check box to audit zero-size files as well.*

3. To specify the status of interception and shadow copying of the data received/sent to cloud storage, check if the audit and access are not denied for this storage and select the necessary status from the drop-down list in the **Shadow copy** column.

Interception of information is carried out by **SecureTower** agent by shadow copying of the data transferred to/from cloud storages. The copy of the intercepted data is stored in the shadow copy storage located on the local computer, and then is transferred to the Endpoint agent control server to save the data to the database. By default, the size of shadow copy storage is 1000 MB. When exceeding this threshold the description of the intercepted files is transferred only. Access to shadow copies of the intercepted information is provided from Client Console.

In case of interception the size of files is considered. By default, files with size smaller than 100 MB are copied in shadow copy storage entirely. Shadow copying of the fragment consisting of the first 100 MB of data is made for files with bigger size.

To optimize interception set wanted parameters of shadow copies. It can be useful for reduction of shadow copy storage size:

- Type wanted size in the **Shadow copy file size limit** (MB) text field;
- Type wanted size in the **Shadow copy storage size limit** (MB) text field.

Files exclusions

To exclude the certain files from the common control setting in accordance with their extensions as well as to familiarize with the default exclusions click **File extension exclusions**. Follow the recommendations given below:

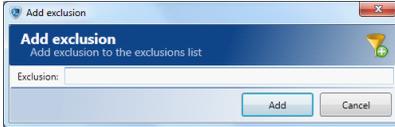
In exclusions manager window, you will see two exclusion modes: a **white list** and a **black list** of file extensions. You can select only one type of exclusion mode to apply to the extensions list.

- Once you mark the list of extensions as included into the **white list**, file with this extensions only will be excluded from the common control settings; all files with other extensions will be controlled as it was specified before.

- If you mark the list of extensions as included into the **black list**, files with other than these extensions will be excluded from the common control settings; only the files with extensions listed in the window will be controlled as it was specified before .

Note: *The second exclusion mode is selected by default.*

1. To add extension in exclusions, click **Add exclusion** and type in extensions you need to exclude.

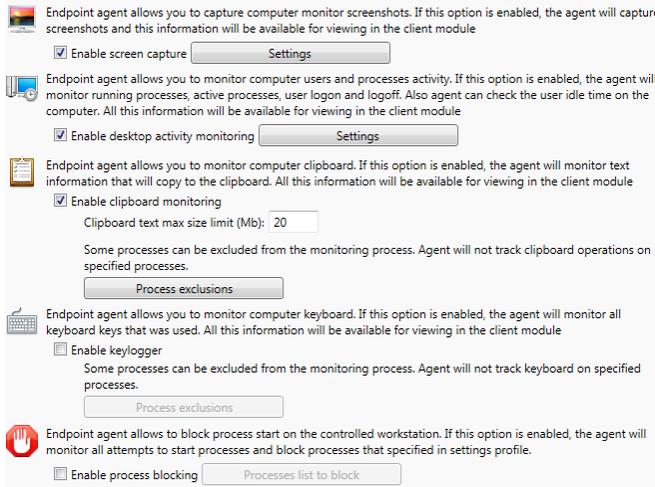


The list of selected exclusions will be displayed in the manager window. The quantity of listed exceptions is displayed in the **Exclusions count** field.

2. For other operation with exclusions follow the recommendations given in [Managing interception exclusions](#) chapter.
3. To save exclusions, click **OK**.

11.4.1.14 Desktop activity

The system enables making screenshots of user computers with installed agents at predefined intervals. To configure screenshot parameters, click the **Desktop activity** tab of the **Endpoint agent settings profile** window.

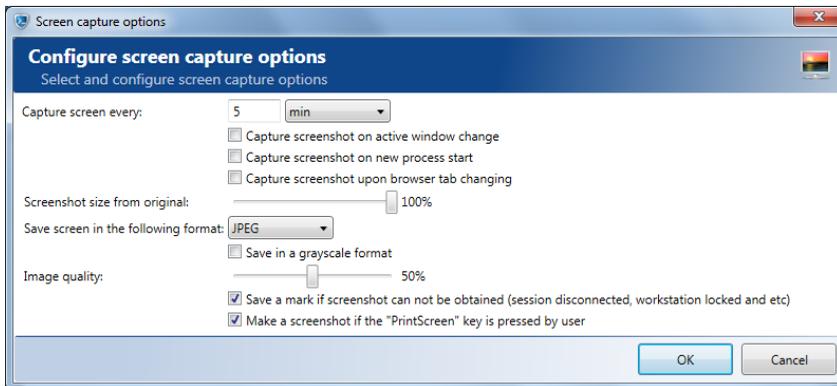


The screenshot shows the 'Desktop activity' settings window. It contains four main sections, each with a description, a checked checkbox, and a 'Settings' button:

- Enable screen capture:** Endpoint agent allows you to capture computer monitor screenshots. If this option is enabled, the agent will capture screenshots and this information will be available for viewing in the client module.
- Enable desktop activity monitoring:** Endpoint agent allows you to monitor computer users and processes activity. If this option is enabled, the agent will monitor running processes, active processes, user logon and logoff. Also agent can check the user idle time on the computer. All this information will be available for viewing in the client module.
- Enable clipboard monitoring:** Endpoint agent allows you to monitor computer clipboard. If this option is enabled, the agent will monitor text information that will copy to the clipboard. All this information will be available for viewing in the client module. Below this is a 'Clipboard text max size limit (Mb): 20' field and a 'Process exclusions' button.
- Enable keylogger:** Endpoint agent allows you to monitor computer keyboard. If this option is enabled, the agent will monitor all keyboard keys that was used. All this information will be available for viewing in the client module. Below this is a 'Process exclusions' button.

At the bottom, there is an option for 'Enable process blocking' with a 'Processes list to block' button.

Screen capture



The screenshot shows the 'Configure screen capture options' dialog box. It has a title bar with 'Screen capture options' and a close button. The main area is titled 'Configure screen capture options' and 'Select and configure screen capture options'. It contains the following settings:

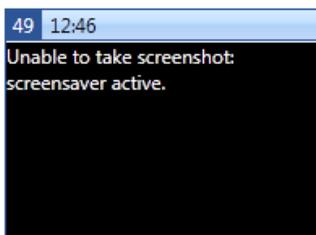
- Capture screen every:** 5 min (dropdown)
- Capture screenshot on active window change
- Capture screenshot on new process start
- Capture screenshot upon browser tab changing
- Screenshot size from original:** 100% (slider)
- Save screen in the following format:** JPEG (dropdown)
- Save in a grayscale format
- Image quality:** 50% (slider)
- Save a mark if screenshot can not be obtained (session disconnected, workstation locked and etc)
- Make a screenshot if the "PrintScreen" key is pressed by user

Buttons for 'OK' and 'Cancel' are at the bottom right.

1. To enable screen capture function, select the corresponding option.
2. To specify the conditions on which screenshots will be taken, click **Settings** next to the screen capture check box.
3. Type a period value into the **Capture screen every** text field and select a unit of measurement – minutes or hours – from the drop-down list to the right. *The specified interval is calculated from the moment when the previous screenshot was made and*

doesn't depend on the matter of capturing.

4. To specify additional conditions of the capture, select:
 - **Capture screenshot on active window change.** Agent will make screenshot upon toggling between active windows (the active window is in front of other windows), for example, toggling between Word and Excel open windows. If any system process was activated or **SecureTower** endpoint agent couldn't find a way to executable file of application, a screenshot will not be captured.
 - **Capture screenshot on new process start.** Agent will make screenshot every time when a new process is started on the controlled computer.
 - **Capture screenshot upon browser tab changing.** Agent will make screenshot when user switches between tabs in the web browser window.
5. Drag the slider to set the size of screenshots to be taken in percentages from the original desktop resolution. This option can be useful to decrease the disk space needed to store the screenshots.
6. Select a format to save screenshots from the drop-down menu – PNG or JPEG. You can check the **Save in a gray scale format** option to reduce output file size.
7. If you have selected JPEG format for screenshots, you can adjust the quality of images by dragging the **Image quality** slider. The higher the quality of the image, the more disk space will be occupied by the screenshot files.
8. If option **Save a mark if screenshot cannot be obtained** is checked, the system will save and display a blank (black) screen whenever it is impossible to obtain a screenshot. The blank screen will display an error message stating the reason why a screenshot could not be taken at specific time.



Possible error messages include:

- Unable to take screenshot due to unknown error.
 - Unable to take screenshot: error while taking the screenshot.
 - Unable to take screenshot: screensaver active.
 - Unable to take screenshot: computer idle.
 - Unable to take screenshot: session inactive.
9. To make a screenshot when the "Print Screen" key is pressed select the corresponding option.

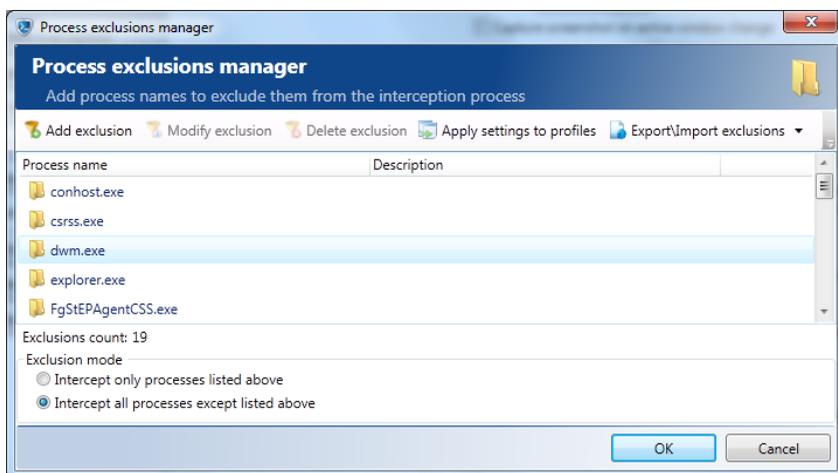
Attention: If the **Capture screenshot on active window change** option is checked a total amount of screenshots will increase seriously and a network overloading will occur as a result. Activating of this option for profiles with restricted quantity of objects is recommended.

User and process activity monitoring

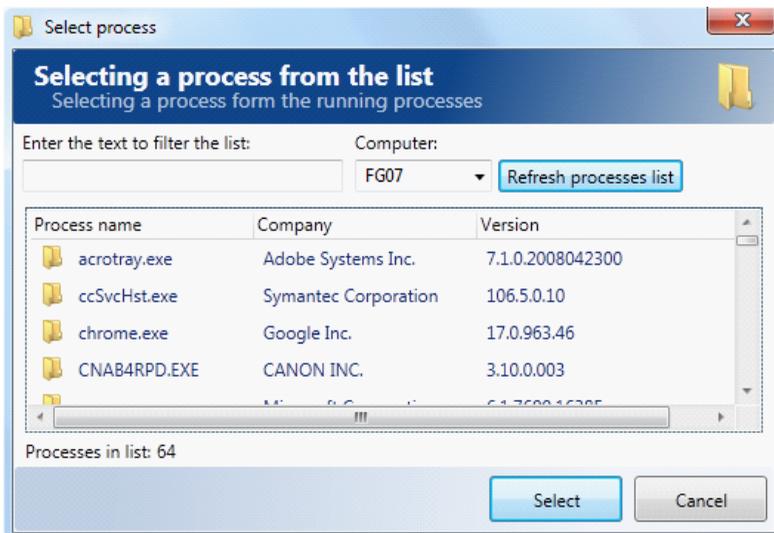
SecureTower system can monitor the endpoint activity, gathering statistics on computer active/idle time and applications (including Win RT (Metro) and virtual desktop) run by users.

To enable the function, select **Enable desktop activity monitoring** check box.

To exclude the certain processes from the application statistics:



1. Click the necessary exclusion mode radio button to select the mode. There are two exclusions modes in exclusions manager window: a **white list** and a **black list** of processes. You can select only one type of exclusions modes to apply to the list:
 - Once you mark the list of processes as included into the **white list (Intercept only processes listed above)**, only this processes activity will be under control; all other processes activity will be ignored.
 - If you mark the list of processes as included into the **black list (Intercept all processes except listed above)**, the system will ignore start and stop of the processes listed, herewith the statistics on all other processes will be collected.
2. To add new processes to the list, click **Add exclusion**.
3. Enter the name in the text field of the dialog box, or click  next to the text field.



The process selection window displays all processes running on the selected computer.

To view a list of processes run on another computer, select it from the **Computer** drop-down menu and click **Refresh processes list**. To facilitate search for a specific process in the list type the characters contained in the name of the process into the filtering text box. Highlight the desired process in the list and click **Select**.

4. In the exclusions dialog box, click **Add**. The process will be added to the list of exclusions.
5. For other operation with exclusions follow the recommendations from [Managing interception exclusions](#) section.
6. To save the settings, click **OK**.

After the necessary exclusions are configured, the period (in minutes) of user inactivity (absence of keyboard hits, mouse movements and clicks), after which the system will mark the computer as idle, can be set. By default the inactivity period is set to 5 minutes.

Clipboard monitoring

SecureTower system enables tracing clipboard contents at workstations. All acquired information will be available for viewing from Client Console and can be analyzed automatically in Security Center (in case of appropriate policies setup).

To enable the function of clipboard monitoring check corresponding option.

To exclude operations with clipboard in particular applications from interception, click the **Processes exclusions** button in the corresponding section and specify the list of such processes name as described [above](#).

Keylogger

SecureTower provides complex information about users computer activity by using keystroke logging. To enable recording (or logging) the keys struck on a keyboard select corresponding check box. All data about struck keys and corresponding applications are available from Client Console and can be analyzed automatically in Security center (in case of appropriate policies setup).

To exclude user activity on keyboard in particular applications from interception, click the **Processes exclusions** button in the corresponding section and specify the list of such processes name as described [above](#).

Process activity blocking

EndPoint Agent not only controls processes activity but provides user with tool of disabling the particular processes start. To create the list of processes which start must be blocked, enable the corresponding option and click **Processes list to block**. Add processes attributes to the list as described below:

1. To add a new attribute to the list click **Add**.
2. Click the button with predefined attribute type in the corresponding field, then click the necessary exclusion type to select it.
3. Type the attribute in accordance with selected type in the **Attribute** text field, or click the **Selection** icon next to the text field. The processes of selected workstation with their attributes will be listed in the newly opened window. To view a list of processes run on another computer, click the unfold button of the **Computer** drop-down list, select the necessary computer name in the list and click **Refresh processes list**. To facilitate search for a specific process in the list type the characters contained in the name of the process into the filtering text box. Highlight the desired process in the list and click **Select**.
4. Click **Add** in the blocking manager window.
5. For other operation with exclusions follow the recommendations from [Managing interception exclusions](#) section.

The processes from the list can't be started on the controlled workstation.

11.4.1.15 Audio/video Monitoring

To enable online listening to audio from microphone (or other audio recording device) connected to workstation and viewing video from user desktops and to configure scheduler for auto recording, click the **Audio/video Monitoring** tab of the **Endpoint agent settings profile** window. Auto recording is also available for audio stream from speakers and for video from web camera.

Note 1: *Speakers auto recording is supported on Windows Vista and above.*

Note 2: *If there is more than one microphone connected to workstation, only the one, that is set by default in system, will be available for monitoring .*

1. Select the **Enable audio/video monitoring** option check box.
2. To allow desktop video viewing, select the **Enable desktop viewing** check box.
3. To allow listening to audio from the microphone connected to controlled workstation, select the **Enable microphone listening** check box.
4. Enter the port number to establish connection between agent and Client Console in the **Connection port** text box.
5. To create an *Inbound Port Allow Rule for Windows Firewall* while connecting automatically, select the corresponding option check box.
6. To create a scheduler for auto recording, click **Add schedule** in the corresponding section of the window. Configure schedules for auto recording of microphone and speakers audio and for web camera and desktop video. For more information about schedule configuring, see [Configuring the scheduler](#).
7. To set the mode of video recording, click the relevant radio button under the scheduler table:
 - To record video in color format, click **Color**.
 - To record video in black-and-white, click **Grayscale**.

Note 3: *If a web camera is used by another application (e.g. Skype) at start of auto recording, the agent can not connect to the cam and the recording can not be performed. And vice versa, while auto recording video from web camera, it will be not available for other program.*

11.4.1.16 Data blocking

To block traffic of data, click the **Data blocking** tab of the **Endpoint agent settings profile** window.

Data blocking is intended to block e-mail messages transferred with MAPI and SMTP and data transferred with HTTP(S). When sending, all SMTP and MAPI messages and HTTP POST and GET requests with attachments will be intercepted and analyzed by Endpoint agent control server to find content that meet search conditions of blocking rules.

Note: *Analysis of SMTP message can be time consumable depending on the message data size and a mail server connection speed. When large volumes of data or slow connection are taking place a time delay required for the analysis can lead to mail server connection lost because of the mail server response timeout exceeding. It is recommended to increase the value of timeout to 10 minutes (according to the SMTP specification) in mail client settings for computer with **SecureTower** endpoint agent.*

If the SMTP and MAPI message is analyzed successfully and sending is approved, it will be sent to the mail server for further processing and delivery to the recipient. The fact of interception and analysis remains invisible for the user.

If the data transferred with message activates one or more rules, transfer of such messages will be blocked. In this case, the user will get an error message: "Message was blocked by security policy!" in mail client window for SMTP case and a message with notification about failure for MAPI case. E-mail messages that are blocked by the system are placed in the database, and additional attribute "Blocked" with a list of rules, which led to the data blocking is added to messages attributes .

HTTP blocking is similar to SMTP, blocking rules can be set up for both the HTTP POST and the GET request by the means of corresponding blocking rules. HTTP GET blocking makes it possible to deny browsing specified insecure sites. HTTP POST blocking enables control and prevention of any Internet activity such as posting in web-chats, social networks conversations, activity of specified malicious and utility software and so on.

If the data transferred over HTTP(S) activates one or more rules, transfer will be blocked. In this case, the user will get an error message: "Content is not available due to corporate security policy!" in his web browser window. The message can be customized by system administrator (for details see [Http blocking message editing](#)).

Note: To receive notifications about blocking rules operation add corresponding security rule in Security Center of **SecureTower Client Console** (for details, see **General security rule of User Guide**). Alerts for incidents connected with web-sites attending (HTTP-GET) are not supported in the current version of the system.

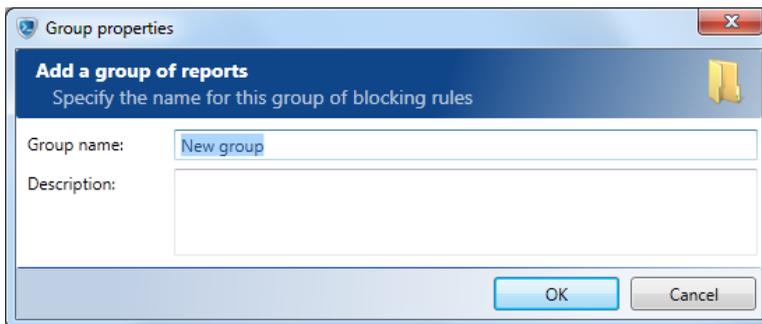
To activate blocking mode, add a blocking rule or group of rules as described below.

Creating a group

The root **Blocking rules** group is created by default and unavailable for deleting. Within the **Blocking rules** group creation of other groups or single rule is possible. Groups and rules can be created at any hierarchy level as well.

To create a new group of rules:

1. On the **Add** menu, click **Group** or right-click the root group in the list, point **Add**, and then click **Group**.
2. In the **Group name** text box of the opened dialogue window, enter the name of the created group of rules.
3. Fill out the **Description** text box (optional) with the group description.



4. To save the settings, click **OK**. The newly added group appears in the list of blocking rules and is switched on by default.
5. If it is necessary to save the group but not use it (with all enclosures), clear its check box.
6. Configure the blocking rule as described further.

To modify a group name and description, click the necessary group and click **Modify** on the tab ribbon toolbar or right-click it in the list and click **Modify**. In the opened dialogue window, make the necessary changes in accordance with the instructions provided above.

To delete a group, click the necessary one and click **Delete** on the tab ribbon toolbar or right-click it in the list and click **Delete**. In the action confirmation dialogue window, click **Yes**.

The information for each group (rule) with the name and the description of the group (rule) is displayed in the window. Content of the group can be expanded or collapsed by clicking the corresponding sign  /  next to the group name.



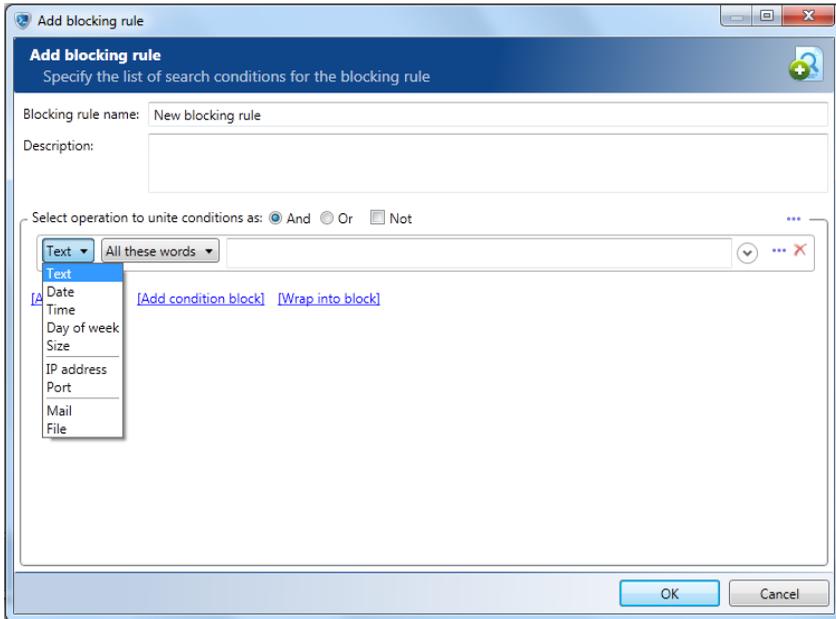
Note: To select or clear a number of check boxes simultaneously, press and hold **Ctrl** or **Shift** on your keyboard and click the necessary rules to highlight them, then right-click any highlighted rule and click the necessary command in the context menu.

Creating a new SMTP or MAPI blocking rule

To create a new rule:

1. Click the group which this rule will be related to.
2. Click **Add** in the ribbon toolbar of the window or right-click the rule in the list and point **Add** in the context menu.
3. Click **SMTP blocking rule** or **MAPI blocking rule** (depending on protocol that is necessary to block).
4. Enter the name of the created rule in the **Blocking rule name** text box of the opened dialogue window
5. Fill out the **Description** text box (optional) with the rule description.
6. Click **Add condition** link to specify conditions.
7. In the section under the **Description** text box specify the conditions for the search, that will be conducted by the system in an automatic mode. Data can be searched by a certain text in the intercepted data, IP address (as well as local or remote), by the specified port (as well as local or remote), by the size of data and by the interception date. Condition types are available in the drop-down list opened by clicking **Text**. For various search conditions the different relevant operations can be specified (see below

for details).



8. To save the settings, click **OK**. The newly added rule appears in the list of blocking rules and is switched on by default.

9. If it is necessary to save the rule but not use it, clear its check box.

To modify a rule, click the necessary rule and click **Modify** on the tab ribbon toolbar or double-click the necessary rule or right-click the rule in the list and click **Modify**. In the opened dialogue window, make the necessary changes in accordance with the instructions provided above.

To delete a rule, click the necessary rule and click **Delete** on the tab ribbon toolbar or right-click it in the list and click **Delete**. In the action confirmation dialogue window, click **Yes**.

Text search

The possibility to search documents containing any of the specified words, all the words specified, an exact phrase or none of the words entered in the search query; if you enter several words into the line, they are to be separated by spaces; if you wish to add an exact expression alongside with separate words, the expression has to be put in quotes.

Besides, you can specify additional conditions of search by keywords. To add auxiliary conditions click the expand button  to the right of the text field:

- **Fuzzy search** - search for mistyped or similar words. When this option is checked, you can set a threshold, i.e. the extent to which the words detected in the traffic flows can differ from the ones entered into the text field. It is not recommended to set a high value of this parameter when searching for short words, as it may result in too many false positives of the security policy.
- **Word proximity** (applicable only to search by all specified words) - searching for all entered words taking account of their proximity in the text. For example, if value 5 is set, the security rule will be triggered if the system detects the search query words in the traffic flow, but only in case there are not more than 5 other words between them.
- **Strict word order** (only if “Word proximity” option is enabled) - If this option is enabled, the security policy will only work if the system detects the search query words in the exact same order as they were entered into the text field.
- **Transliteration** – transliteration is a feature that is only applied to the Russian language and used to search for Cyrillic words transliterated with Latin symbols.

Search by date

Specify one of the following conditions: **Equal** (search for data transferred on the specified date), **Not equal** (search for data transferred on any date except specified), **Within range** (search for data transferred during the specified period), **Beyond range** (search for data transferred on any date except the specified period).

Search by time and day of week

To search by time you can specify conditions similar to the ones for search by dates.

To search by day of week you can specify one of the following conditions: **Equal** (search for data transferred on the specified days of week) or **Not equal** (search for data transferred on any day of the week except specified).

Search by size

The size of SMTP message is assessed as size of SMTP file in .msg format. It should be kept in mind that the size of SMTP message in .msg format is always bigger than initial due to added caption and converting attachments to text format that cause increasing of transferred message size.

Specify the following conditions: **Equal** (search for documents of specified size), **Not equal** (search for documents of any size except specified), **Within range** (specifying

the smallest and largest size of documents to search for), **Beyond range** (search for documents of any size except specified range). Once you have entered a necessary number in the text field, specify the unit of measurement for the specified document size (**Bytes, Kilobytes, Megabytes, Gigabytes**).

Search by IP or port

When searching by IP addresses or ports, one can set the following parameters:

- **local or remote** (to search for data transmitted from/to local or remote computers having the specified IP addresses or via specified local or remote ports), **local** (to search only for data transmitted from/to the local computer with the specified IP address or via specified local port), **remote** (to search only for data transmitted from/to the remote computer with the specified IP address or via specified remote port);
- **equal** (to search for data transmitted from/to specific computer having the specified IP address or via specified port), **not equal** (to search for data transmitted from/to any computers except for the one having the specified IP address or via any port except for the specified one), **within range** (to search for data transmitted from/to computer having IP addresses within the specified range or via specified range of ports), **beyond range** (to search for data transmitted from/to any computers except for those having IP addresses within the specified range or via any port except for the specified range of ports).

Search in e-mail traffic

When searching in the e-mail traffic, one can set the following parameters:

- **from address** - search for e-mails that contain/do not contain the specified expression in the "Sender" field. Several entries separated by spaces can be specified in one condition line;
- **to address** - search for e-mails that contain/do not contain the specified expression in the "Recipient" field. Several entries separated by spaces can be specified in one condition line;
- **subject** (search for e-mails that contain/do not contain the specified expression in the "Subject" field);
- **other header fields** (search for e-mails that contain/do not contain the specified expression in other header fields);
- **messages with attachments** (search for e-mails that include/do not include attached files).

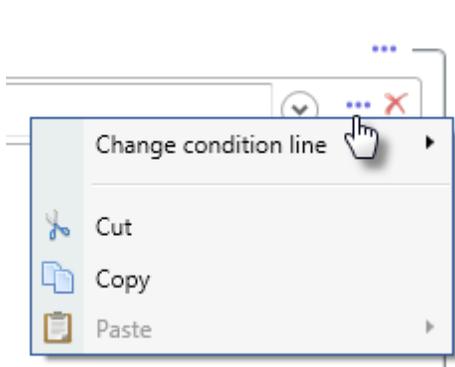
Search by file parameters

To search for files based on their **Names**, you can select one of the two further options – **Equal** or **Not equal** – to search for files with the specified name or any files except having the specified name (the name should be entered into the text field on the right)

In case you choose to search for files by their **Extensions**, you can select one of the three further options: **Equal** (search for files having the specified extension), **Not equal** (search for files having any extension except specified) or **Extension does not match** the file type (to search for files with a deliberately changed extension).

Search conditions

1. Search may be carried out with logical disjunction (the “**OR**” operation) or a logical conjunction (the “**AND**” operation) of several search conditions or condition block:
 - Upon selecting logical “**AND**” search operator, notifications will be delivered only in cases of information transfer is satisfy ALL the specified search conditions simultaneously. For this, in the **Select operation to unite conditions as section**, check the **And** option.
 - Upon selecting the “**OR**” search operation, notifications will be delivered in cases of information transfer is satisfy ANY of the specified search conditions or search condition blocks. For this, in the **Select operation to unite conditions as section**, check the **Or** option.
2. To add a new search condition, click the **Add condition** link. To delete some search condition, click the **Delete** icon  in the right part of the corresponding condition. By default, there is a form for entering the first search condition in this window, but it can be deleted if a search condition block should be created instead.
3. To add an entire search condition block, click the **Add condition block** link. Creating condition blocks helps conduct automatic search subject to complex or advanced search conditions. New blocks or conditions can be created within other blocks and conditions.
4. When creating a new or editing an existing rule numerous advanced procedures for search conditions and conditions block are available from the **Tools** menu (the icon in the end of a condition line).



To work with advanced procedures, click the **Tools** icon  and select a necessary one:

- To change the item line, point to **Conditions line change** and click one of available commands.
- Click **Cut** to remove selected item from the parent block body and copy it to clipboard. After applying this operation the **Paste** procedure is available for item that was cut within any blocking rule.
- Click **Copy** to copy selected item to clipboard. After applying this operation the **Paste** procedure is available for item that was copy within any blocking rule.
- The **Paste** procedure is available when any item was previously copied or cut. Point to **Paste**, and then:
 - To insert item from clipboard in the specified position within the parent block body, click **Paste into block**.
 - To paste item on the line above selected search condition or block, click **Paste above**.
 - To paste item on the line below selected search condition or block, click **Paste below**.
- Click **Copy search condition as image** to copy the root block of search conditions to clipboard as screenshot of the block body. This procedure is available for a root block only.
- Click **Save search condition as image** to save the root block of search conditions to clipboard as PNG format file with screenshot of the block body. This procedure is available for the root block only.

Creating a new HTTP/HTTPS blocking rule

To create a new rule:

1. Click the group which this rule will be related to.
2. Click **Add** in the ribbon toolbar of the window or right-click the rule in the list and point to **Add** in the context menu.
3. Click **HTTP blocking rule**.
4. Proceed as described in [Creating a new SMTP blocking rule](#) section of this chapter.

Data can be searched by a certain text in the intercepted data, IP address (as well as local or remote), by the specified port (as well as local or remote), by the size of data and by the interception date, by the Web-field parameters (field names of request header) and by the SSL connection establishment event. Condition and parameters types are available in drop-down lists.

Working with HTTP POST blocking conditions parameters is similar to SMTP, except **HTTP method**, **SSL** and **Web-field** conditions.

Attention: *To use functionality of blocking in proper way, it is necessary to familiarize with typical requests structure.*

Blocking by HTTP method

The system enables identification and blocking of GET and POST HTTP(S) requests.

To block any HTTP(S) request by the method it was sent use a corresponding parameter from the **HTTP method** blocking condition.

This type of blocking condition is useful to go with any other one to enhance a rule performance.

SSL - connection

To block encrypted HTTP request, select the **SSL** condition type and the **Yes** value or select **No** to enable only requests transferred over SSL.

Web - fields

System allows to block the HTTP(S) requests in accordance with results of content analysis of request web field. There are two ways to set the web-field that must be analysed: select the one from preset or specify the user-defined web field name.

To block requests in accordance with results of web field analysis:

1. Select the **Web-field** condition type from the list.

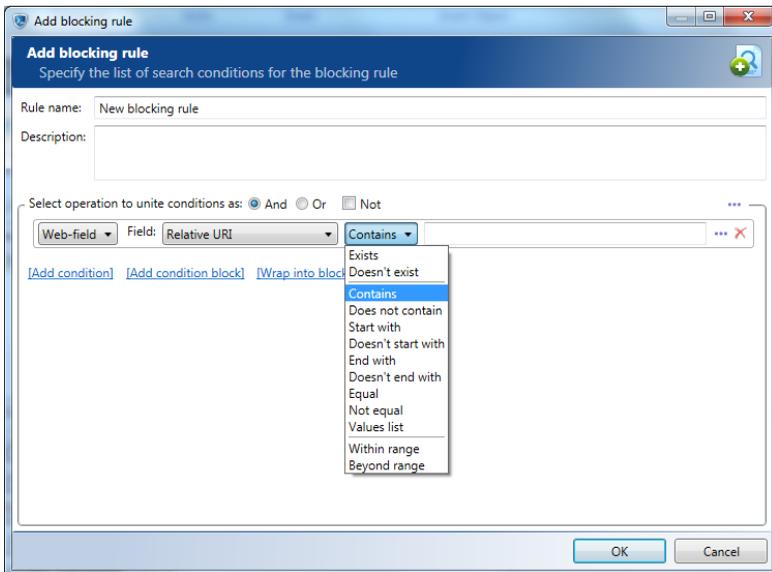
2. Set the web field name in the corresponding field:

- Select the one from preset name list:
 - **Relative URI** (requests with relative URI that satisfies search conditions will be blocked);
 - **Host** (requests with HOST field that satisfies search conditions will be blocked);
 - **Content-Length** (if the length of a request in byte satisfies search conditions, such request will be blocked);
 - **User-Agent** (requests with User-Agent field that satisfies search conditions will be blocked).

or

- Select the **Custom** filed in the list and type a web field name you need to control. For example, transfer of data with particular format can be blocked, using the **Content-Type** field name.

3. Select the compare parameter in the corresponding list and enter the value of search condition.



The combination of different types of search conditions enables high efficiency of blocking rules. For example, the combination of conditions which provide search for requests with both the **URI** field and the **Host** field contain specified symbols or text (parameters **Contains** or **Equal**), will allow administrator to deny access to separate web pages or elements of the particular web resource.

Using the **User-Agent** field with parameter **Is absent**, for example, allows administrator to disable network activity of the service and harmful software

which doesn't use this field in POST requests usually.

Using of customer field as search conditions can be useful too. So, restriction of transferred message size by defining the **Content-Length** field with the **Beyond range** parameter value in bytes is possible.

Export/Import filters

The system enables saving (exporting) the list of blocking rules into a file (*.strb) and subsequently restore (import) the list.

1. To export the rules list select **Export...** in the drop-down menu **Tools** in the **Blocking rules** tab .

In the new window select the rules which will be exported by checking the boxes in the corresponding lines. After you have selected the necessary rules, click **Export**.

In the new window, select a folder where you wish to save the file, specify the name of the file and click **Save**.

2. To import a list of rules from a previously saved file, select **Import ...** in the drop-down menu **Tools**.

In the new window select a folder and a *.strb file with rules.

After you have selected the file, click **Open**.

Next, one have to select the rules for import by checking the corresponding boxes and specify one of the following import modes:

- Update with replacing if rules names matching - if any of the current rules has the same name as any imported rule, it will be replaced with the new one;
- Update with renaming if rules names matching - if any of the current rules has the same name as any imported rule, the new rule will be renamed and imported under the new name;
- Replace the current rules with a new - all the current rules will be deleted and the new ones will be imported.

Click **Import**.

Http blocking message editing

To edit message text select the corresponding option from the drop-down **Tools** menu on the **Blocking rules** tab.

Edit the text in the text field and click **OK** to save the result.

Go to **SecureTower** Client Console to proceed working with blocked data (see Search results list, General security rule, Viewing notifications in Security Center chapters of

User Guide.)

Note: *The list of rules is common for all existed settings profile. When created the rule will be added automatically to all profile in inactive mode. To activate this rule in other profile go to a necessary profile and check the corresponding check box in the **Data blocking** tab.*

11.4.1.17 File system control

SecureTower agents keep track if any document with confidential content or data that need to be protected from unwanted disclosure are stored or appeared on the controlled workstation. Monitoring is conducted automatically and based on comparing the hashes of files from [files hash banks](#) with the ones in file system of workstation. Only the file hash is taken into account upon comparing (not a name or other file attributes).

The personal settings of file system control can be assigned to the particular users and workstations by specifying different hash banks in different profiles.

 **Attention!** *File system control will be effective only on the computers that was included into the list of computers for [indexing](#).*

To enable control of workstations and users file system that is specified as profile objects:

1. Select the **Enable hash data banks** check box.
2. Select the necessary data bank check box in the list. If the list is empty, create a data bank of hashes and proceed with file system control configuring. For more information see [Configuring files hash data banks](#).

If the control option is enabled and one or more data banks are selected, the file systems of workstations that belong to set of the current profile objects will be scanned by agents. The data concerning matches between hashes from controlled computers and data banks will be stored in the system database and can be accessed from Client Console.

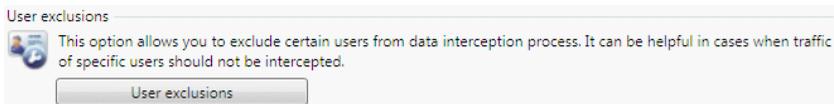
11.4.1.18 Miscellaneous agent settings

To access other settings of endpoint agents, click the **Other** tab of the **Endpoint agent settings profile** window.

Excluding users from interception

One can exclude a particular user from interception of all network traffic and from control of computer and user activity. If a user is excluded from interception, the agent will ignore all type of activity related to this user.

1. To exclude a certain user from interception, in the **Other** tab, click **User exclusions**.



2. In the exclusions manager window, you will see two exclusion modes: **white list** (the **Intercept only users listed above** radio button) and **black list** (the **Intercept all users except listed above** radio button) of users. You can only select one type of exclusion

mode to apply to the list of users that you enter in the **User name** window.

- Once you mark the users as included in to the **white list**, the network activities of these users only will be intercepted; all other users will be ignored.
 - If you mark the users as included into the **black list**, all network activities involving users other than these will be intercepted; only the users listed in the **User name** window will be ignored.
3. To add users that you want to include into the black or white list, click **Add exclusion**.
 4. Select the necessary user in the list of Active Directory users or from the localhost user list. For more information, see [Selecting a user account to start up](#).
 5. For other operation with exclusions follow the recommendations from [Managing interception exclusions](#) section.
 6. To save the settings, click **OK**.

Agent protection

For different protection modes select one of the options in the **Protection mode** drop-down menu:

- **Endpoint agent protection disabled** (the agent is not protected be termination or removal by user, and is not hidden in the process list);
- **Protect the endpoint agent on remote computer from terminating by user action** (if a user attempts to finish or delete the endpoint agent from their workstation, an operating system warning will be displayed informing of a possible system failure in case the user finishes the agent process; if the user continues agent termination, the system will restart and the agent will be recovered);
- **Hide the endpoint agent on the remote computer** (the agent process and service, as well as the agent files and folders will be hidden on the user computers).



Warning! In some cases agent masking function may cause a conflict with Antivirus software.

Agent visualization

Agent visualization inform an endpoint user about agent activity on workstation.

To allow agent visualization and to configure the agent alert messages, select the **Show agent icon in the system tray** option. The agent icon will be shown in the notification area (system tray). For cases, when traffic blocking is taken place, the alert about blocking will be displayed next to the agent icon in system tray.

To configure alert about blocking:

1. Click **Settings** next to the visualisations check box.
2. In the setting window select the type of blocking for which the alert is necessary to be configured.

3. If necessary, click **Configure notification** related to the blocking type, and then edit the text of alert and click **OK**.
4. Click **OK** to save the settings.

Local data storage

In case when a local data storage is enabled on endpoint agents, all data transmitted by the user while his computer is not connected to the corporate network, will be saved into a temporary storage on the endpoint, and when the computer is re-connected to the network, all stored data will be automatically transferred in a background mode to the server for analysis.

To enable/disable local data storage on endpoints, select/clear the corresponding check box.

Storage of the data is performed in rotation mode, the obsolete file will be replaced with the new one when the **Max storage size** is exceeded.

One can specify the followed data storage options:

- **Max storage size** - fixed size of data storage. The default value is 100 MB.
- **Restrict the storage size by free disc space** - dynamic size that considered as per cent of free space on the disk. Isn't specified by default.
- **Storing limit** - time limit for storing of intercepted information. The default value is 30 days. Value of storing limit must be within the 1-30 days range.

MS Outlook integration

MS Outlook integration enables interception of encrypted MAPI traffic.

To allow MS Outlook integration, select the corresponding option.

Note: *If MS Outlook integration is enabled, it is recommended to deactivate MAPI interception option in [Network traffic interception](#) tab.*

Communications with server speed restriction

To restrict the speed of data transfer between the server and the agent enter the speed value(KB/sec) in the corresponding field. Data will be transmitted with specified speed if another do not specified by the scheduler settings.

Schedule for agent data transfer

The transfer of data intercepted by the agent is governed by user-defined scheduler if the corresponding option is selected. In general, if the scheduler is not used in profile, the agent send all type of intercepted data.

To use scheduler, select the corresponding option. While configuring the scheduler one can select a data type to transfer to the server:

- all intercepted data;
- only auto recorded audio and video from user workstation captured while monitoring;
- all data except for auto recorded audio and video.

To restrict the speed of agent-server interaction, specify the necessary value for each schedule. If the schedule is created and using of scheduler is activated, data will be transmitted with speed specified by the schedule. Herewith, the maximum transfer speed will be ignored.

 **Attention!** *If the **Use scheduler** option is selected and no one scheduler is created or there is no one active schedule - the data transmission will not be performed from the agent to the server at all.*

For more information about configuring the scheduler, see [Configuring the scheduler](#).

Note: *To force agent to send data not on schedule, click the [General](#) tab of the Agents schema window or force sending from the [agent context menu](#).*

11.4.1.19 Managing interception exclusions

Working with exclusions

1. To modify/delete any exclusions, click the corresponding row in the list of exclusions and click **Modify** or **Delete exclusions** correspondingly.
2. To apply the settings of currently edited exclusions to any other existed profile, click **Apply setting to profiles**:

Select the necessary profiles from the list by checking corresponding check box in the **Apply to profiles** window. One can also use the selection buttons below the list:

- Click **Select all** to check all the profiles from the list.
- Click **Unselect** to cancel selection that was made before.
- Click **Inverse selection** to cancel selection that was made before and select all unselected profiles in the list simultaneously.

Select an integration mode from the **Replace mode** section:

- To update exclusions currently existed in selected profiles with exclusions from edited profile click **Update with new**.
- To replace exclusions currently existed in selected profiles with exclusions from edited profile click **Replace with new**.
- To change the exclusions mode of selected profiles to the currently edited mode select the corresponding check box.

Click **Apply to profiles** to finish with import of edited profile exclusions to selected

ones.

3. To import or export created exclusions click **Export/Import** in the exclusions manager window and select the necessary option from drop-down list:
 - Click **Import** to download the corresponding type of exclusions created previously to currently edited profile. In the newly opened window select the XML file with exclusions data to import and click Open to download it. In the opened **Import exclusions** window check the necessary exclusions to download and click **Import** to finish.
 - Click **Export** to upload currently edited exclusions to external XML file. In the newly opened window specify a name of file that need to be uploaded to and click **Save** to finish.

11.4.2 Managing profile list

1. To delete an existing agent settings profile, double-click a profile you need in the list and click corresponding command in the context menu or click **Delete profile** on the toolbar of the **Agent settings manager** window. In the confirmation dialog box, click **Yes**.
2. To disable an agent settings profile, double-click a profile you need in the list and click corresponding command in the context menu. In the confirmation dialog box, click **Yes**. This function is also available during profile editing or creating in the **Endpoint agent settings profile** window. Clear the **Settings profile enabled** check box if you do not want to use an appropriate profile at present, but you are going to use it further.

The disabled profile will appears in the list dimmed and becomes invisible for agents. To discard the action right-click a profile in the list, and then click **Enable profile** in the context menu.

3. To make a copy of a profile, right-click the necessary profile, and then click the corresponding command in the context menu or click **Copy profile**. In the confirmation window click **Yes**. The copy of the selected profile will be displayed in the list with mark (*copy*). Copying can be useful for a new profile creation with settings of existed profile as a basis.

11.4.3 Priority of agent profile

SecureTower system applies existing profiles of settings according to item position in the list of profiles in the **Agent settings manager** window.

Thus, the lower profile line position in the list, the higher priority of its application. For example, if the same object is defined in the field **Applied to**: for two different profiles, system will apply to this object the settings of profile with lower position: *for data interception of the Administrator user account, the settings specified in the Profile2, instead of Profile1, will be applied.*

However if the user account is attached to the computer with higher priority profile, the profile of the computer will have a senior level of priority and for data interception of the attached user the computer profile will be applied: *if Administrator is attached to FG-LAPTOP computer, Profile3 settings will be applied to user Administrator.*

Profile description	Applied to
<input type="checkbox"/> Default profile	By default to all computers and users
<input type="checkbox"/> Profile1	PG-DB,Administrator,FG-LAPTOP
<input type="checkbox"/> Profile2	Administrator,FG-LAPTOP
<input type="checkbox"/> Profile3	FG-LAPTOP

To change profile position in the list, click **Move up** or **Move down** on the toolbar.

Note: The **Move up/Move down** commands are not available for Default profile. This profile always has lower priority.

11.5 Automatic assignment of contact information

Endpoint control agents support automatic linking of user contact information (Skype accounts, ICQ numbers, e-mails, IP-addresses) to user cards. This function facilitates user identification in the network. To activate this function, click the **Endpoint agents options** tab of the **Endpoint agent control center** window and select the corresponding option in the relevant section.

Auto assign contact information to users



Use this option to allow SecureTower automatically link contact information intercepted by endpoint agents such as messenger UINs, e-mail addresses, IP addresses and etc to the user cards. Contact linking will allow to correctly identificate users that sent information across the network.

Auto assign contact information to users

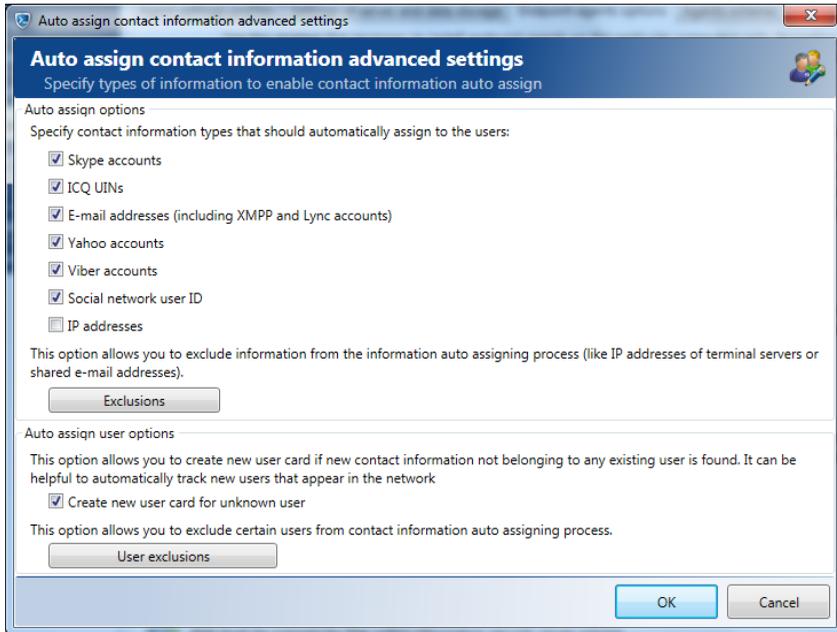
Users server connection parameters:

Server address:

Note: In order the system could perform automatic assignment of contact information, a Windows Active Directory account must be linked to every user having an agent installed on his computer (refer to section [User Network identification](#)). Contact information will not be automatically linked to user cards with no information about a corresponding Active Directory account.

⚠ Attention: Upon automatic linking of user contact information the data from the cache of Active Directory are considered only. If any changes within Active Directory structure were made in the period between cache updating and such operation, the operation will be performed without taking this changes into account. To take the non-fixed in cache changes of AD structure into account urgently, [update Active Directory structure manually](#).

1. Enter the address of the user server into the **Server address** text field.
2. To configure automatic assignment parameters, click **Auto assign advanced settings**.

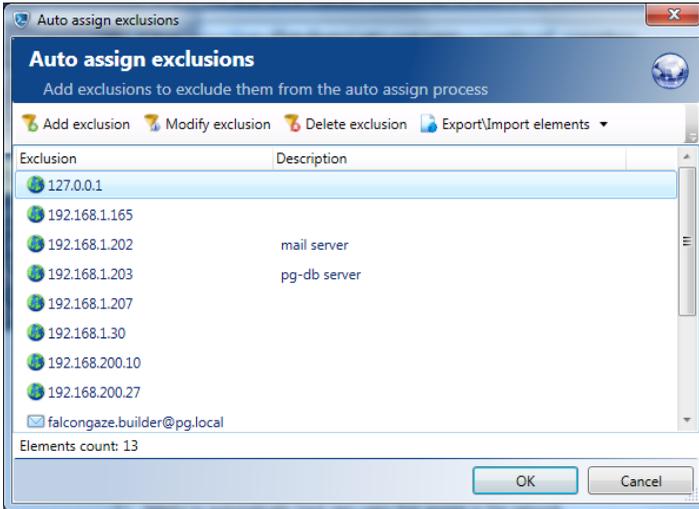


3. In the advanced settings window select the types of information that will be automatically assigned to users by selecting/clearing the corresponding check box.
4. In some cases it is necessary to forbid linking of a certain identification information to user profiles. For example, it is important to exclude IP addresses of terminal servers from this process. This will help to avoid errors caused by linking the same IP to several users working on such servers. Besides, the IP addresses of mail servers should also be excluded from automatic assignment. To set up exclusions, click **Exclusions** and follow the guideline from [Exclusions](#) section of this chapter.
5. The option of user card creation for unknown contacts serves to auto create a user card when a new contact data is detected and it does not belong to any of the existing users. This function can be used to automatically track new users appearing in the network. To activate this option, click **Create new user card for unknown user**.
6. Certain users can be excluded from automatic assignment of contact information. In this case no information will be added to the specified users cards automatically. To enable user exclusion, click **User exclusions** and follow the guideline from [User exclusions](#) section of this chapter.
7. After you have configured all the advanced settings of the automatic assignment feature, click **OK** to save the changes.

Exclusions

1. In the exclusion window click **Add exclusion**.

2. In the **Exclusion type** menu, select a type of identification information you wish to exclude from automatic assignment.
3. Enter the corresponding data into the **Exclusions** text field.
4. Click **Add**.



5. Once all the necessary exclusion have been added to the exclusion list, click **OK**.

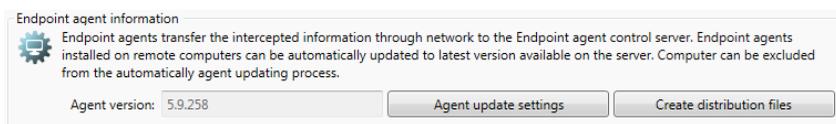
User exclusions

1. In the User exclusions manager window, click **Add exclusion**.
2. A window will open in which you are to select users you wish to exclude from automatic assignment of contact information.
3. Select a user in the list of all Active Directory accounts. To select multiple fields hold down Ctrl on your keyboard and click on the fields' titles. Use the search field above the user list to facilitate search through a long list. Enter letters into the field and the system will display only those users that have the specified letters in their account name or e-mail address.
4. After you have highlighted all the necessary users, click **Select** to add them to the exclusion list.
5. Once all the necessary users have been added to the exclusion list, click **OK**.

11.6 Updating endpoint agents version

Endpoint agents installed on computers of your network with Endpoint agent control center are updated automatically. To view the information about the current version of agents, click the **Endpoint agents options** tab of the **Endpoint agent control center** window, and then go to the **Endpoint agent information** section. The version is displayed in the **Agent version** box.

Note: Agents, that were installed manually or by Group Policy and still are not under server's control, must be updated manually by administrator. To update the agents manually, start the Installation Wizard (for more information, see [Manual agent installation](#)) or use Group Policy (for more information, see [Remote agent installation by Group Policy](#)). To familiarize with version of uncontrolled agents click the Agents schema tab (for more information, see [Monitoring endpoint agents status](#)).



To set an update mode for the particular agent (on the particular computers):

1. Click **Agent update settings**.
2. In the newly opened window click the radio button related to the necessary update mode:
 - To update only the agents, that is specified in the list, select **Update only the agents on computers listed above**.
 - To update the agents on all computers except the specified in the list, select **Update the agents on all computers except listed above**.
3. Click **Add object** on the window toolbar and specify the computers as described in [The list of excluded computers](#).

Creating a distribution file

To create distribution files to install agent with all current settings, click **Create distribution files** and enter the name and the save path in the corresponding window. The distribution files will be compressed into ZIP archive and saved on the disc.

11.7 Setting up computers indexing

Indexing of workstation is a part of file system control and enables search of the sensitive files within computer file system. The set of sensitive files is stored in the [system data banks](#) of file hashes. The mode of data banks applying is determined upon [file system control](#) configuring.

Indexing is based on the list of controlled computers and indexing rules. Indexing statistics for each computer is provided in the corresponding tab of agents schema (for more information, see [Monitoring endpoint agents status](#)).

To enable and configure computer indexing, click the **Endpoint agents options** tab of the **Endpoint agent control center** window, and then select the check box of relative option in the **Computer for indexing** section.



To set the list of computers for indexing and hash calculating (a particular computer or group):

Note 1: *Indexing of all controlled computers is executed by preset rules.*

1. Click **Computers for indexing**.
2. In the newly opened window click the radio button corresponded to the necessary mode of the list processing:
 - To index only the workstations, that names are included to the list, select **Index only objects listed above**. In this case the file systems of other network computers will not be indexed and checked upon search of sensitive files.
 - To index all workstations of the network, except listed, select **Index all computers except listed above**. In this case file systems of all computers in the network will be indexed and taken into account upon search of sensitive files.
3. Click **Add object** on the window toolbar and specify the computers as described in [The list of excluded computers](#).
4. Configure indexing rules:
 - To configure and apply the personal settings to selected object, click the object line in the list, then click **Configure personal indexing settings** on the toolbar. Then follow the recommendation of [Configuring indexing filters](#) and [Configuring schedule](#) sections of this chapter. The object with personal indexing settings will be marked with icon of custom settings .

Domain	Object
pg.local	 Computers
	 FG-SRV.pg.local
	 PG-AC.pg.local
	 PG-PDC.pg.local

- To apply common settings to object or group with personal ones, click the necessary entries in the list, and then click **Indexing settings** on the footer bar. Then click **Apply default settings**.
5. To change configuration of common settings, click **Indexing settings** on the footer bar and then click **Configure default settings**. Then follow the recommendation of

[Configuring indexing filters](#) and [Configuring schedule](#) sections of this chapter.

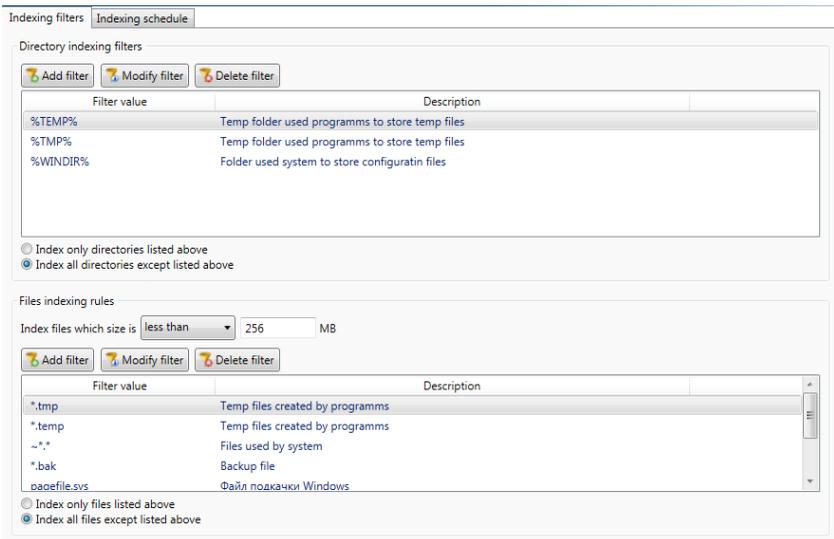
Note: By default the common preset settings are applying to all indexing objects. Herewith, the temporary and other system files and directories are excluded from indexing. One can modify the presets for all objects simultaneously, except objects with personal settings.

6. To perform other operations with list of computers follow the recommendations given in [Exclusions from interceptions](#).
7. Click **OK** when finish configuring.

Configuring indexing filters

The filters of directories and files are available for configuring in the **Indexing filters configuring** window. Set the filters as described further, and then configure hash calculating schedules.

To reset personal settings to default, click **Apply default settings** on the footer bar.



Indexing filters | Indexing schedule

Directory indexing filters

Filter value	Description
%TEMP%	Temp folder used programm to store temp files
%TMP%	Temp folder used programm to store temp files
%WINDIR%	Folder used system to store configuratin files

Index only directories listed above
 Index all directories except listed above

Files indexing rules

Index files which size is MB

Filter value	Description
*.tmp	Temp files created by programm
*.temp	Temp files created by programm
-*.*	Files used by system
*.bak	Backup file
pagefile.sys	Файл подкачки Windows

Index only files listed above
 Index all files except listed above

To customise indexing rule for directories, in the **Directory indexing filters** section:

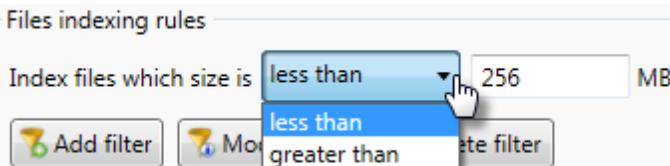
1. Select the one from the filtering modes:
 - To index only files from directories that satisfy the filters, select the **Index only directories listed above** mode. All other directories will not be indexed.
 - To index all directories of the file system of workstation, except the directories satisfied the filters, select the **Index all directories except listed above** mode. Directories that satisfy the filters listed in the list will not be indexed.
2. Click **Add filter**.
3. Type the necessary environment variable in the **Filter value** text field and description in

the related text field if necessary. Click **OK**.

4. To modify or remove a filter from the list, click the necessary one in the list, and then click the button related to the action on the section toolbar.

To customise indexing rule for files that should be indexed, in the **Files indexing rules** section: :

1. Specify file size restrictions for indexing. To do this click the drop-down button with preset value (**less than**). Click the necessary value of condition and type the limit of file size. The files, which size is not meet the limit will not be indexed.



2. Select the one from the filtering modes:

- To index only files that satisfy the filters, select the **Index only files listed above** mode. All other files will not be indexed.
- To index all directories of the file system of workstation, except the directories satisfied the filters, select the **Index all files except listed above** mode. Files that satisfy the filters listed in the list will not be indexed.

3. Click **Add filter**.

4. Type the necessary value in the **Filter value** text field and description in the related text field if necessary. Click **OK**.

5. To modify or remove a filter from the list, click the necessary one in the list, and then click the button related to the action on the section toolbar.

Configuring schedule

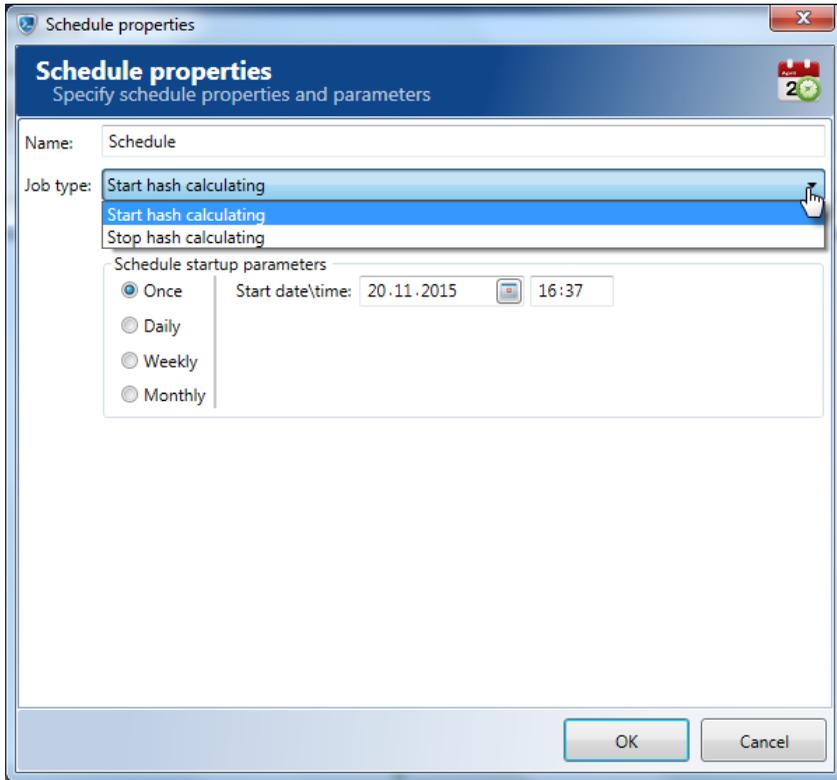
Indexing task is executed in the continuous mode and doesn't need to be configured manually. By default hash calculating is also executed in the same way, but user can configure the task schedule manually.

To configure schedules of the hash calculating tasks, click the **Indexing schedule** tab in the rule configuring window:

1. Click **Add schedule**.

2. In the **Schedule properties** window type the schedule name in the related text field.

3. Click the drop-down arrow next to the **Job type** field, and then click the necessary type task type:



- **Start hash calculating.** This task provides control of changes in file systems. It is recommended to start this task during night time. At least one start task must be configured.
 - **Stop hash calculating.** If the huge amount of data is to be indexed, the hash calculating processes can be very time and resource-consuming. Therefore it is recommended to set a task not only for the start but for the stop of the calculating procedure.
4. Follow the steps from [Creating a schedule](#) to set a startup parameters of the task execution. Click **OK** when finish. To modify or remove a schedule from the list, click the necessary one in the list, and then click the button related to the action on the window toolbar.
 5. Click **Save** when finish rule and schedule configuring.

Resetting default settings to presets

It's possible to reset default settings to presets if default settings has been changed by user. To reset settings:

1. Click **Indexing settings** on the footer bar.
2. Then click **Configure default settings**.
3. Click **Apply presets** on the footer bar of the default settings window.

11.8 License server information

In the **license server information** section on the **Settings of server and data storage** tab of the **Endpoint agent control center** window you are to specify the parameters of access to **SecureTower** license server.

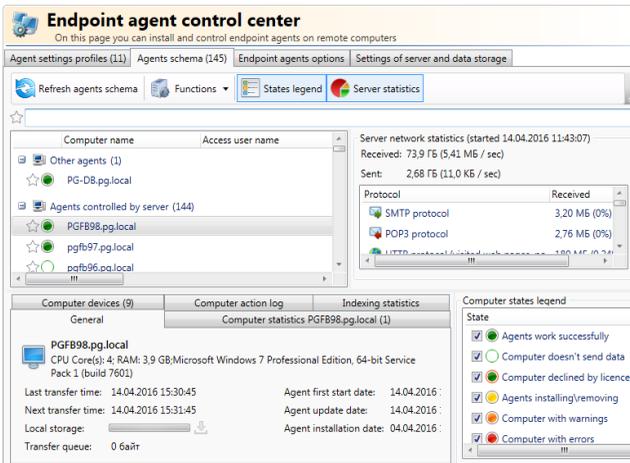
Specify the server address and port used to connect to it in the corresponding fields. Follow recommendations from [Setting up connection to the license server](#).

11.9 Monitoring endpoint agents status

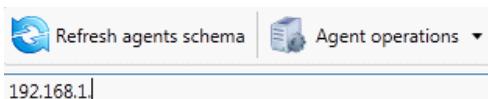
In the **Agents schema** window, you can monitor not only the agents' installation progress, but the status of the agents (for example, a message that some agent was disabled or that some agents need to be updated, etc.) too.

To view the status of the agents installed or being installed, select the **Agents schema** tab in the **Endpoint agent control center** window.

- In the opened window you will see the list of workstations with their IP addresses, information on the version of agents installed, date and time of their last activity current status, current scheduled agent tasks and access user name.



- The agents' status window is automatically refreshed every 30 seconds. To immediately receive updated information about agents status, click **Refresh agents schema** on the command bar.
- To find a particular computer in the list, enter the name or IP address of the computer you are searching for or user account name in the text field on the filter bar. As you type, the list will display only the computers that have the entered symbols in their name/IP address.



- To mark the agent as favorite, click the **Favorites** button ☆ next to the computer name. To filter the list by favorites, click the **Favorites** button on the filter bar.
- To mark in color the agents entries on the scheme in accordance with their last activity time, right-click the corresponding header of the scheme, and then click **Enable advanced time mode**. The following color are reserved for last activity status:

- [0;5 min] - regular color;

- (5;30 min] - orange;

- (30 min; +inf) - red;

- computer is not connected or can't be pinged - серый.

All agents are grouped by types – controlled by server and other.

	Computer name	Access user name	IP Address
+	Agents controlled by server (47)		
+	Other agents (1)		

The agents controlled by Server are in the first group. By default, the agents installed with Administrator Console get to this group.

The agents not controlled by Server with installation independent settings are in the second group. By default the agents installed through group policies or manually get to this group.

The main distinction is that agents of the first group may be launched (if they were stopped) or reinstalled (if they were damaged) directly by Endpoint agent control server of **SecureTower**.

Agents of the second group work independently. Server receives from them information, but doesn't supervise their installation, updating and restoration.

Agents from the second group are working in independent mode. Server receives information from them, but doesn't control their installation, updating and restoration.

Note: *In case of Endpoint agent control server address change, for communication restoration via new port and receiving up-to-date information from agents of the second group, updating of these agents should be carrying out manually.*

For optimization of interaction process with agents it is recommended to move agents of the second group to the list controlled by server. For relocation of agents from one group to another use corresponding options of the context menu called by right-clicking on a computer in the list (see below).

Context menu

- **Relocation of agents**

To add the computer to the controlled by server list (the option is available only for agents from **Other agents** group) click on corresponding options in context menu. In case of this and followed clicking on the **Apply Changes** button in the lower right corner of **Agents schema** window the agent will be moved to the controlled by server list. Other shortcut options will be available in the **Functions menu**.

- **Remove agent and exclude computer from schema**

If you select this option, the system will try to connect to this computer and remove the agent from it. In case the computer name was entered incorrectly or the computer cannot be accessed for any other reason, the system will keep trying to connect to this computer until it succeeds and uninstalls the agent. To simply remove the computer from the list (without trying to uninstall the agent), use the next option.

- **Exclude computer from schema without any additional actions**

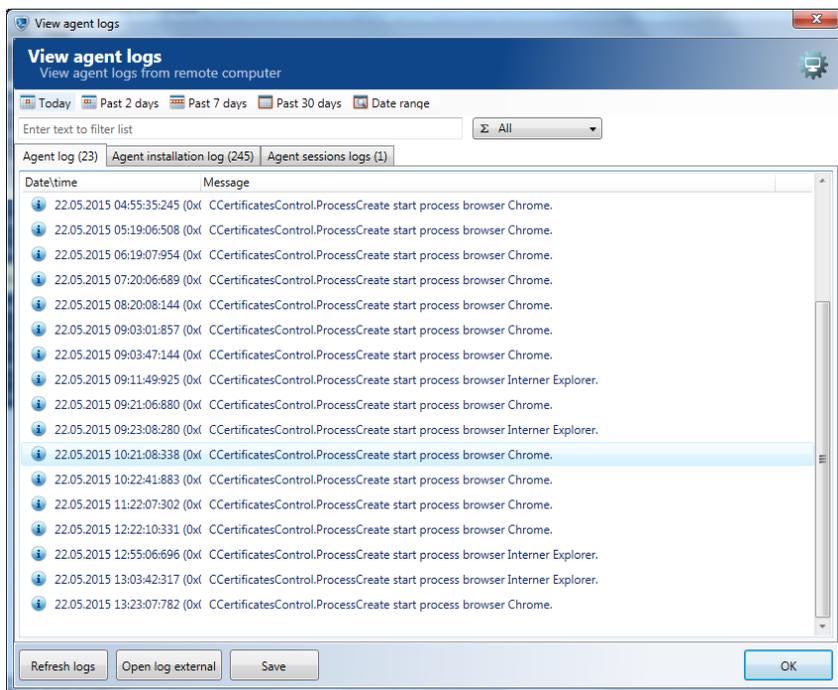
If you select this option, the system will not try to connect to the specified computer, and will simply remove it from the list.

- **Clear Endpoint Agent statistics**

If you select this option, the system will delete all statistics about intercepted data from this computer.

- **View agent logs**

This option is used to access a full agent log on a specified computer. When you select this option, all technical information about the agent on the selected computer, including records of agent events and statuses, installation and sessions will be provided in the new window. Select the corresponding log type tab to investigate agent logs.



One can use the following features during logs viewing: To select the date range you need to be represented in the displayed log, use the corresponding button on the window toolbar.

- To display the log records corresponded to particular event type, click the **All** button and click the necessary one.
- To display records that contain the particular word or phrase in its message text, type the words you are searching for in the text field. As you type, the list will display only the records with the messages which have the entered symbols in their text.
- To update logs to the up to date condition while viewing click **Refresh logs**.
- To open log in the external application click the Open log external button. Log will be opened in the associated text editor (for example, Notepad).
- To save logs (for example, to send to **Falcongaze** Technical Support Service), click **Save**.
 - **Restart agent**
 - **Enable extended log mode**

Please note that extended logging significantly increases the size of system logs, therefore it is not recommended to use this option on a regular basis – enable it temporarily as needed

- **Force agent to upload data to server**
- **Set computer access credentials**

Access credentials can be set for the particular computer with SecureTower agent. User account under which EndPoint agent server is started has full access to the all computers with SecureTower agent by default, if other condition isn't specified. To set a computer access credentials, select the corresponding option from the computer context menu and follow recommendations from the [Assigning access credentials](#) chapter.

Attention: *A user account under which Endpoint agent control server works should have permissions to access the resources of the computer on which this agent is set. If this account has no sufficient rights or if the server can't get access to the remote computer for other reason (f. e., the computer is switched off), the agent will not be controlled by the server and the user will see the corresponding warning message.*

Functions menu

When you select a computer in the list, the following commands will be available on the **Functions** menu:

- **Clear Endpoint Agent server statistics.** One can use this command to clear the section with statistics of data, accepted by server and delete corresponding information from the system.
- **Remove agent and exclude computer from schema.** Use this command to delete the agent module from specified user workstation and exclude the one from schema.
- **Exclude computer from schema without any additional actions.** Use this command to exclude computer with the agent module from the list of agents which are under server control but without agent removing action.
- **View agent logs.** One can use this command to inspect all technical information about selected computer, including records of agent event and statuses, installation and sessions.

The commands above are available on the [context menu](#) (for detailed information see recommendations given for the [context menu](#) options). One more command is accessible from the functions menu only:

- **Export agents list.** Use this command to export the list of displayed agents to Excel, TXT or CSV file according to selection. Hereby the agents data and status information will be exported too.

States legend menu

Click **States legend** to display/hide the agent status legend in the right lower part of the window.

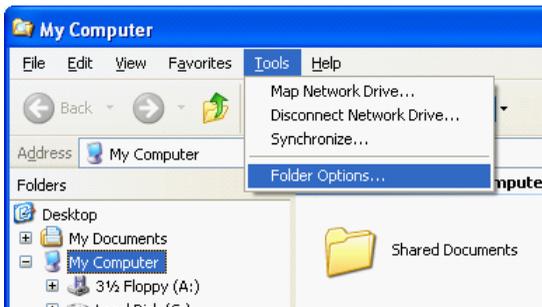
Computer states legend

State	Quantity
<input checked="" type="checkbox"/>  Agents work successfully	0
<input checked="" type="checkbox"/>  Computer doesn't send data	0
<input checked="" type="checkbox"/>  Computer declined by licence	0
<input checked="" type="checkbox"/>  Agents installing/removing	0
<input checked="" type="checkbox"/>  Computer with warnings	0
<input checked="" type="checkbox"/>  Computer with errors	0
<input checked="" type="checkbox"/>  Computer unavailable	0

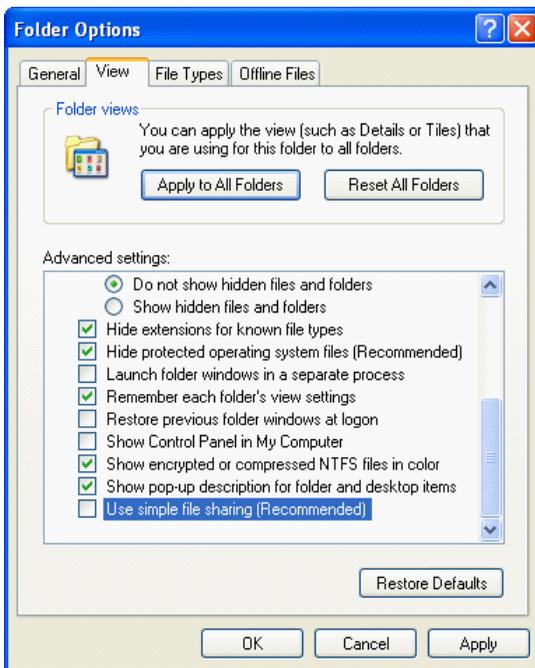
State	<i>Types of agent status messages:</i>
 Agents work successfully	Agent service installed
	Agent service started
	Agent service running successfully
<input checked="" type="checkbox"/>  Computer doesn't send data	No data to send
	Workstation is switched off
	Workstation is switched on, but a user has logged out or finished his session by another way
 Agents installing\removing	Agent service not installed
	Installing agent in progress
	Removing agent in progress
 Computer with warnings	Agent service stopped
	Workstation not found (could be turned off)
 Computer with errors	Workstation SCM (=Service Control Management) could not be accessed (<i>see Note below</i>)
	Workstation hard disks could not be accessed
	Workstation registry could not be accessed
	Agent installer service could not be installed or started
 Computer unavailable	Workstation could not be found (name could be incorrect)
	Unknown

Note: One of the reasons for this type of error on Windows XP machines may be the Simple File Sharing option. To eliminate this error, disable this option:

- double-click My computer icon on the remote machine
- select Tools – Folder options... in the main menu

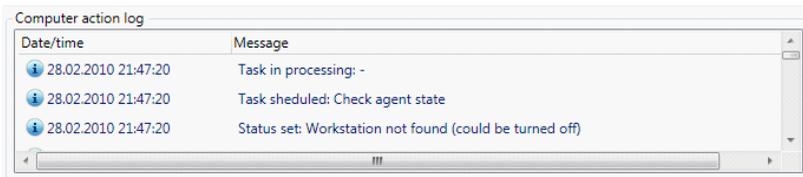


- in the new window click the **View** tab
- clear the **Use simple file sharing** check box in the **Advanced settings** list



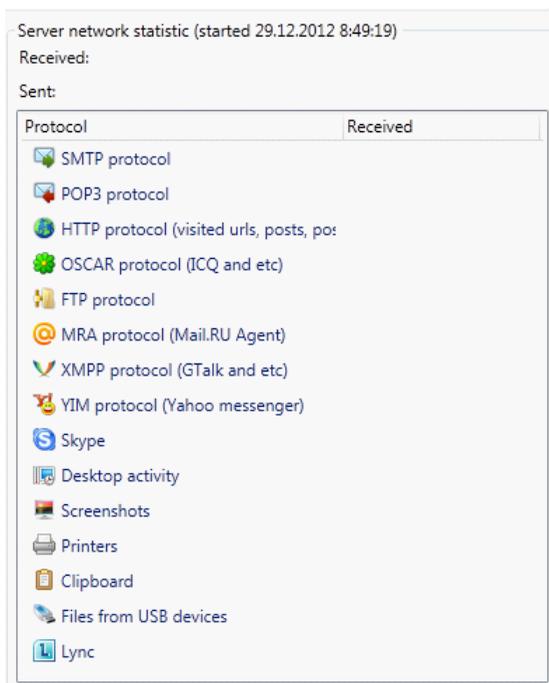
- click **Apply**
- close all settings windows by clicking **OK** in each of them

To view the status messages log for the agent installed on some workstation, click the line with the necessary workstation in the agents' status window, and you will see 100 latest messages on the selected agent's status in the **Agent status log** section located under the list of agents.



Server statistics

Upon clicking **Server statistics** in toolbar section of the **Agents schema** window, the section with statistics of data accepted by server is displayed/disappeared in the right area of the window.

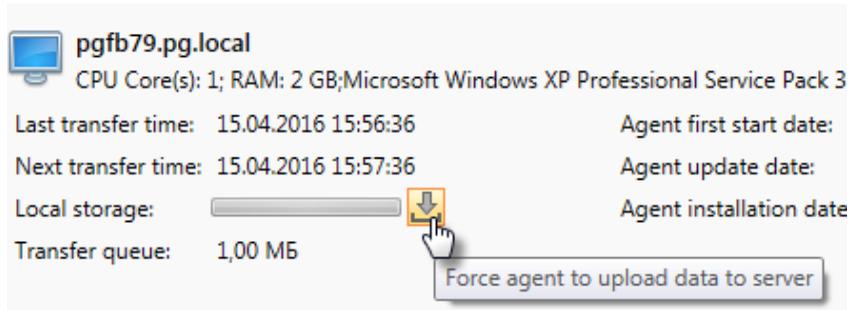


Statistics

To view interception statistics of the specified agent, log of status messages of the agent

and the parameters of the devices connected to the computer on which the agent is set, click a line of the required workstation, and the relevant information will be displayed in the lower part of a window under the list of agents.

The **General** tab provides console user with general information about computer parameters, transfer status, agent operation. Also the force upload button is accessible to force agent to upload data to server despite a scheduler.

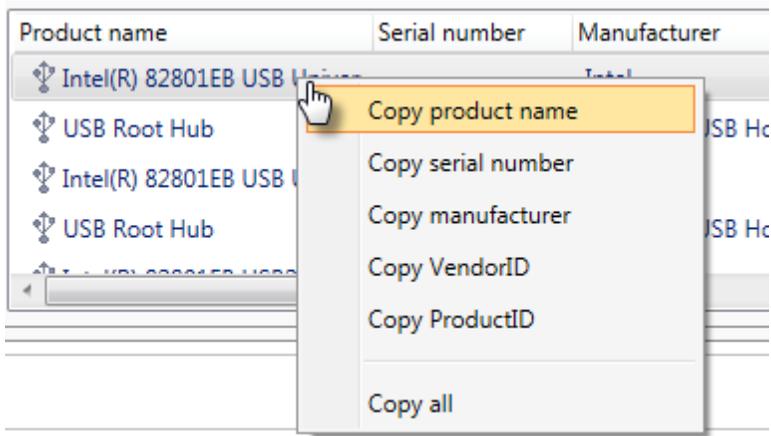


In the **Computer statistics** tab statistics of the traffic intercepted from this computer and traffic of the particular user working at this computer is displayed. Also for each user of the selected computer the applied profile name is specified. To copy user SID, right-click the user's name and click the relevant command in the pop-up menu. To display a profile application time and general information hover over the user's line - the hint will appear. To inspect the profile parameters hover over the profile name and click it. Names of the users attached to this computer, but inactive at present (for example, quitted the system) are dimmed. Interception statistics (per protocol) is displayed in accordance with selected user.

The **Computer action log** tab is used to find a full agent log on a specific computer. Click this tab and inspect all technical information about selected computer, including records of agent event and statuses, installation and sessions. To copy the necessary entry to clipboard right-click it and then click **Copy row** in the context menu or select the row and press Ctrl+C. To copy log click **Copy all** in the context menu.

The **Computer devices** tab is used to find a full information about devices connected to computer. Click this tab and inspect devices parameters. This data may be copied to clipboard and used for devices interception configuring (see [Devices control](#) for details). To copy the necessary parameter value to clipboard right-click it and then click the necessary command in the context menu. To copy all devices list together with parameters click **Copy all** in the context menu or press Ctrl+C.

Product name	Serial number	Manufacturer
Intel(R) 82801EB USB		
USB Root Hub		
Intel(R) 82801EB USB		
USB Root Hub		
Intel(R) 82801EB USB		



The **Indexing statistics** tab presents results of the computer file system indexing.

12 Setting up mail processing

SecureTower Mail Processing Server initially intercepts e-mails sent via third-party mail servers. The system can integrate with mail servers based on MS Exchange and other software using POP3 and SMTP protocols (Lotus Domino, Postfix, Sendmail, etc.).

12.1 Setting up mail interception

To configure connections to mail servers and modify existed ones go to the **Mail server connections** section and follow the guidelines given in corresponding chapter: [MS Exchange connection](#), [Connecting to mail server over POP3 protocol](#), [Receiving mail from server over SMTP protocol](#).

When the connections is configured, them (active and inactive) will be added to the mail servers connections list. The inactive ones will be dimmed in the list.

Connection name	Mail server address	Last update date	Recent: received/skipped/error	Total: received/skipped/error
pg-m (non3)	PG-M		0/0/0	0/0/0
pg-m (Exchange)	pg-m	05.05.2015 15:46:03	1/0/0	301/2/1
SMTP подключение1	PG-DB:25		0/0/0	0/0/0

Entry of each connection contains the following data:

Mail server address - the connected server name;

Last update date - date and time of the last operation of mail receiving from the server.

Recent: received/... - statistic of mail processing since the last session of mail receiving have been started. "Received" - the number of intercepted emails which were saved to the database. "Skipped" - the number of the emails that was ignored upon interception due to different reason: the email is in the list of exclusions; excess of the mail licence limit; the SecureTower Security Center email; internal MS Exchange system mail; the mail with the size more than 100 MB (by default). "Error" - the number of errors that occurred upon receiving or saving processes .

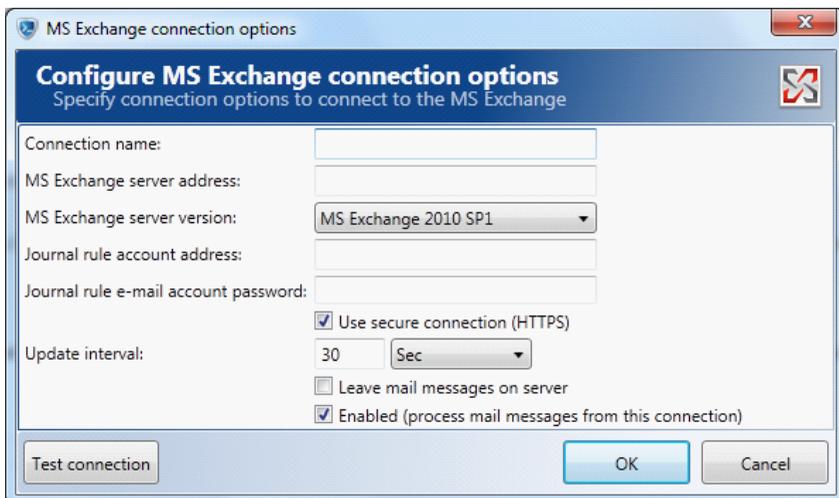
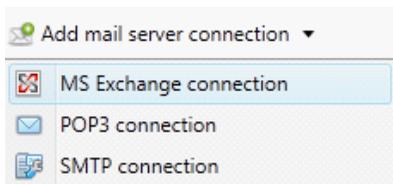
Total: received/... - statistic of mail processed since MPS service start-up.

12.1.1 MS Exchange connection

Note: Before you proceed with configuring MS Exchange e-mail interception in **SecureTower**, you need to set up mail journalling mechanism on your mail server. All mail transmitted through the server will be simultaneously copied to a special mailbox which will be controlled by **SecureTower** Mail Processing Server. See instructions for setting up mail journalling in paragraph [Configuring a mail journalling mechanism](#)

Open **SecureTower** Administrator Console – **Mail Processing** tab, and follow the instructions below.

Select **MS Exchange connection** in the **Add mail server** connection drop-down menu.



In the new window you need to specify the following settings:

Connection name (any name for the convenience of identification);

MS Exchange server address (the name of your physical server where MS Exchange Server is installed);

MS Exchange version (version of the software installed on your server). Supported versions include MS Exchange 2007, 2010, 2013 (including 2010 and 2013 with Service Pack 1);

Journal rule account address (the name of an account to which all mail will be copied according to the journalling rule created in paragraph [MS Exchange](#));

Journal rule account password (password for the journalling account)

In case you need to use secure connection to your mail server, check the corresponding box.

Update interval (SecureTower will establish a connection to the mail server and extract new messages with the specified interval. Enter a value in the text field and select a unit – seconds, minutes or hours);

If you wish that all mail remains on the mail server after SecureTower extracts it, check the corresponding box. Otherwise all mail will be deleted from the server after extraction.

To enable/disable the connection select/clear the **Enabled** check box.

Click **Test connection** to make sure all specified parameters are correct. If the test completes successfully, the system will display a corresponding message. Otherwise

check your settings again. To save settings, click **OK**, then click **Apply changes** in the lower right corner of Administrator Console main window.

12.1.2 Connecting to mail server over POP3 protocol

SecureTower system can control mail transferred via mail servers based on various software (like Lotus Domino, etc.) by connecting to such servers and extracting mail over POP3 protocol (including SSL-encrypted). To use this function you need first to set up mail journaling on your server (similar to journaling in MS Exchange – see [Configuring a mail journaling mechanism](#)) or some other mechanism which will enable **SecureTower** to extract the copies of all e-mails from a single account.

To set up a connection to a mail server over POP3, select **POP3 connection** in the **Add mail server connection** drop-down menu.



In the new window you need to specify the following settings:

Connection name (any name for the convenience of identification);

Mail server address (the name of your physical server where Lotus Domino, etc. is installed);

Account name (the name of an account to which all mail will be copied, i.e. the mail journaling account);

Account password (password for the journaling account)

In case you need to use secure connection to your mail server, check the corresponding box.

Update interval (**SecureTower** will establish a connection to the mail server and extract new messages with the specified interval. Enter a value in the text field and select a unit – seconds, minutes or hours);

If you wish that all mail remains on the mail server after **SecureTower** extracts it, check

the corresponding box. Otherwise all mail will be deleted from the server after extraction.

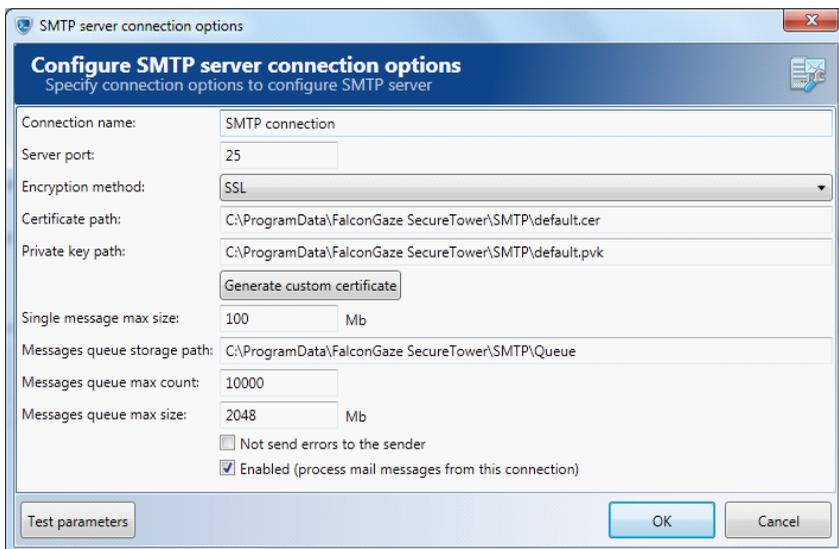
To enable/disable the connection select or clear the **Enabled** check box.

Click **Test connection** to make sure all specified parameters are correct. If the test completes successfully, the system will display a corresponding message. Otherwise check your settings again. To save settings, click **OK**, then **Apply changes** in the lower right corner of Administrator Console main window.

12.1.3 Receiving mail from server over SMTP protocol

SecureTower system may be configured to receive e-mail flows from any mail servers via SMTP protocol (including SSL/STARTTLS-encrypted), i.e. act as a server. To use this function you first need to set up your mail server to send copies of all e-mails to **SecureTower** server.

To set up **SecureTower** SMTP server select **SMTP connection** in the **Add mail server connection** drop-down menu.



In the new window you need to specify the following settings:

- **Connection name** (any name for the convenience of identification);
- **Server port** (the number of TCP/IP port that will be scanned by **SecureTower** server. This should be the port where the e-mail flow is directed to. As a rule, port 25 is used for non-encrypted SMTP, and port 465 – for encrypted SMTP traffic.)
- **Encryption method** (if necessary, select one of the two available encryption methods – SSL or STARTTLS. Encryption makes the connection more secure, but creates additional load on the sending (i.e. corporate e-mail server) and receiving (i.e. **SecureTower** SMTP server) parties).
- **Certificate path** (this parameter is only shown when an encryption method – SSL or

STARTTLS—is selected. In this field you need to enter the full path to the encryption certificate file. If the file does not exist, the certificate will be generated automatically).

- **Private key path** (this parameter is used in the same manner as the previous one).
- **Custom certificate** (the **Generate custom certificate** button generates a certificate and a private key after the user specifies the necessary parameters: domain name and duration. You might need to use this button if the mail server software which sends out the e-mail flow cannot connect to a server having a domain name which does not match the one it expects).
- **Single message max size** (the maximum size of an e-mail to be processed by **SecureTower** server. All larger e-mails will be ignored).
- **Message queue storage path** (the full path to a directory which will be used for temporary storage of all e-mails before they are processed by **SecureTower** and transferred to its database. In case the message flow is too intense, it is recommended to use a RAID array for better performance).
- **Message queue max count** (the maximum length of the e-mail messages queue. When this limit is reached, **SecureTower** SMTP server will temporarily reject new messages until there are empty slots in the queue).
- **Message queue max size** (size limit (in MB) for the e-mail message queue. When this limit is reached, **SecureTower** SMTP server will temporarily reject new messages until there is empty space for the queue).
- **Errors messages** - the check box allows user to disable sending error messages to the sender. In some cases, when **SecureTower** cannot process an e-mail coming from the mail server, an error message may be sent. If you wish to disable sending such messages to your corporate mail server and further – to the e-mail sender – check this box).
- **“Enabled”** (select this check box to enable/disable the SMTP connection).

Click **Test connection** to make sure all specified parameters are correct. If the test completes successfully, the system will display a corresponding message. Otherwise check your settings again. To save settings, click **OK**, then **Apply changes** in the lower right corner of Administrator Console main window.

12.2 Miscellaneous mail processing settings

In the upper part of the Mail processing tab you will be able to see a list of all mail server connections you have created. To delete a connection highlight it in the list and click **Delete mail server connection**. To modify a connection settings, click **Modify mail server connection**.

After you have specified connection parameters, follow instructions below to configure other essential settings.

Select one of the two **Mail processing strategies**:

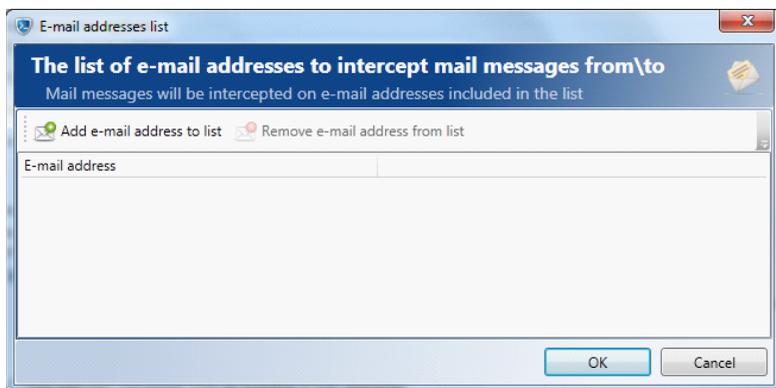
Mail processing strategy

 SecureTower provides mail processing based on the selected processing strategy. To start mail processing, please select the processing strategy below:

- Process mail messages only from specified e-mail addresses
Use this strategy if you need to process only some e-mail addresses. Based on this strategy, SecureTower will process only e-mail addresses that you specified. Any other available e-mails received from configured mail server connections will be ignored.
- Process mail messages from all available e-mail addresses
Use this strategy if you need to process mail messages from all e-mail addresses. Based on this strategy, SecureTower will process all messages received from configured mail server connections except for those sent from or to e-mail addresses on the exception list.

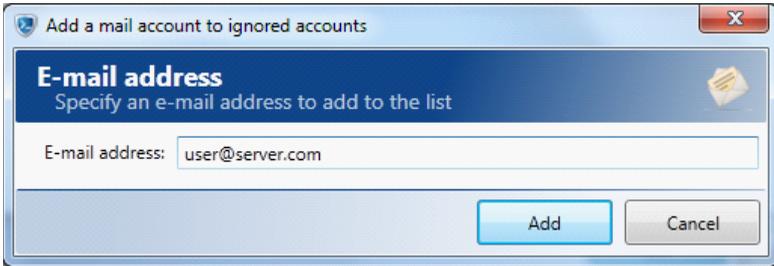
Process mail messages only from specified e-mail addresses

If you select this option you need to specify the e-mail addresses you wish to intercept traffic for. To do so, click **E-mail addresses to process mail messages**. A window will open in which you can add e-mail addresses to intercept traffic for.



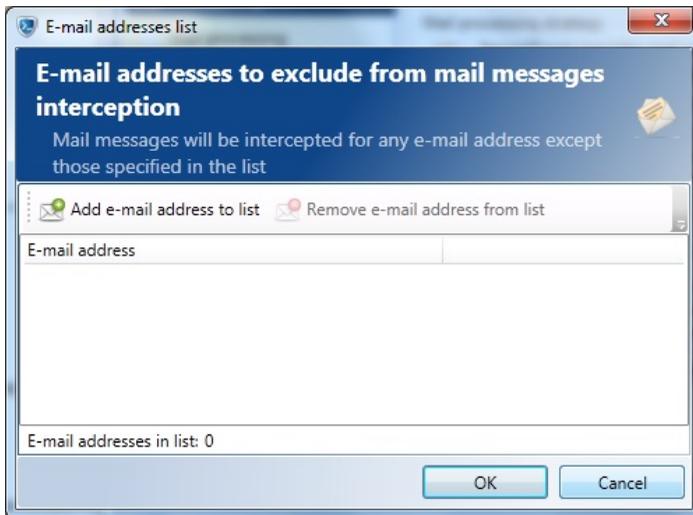
Note: The symbols "*" and "?" can be used to specify the sub-network mask.

To add addresses click **Add e-mail address to list**, type the address in the dialog box and click **Add**. To remove addresses from the list, highlight the address you wish to remove and click **Remove e-mail addresses from list**.



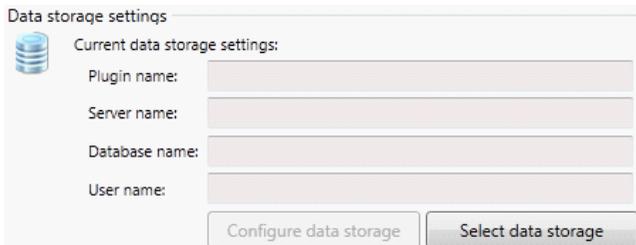
Process mail messages from all available e-mail addresses

If you select this option you may specify the e-mail addresses you wish to exclude from interception. To do so, click **E-mail addresses to exclude from mail messages processing**. Add e-mail addresses that will be excluded from interception. The procedure of adding and removing e-mail addresses is the same as above.



Configure Data storage settings

Select the database to store intercepted mail by clicking **Select data storage**. For detailed information on connection to databases refer to clauses [Selecting data storage type](#).



Data storage settings

Current data storage settings:

Plugin name:

Server name:

Database name:

User name:

Note: In case you use Windows authentication to connect to your MS SQL Server database, you need to configure the Exchange Interception Server startup parameters. To do so, select **Services** in the component selection bar in the left part of the main Administrator Console window and click **Service startup parameters** in the **Exchange Interception Server** section.



Mail processing server

This server allows monitoring third party mail servers and extracting mail messages

Status:  **Running**

In the **Service startup parameters** window select the option **Start under the specified account** option.



Service startup parameters

Configure service startup parameters to tune up the service startup process

Service startup settings

Disabled

Automatically start on system startup

Manually start by user

Service startup account settings

Start under local system account

Start under the specified account

Account name:

 Account name should be in the "DomainName\UserName" form for a domain user and in ".\UserName" form for a local user

Password:

Specify the name and password of the user having access rights for the selected database and click **OK**.

In the **License server information** section type the address of the license server and the port used to connect to it in the corresponding text fields. Follow recommendations from [Setting up connection to the license server](#).

After all parameters have been specified click **Apply changes** to save your settings.

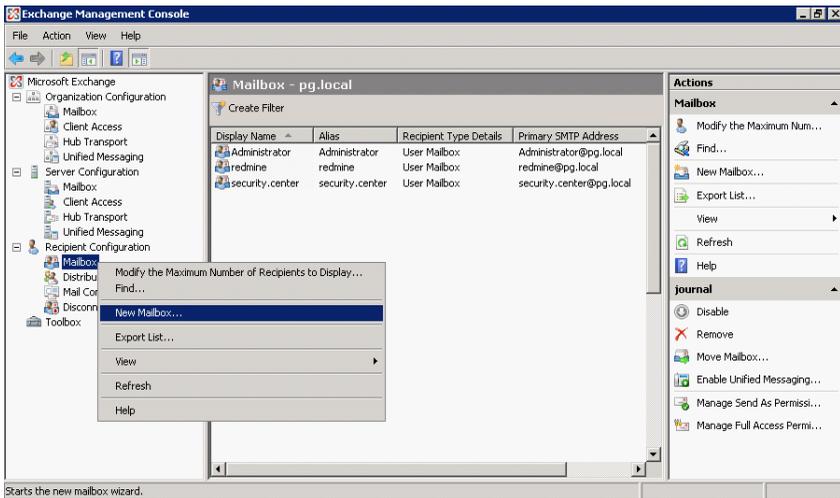
12.3 Configuring a mail journaling mechanism

A journaling mechanism in MS Exchange Server is configured with either internal or external mailbox.

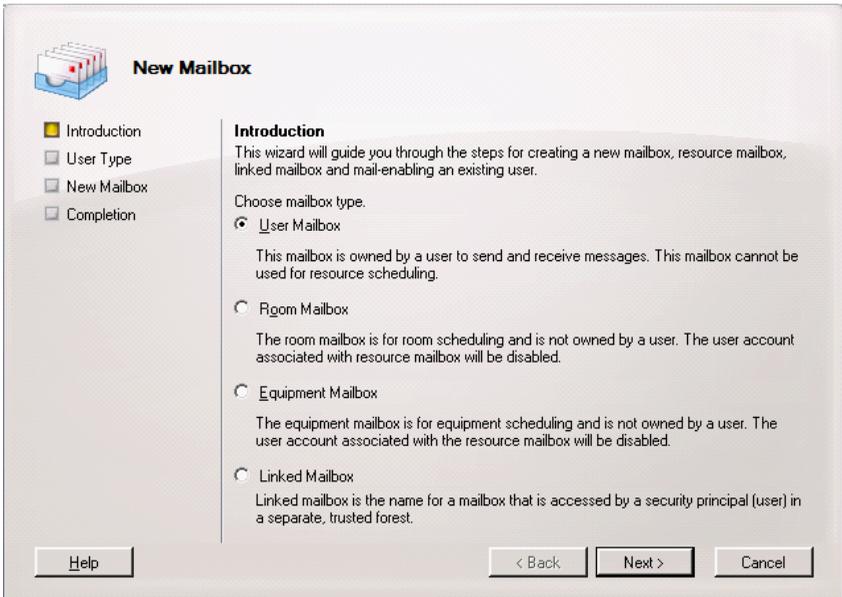
12.3.1 Journaling to internal mailbox

If you use journaling to internal MS Exchange Server mailbox, all e-mails will be copied to a special mailbox, where they will be gathered by **SecureTower** Mail Processing Server. To set up this type of journaling, follow the instructions below.

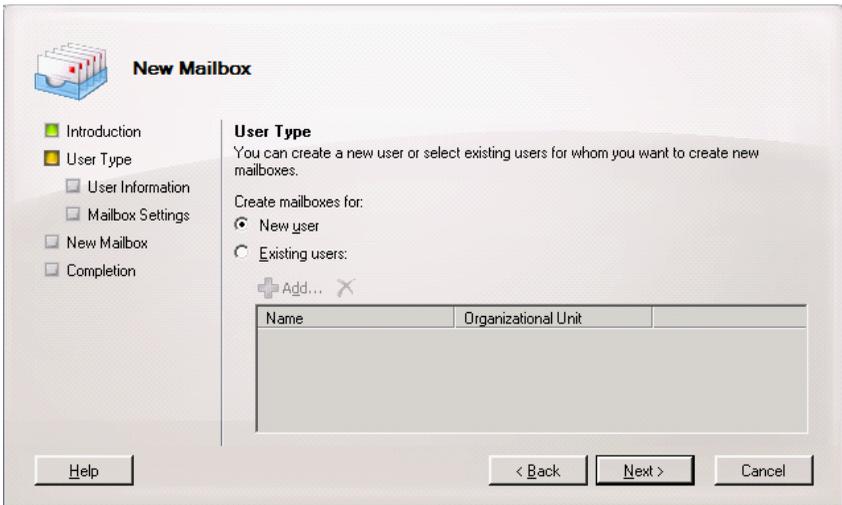
Start Exchange Management Console of your MS Exchange Server application and right-click on the **Mailbox** item under the **Recipient Configuration** option in the left part of the window. A context menu will appear in which you are to select the **New Mailbox** option.



A new mailbox configuration wizard will open where you are to the **User Mailbox** option and click **Next**.

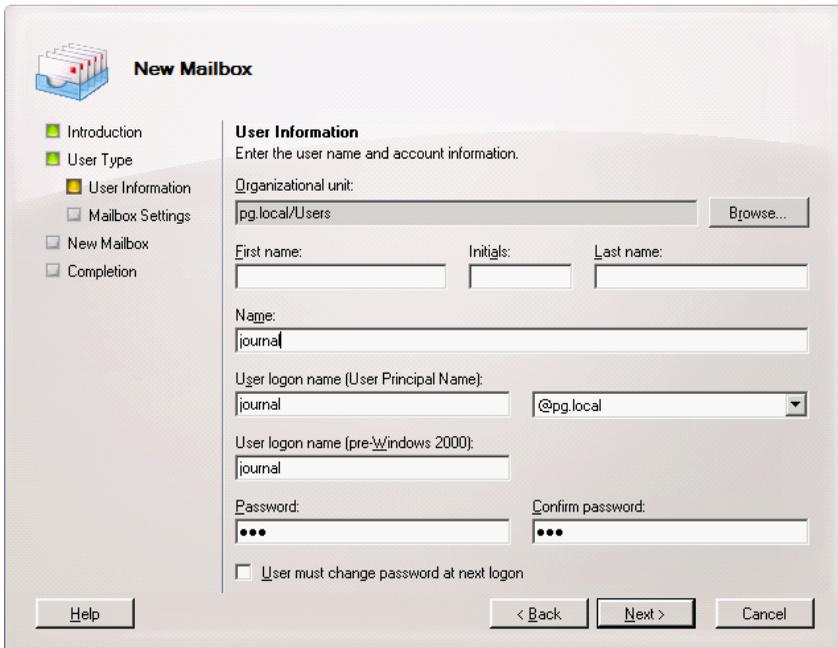


In the next window select **New user** as the user type. Click **Next**.



In the next window specify an Organizational unit the new account will be created in, the Name of the account to create, the User logon name (User Principal Name with the name of the server it is registered on, and pre-Windows 2000 name – these can be the same) and the Password. All other fields are optional.

Click **Next**.



New Mailbox

- Introduction
- User Type
- User Information**
- Mailbox Settings
- New Mailbox
- Completion

User Information
Enter the user name and account information.

Organizational unit:
pg.local/Users Browse...

First name: Initials: Last name:

Name:

User logon name (User Principal Name):
 @pg.local ▼

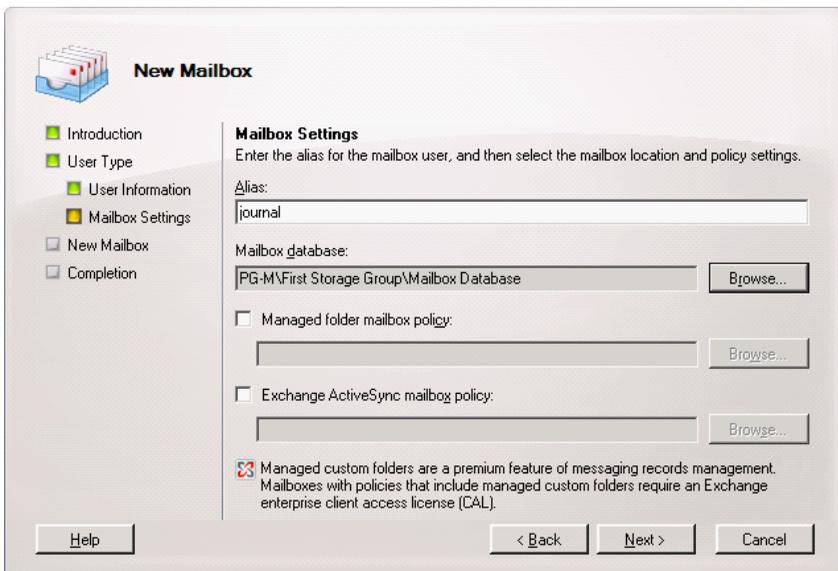
User logon name (pre-Windows 2000):

Password: Confirm password:

User must change password at next logon

Help
< Back
Next >
Cancel

In the next window specify the Alias for the new mailbox (can be the same as the account name) and select the mailbox database used for mail storage. Click **Next**.



New Mailbox

- Introduction
- User Type
- User Information
- Mailbox Settings**
- New Mailbox
- Completion

Mailbox Settings
Enter the alias for the mailbox user, and then select the mailbox location and policy settings.

Alias:

Mailbox database:
PG-M\First Storage Group\Mailbox Database Browse...

Managed folder mailbox policy:
 Browse...

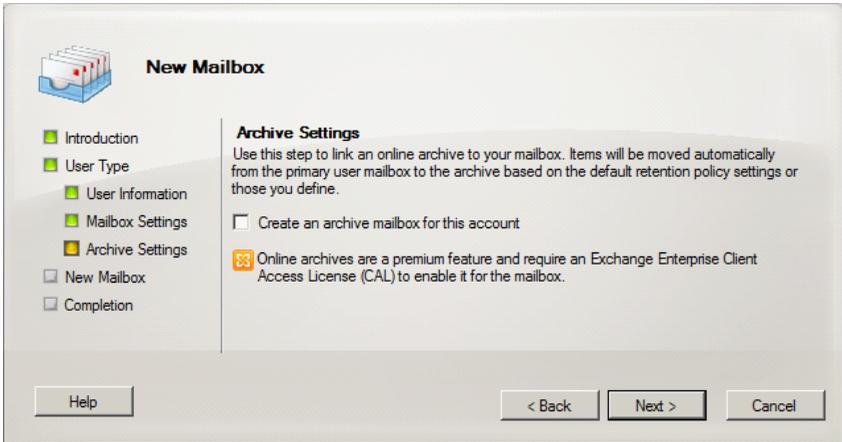
Exchange ActiveSync mailbox policy:
 Browse...

Managed custom folders are a premium feature of messaging records management. Mailboxes with policies that include managed custom folders require an Exchange enterprise client access license (CAL).

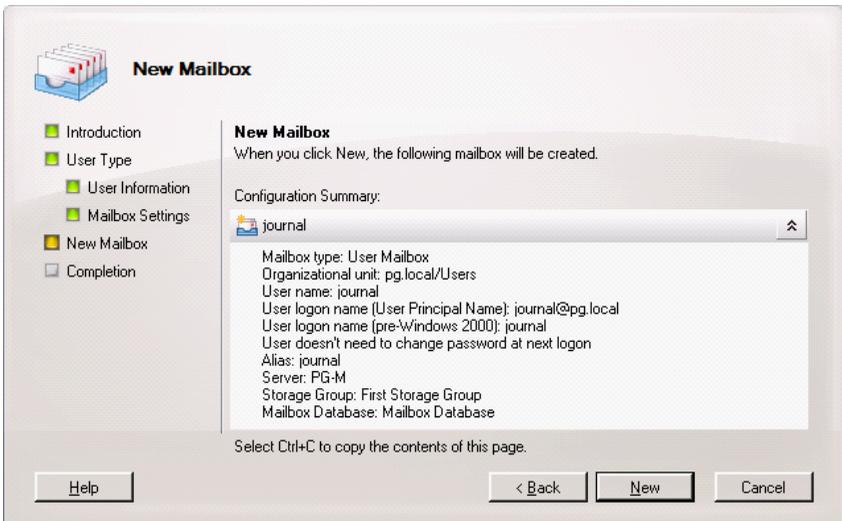
Help
< Back
Next >
Cancel

In case you have MS Exchange Server 2010 version installed on your system, in the next

window you will be suggested to link an online archive to the mailbox. This step is optional and may also be skipped by clicking **Next**.



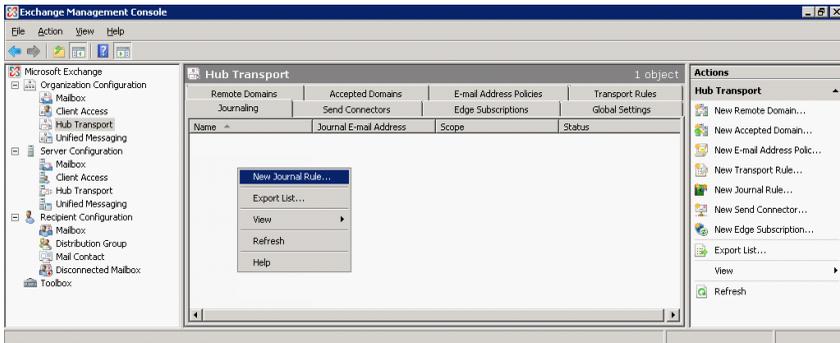
In the next window you will see a summary of all options you have specified for the new mailbox. To change these options click **Back**. To create the new mailbox click **New**.



The new mailbox will be created and will appear in the list of users.

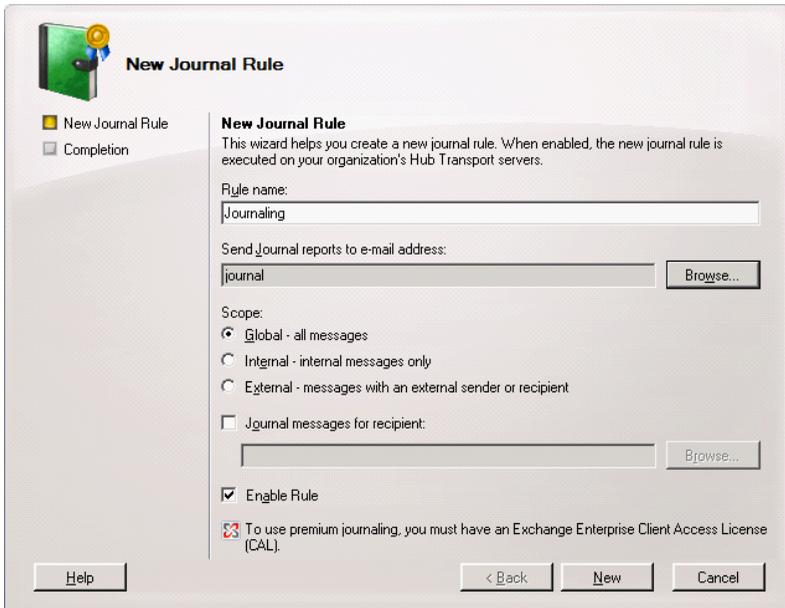
Next, you need to create a transport rule to intercept messages transferred via MS Exchange Server.

Select the **Hub Transport** item under the **Organization Configuration** option in the mail window of the application. Click the **Journalling** tab and right-click on the blank area in the central part of the window. A context menu will appear in which you are to select the **New Journal Rule** option.



A **New Journal Rule Wizard** will open in which you are to specify the following parameters:

- the name of the new rule (type it in the **Rule name** text field);
- the e-mail address all MS Exchange traffic will be sent to (click **Browse** and select the mailbox you have created);
- the **Scope** (select **Global** if you wish to intercept all e-mails, **Internal** – if you wish to intercept only the messages exchanged within the local network, or **External** – if you wish to intercept only messages sent to or received from the outside of your corporate network).



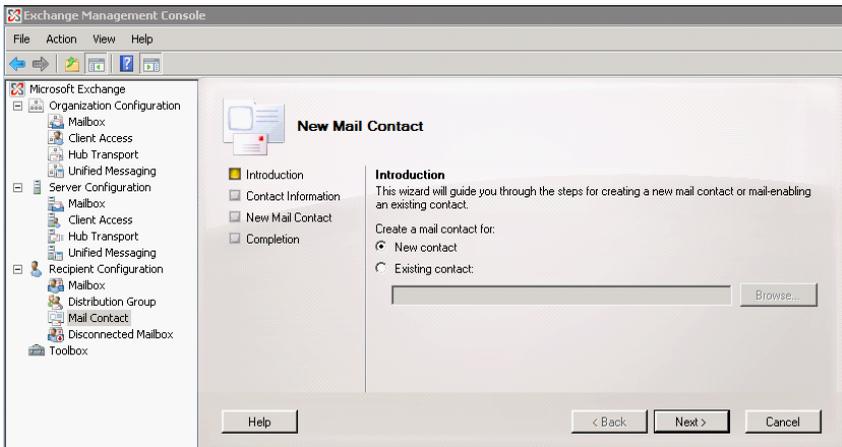
Select the **Enable Rule** check box and click **New** to create the journaling rule and complete the configuration of MS Exchange Server.

Note: For detailed information on all application settings please refer to MS Exchange Server documentation.

12.3.2 Journaling to external mailbox

A journaling rule in MS Exchange Server may be configured to send copies of all e-mails to a special external mailbox, where they will be received by **SecureTower** Mail Processing Server (MPS), i.e. the MPS will act as an external mail server to which the mail flow will be directed. The Mail Processing Server will receive e-mails sent to it over SMTP protocol and store them into its internal database. To configure this type of journaling, follow the instructions below (based on MS Exchange 2007).

First, you have to create a new mail contact with an external mailbox and redirect the mail to a physical server where **SecureTower** Mail Processing Server is installed. To do this, open MS Exchange Management Console and navigate to **Recipient Configuration – Mail Contact**.



Select **New contact** and click **Next**.

New Mail Contact

- Introduction
- Contact Information
- New Mail Contact
- Completion

Contact Information
Enter the account information that is required to create a new mail contact or to mail-enable an existing mail contact.

Organizational unit:

First name: Initials: Last name:

Name:

Alias:

External e-mail address:

In the example above, the name of the external mailbox is set to **external_falcongaze@falcongazemailprocessing.local**. You can set any other name for such mailbox.

Instead of the domain name **falcongazemailprocessing.local** you have to enter the full domain name of the server where **SecureTower** Mail Processing Server is installed. For example, if the server has a name **fg-db** and is located in domain **fg.local**, its full domain name will look like **fg-db.fg.local**

If needed (for example, if the server where **SecureTower** MPS is installed is not in the domain), you can associate the entered server name with a specific IP address. To do this, you need to edit the file C:\Windows\System32\drivers\etc\hosts. Open it and add the following line:

192.168.0.1 falcongazemailprocessing.local

where instead of 192.168.0.1 you should type the IP address of the server where **SecureTower** MPS is installed.

Next, you have to create a journaling rule and direct copies of all e-mails to the mailbox created in the previous step (in the example described above, it is **external_falcongaze**).

New Journal Rule

New Journal Rule
 Completion

New Journal Rule
This wizard helps you create a new journal rule. When enabled, the new journal rule is executed on your organization's Hub Transport servers.

Rule name:
Journaling

Send Journal reports to e-mail address:
external_falcongaze

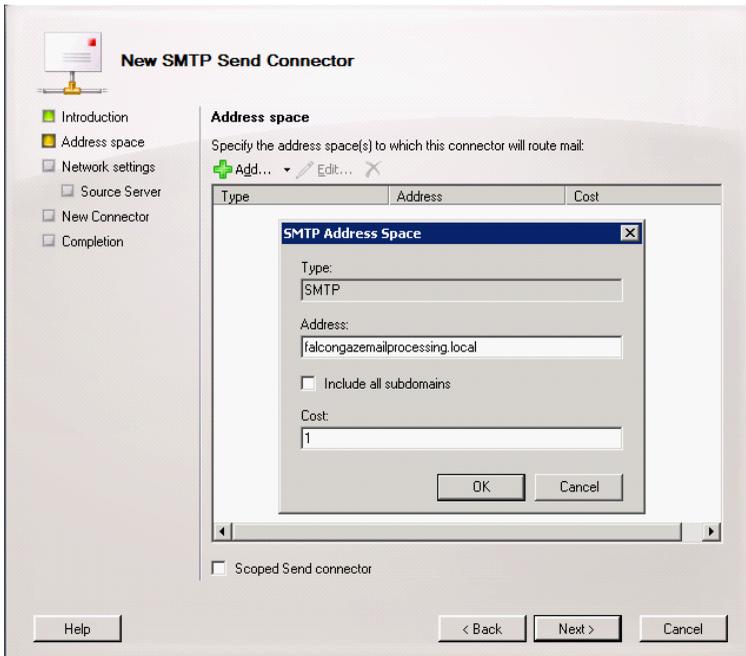
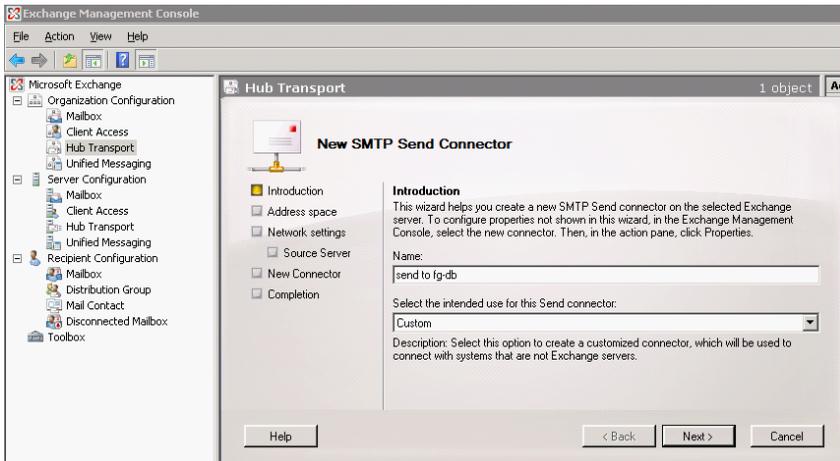
Scope:
 Global - all messages
 Internal - internal messages only
 External - messages with an external sender or recipient

Journal messages for recipient:

Enable Rule
 To use premium journaling, you must have an Exchange Enterprise Client Access License (CAL).

Note: For detailed instructions on creating a journaling rule, refer to paragraph [Journaling to internal mailbox](#).

To enable MS Exchange to send mail over SMTP protocol, you need to add an SMTP Send Connector. To do this, navigate to **Organization Configuration – Hub Transport** in MS Exchange Management Console.



After you have configured journaling in MS Exchange Server, you have to create an SMTP connection in **SecureTower** Administrator Console (**Mail Processing** tab). For detailed instructions on creating an SMTP connection in **SecureTower** refer to paragraph [Receiving mail from server over SMTP protocol](#).

13 Setting up ICAP server

The Internet Content Adaptation Protocol (ICAP) is used by the program to integrate with proxy servers for HTTP(S) network traffic interception.

To configure **SecureTower** and proxy servers integration parameters, click the **ICAP server** tab on the left sidebar of the program's main window.

In order to use the ICAP filter with the most popular proxy SQUID and MS Forefront follow recommendations given below.

SQUID

Squid-3.0 and later come with integrated ICAP support. While installing/upgrading proxy it is necessary to configure the following options as shown below:

- `icap_enable` on
- `icap_send_client_ip` on
- `icap_service service_req reqmod_precache 0 icap://192.168.45.1:1344/reqmod`, where 192.168.45.1 is the IP address of **SecureTower** ICAP server
- `adaptation_access service_req allow all`

MS Forefront

In order to integrate with TMG Forefront with ICAP server the ICAP plugin should be installed first.

Link to download: <http://www.collectivesoftware.com/solutions/content-filtering/icapclient>.

The IP address of **SecureTower** ICAP server should be set upon plugin configuration.

Note: *To prevent the license distribution problems is necessary to ensure the recommendations on firewall configuring (see the [Setting up connection ports for services](#) chapter).*

13.1 General settings

Data storage settings

To configure the database where the information retrieved from traffic via ICAP will be stored, go to the **Data storage settings** section, and click **Select data storage**. For more information see [Selecting data storage type](#).

ICAP server settings

To familiarize with current ICAP settings and to modify them go to the **ICAP server settings** section and click **ICAP server parameters**.

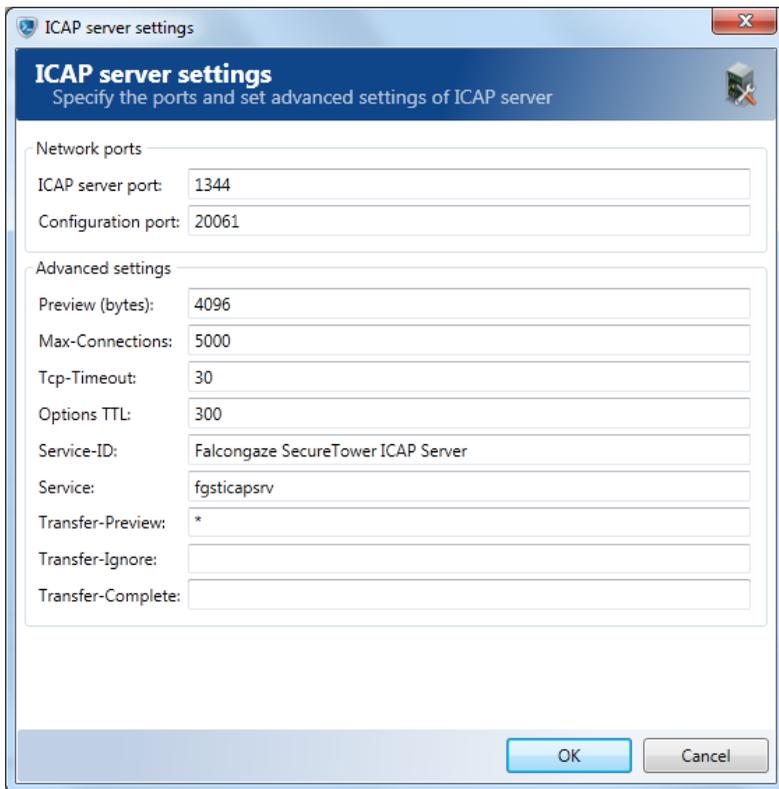
ICAP server settings



You can familiarize with current ICAP settings and configure advanced ICAP parameters

ICAP server settings

In the newly opened window the default networks ports and advanced ICAP settings are provided and accessible for configuring.



Network ports	
ICAP server port:	1344
Configuration port:	20061
Advanced settings	
Preview (bytes):	4096
Max-Connections:	5000
Tcp-Timeout:	30
Options TTL:	300
Service-ID:	Falcongaze SecureTower ICAP Server
Service:	fgsticapsrv
Transfer-Preview:	*
Transfer-Ignore:	
Transfer-Complete:	

1. In the **Networks ports** section the ICAP server port and port for ICAP settings configuring are provided. Specify the user defined port numbers if necessary.
2. In the **Advanced settings** section the following ICAP connection settings are available for viewing and editing (see [RFC 3507 - Internet Content Adaptation Protocol \(ICAP\)](#) for details):

- **Preview:** The number of bytes to be sent by the ICAP client during a preview. This feature enables ICAP server to see the beginning of a transaction, then decide if it wants to opt-out of the transaction early instead of receiving the remainder of the request message. Previewing can yield significant performance improvements in a variety of situations.
- **Max-Connections:** The maximum number of ICAP connections the server is able to support.
- **Tcp-Timeout:** The maximum time of server response waiting in seconds.
- **Options-TTL:** The time (in seconds) for which this configuration (OPTIONS) response is valid. If none is specified, the configuration response does not expire. The ICAP client MAY reissue a configuration request once the Options-TTL expires.
- **Service:** A text description of the vendor and product name.
- **Service-ID:** A short label identifying the ICAP service. It MAY be used in attribute header names. This header MAY be included in the configuration response.
- **Transfer-Preview:** A list of file extensions that should be previewed to the ICAP server before sending them in their entirety. This header MAY be included in the OPTIONS response. Multiple file extensions values should be separated by commas. The wildcard value "*" specifies the default behavior for all the file extensions not specified in any other Transfer-* header (see below).
- **Transfer-Ignore:** A list of file extensions that should NOT be sent to the ICAP server. This header MAY be included in the OPTIONS response. Multiple file extensions should be separated by commas.
- **Transfer-Complete:** A list of file extensions that should be sent in their entirety (without preview) to the ICAP server. This header MAY be included in the OPTIONS response. Multiple file extensions values should be separated by commas.

Note: *If any of Transfer-* are sent, exactly one of them MUST contain the wildcard value "*" to specify the default. If no Transfer-* are sent, all responses will be sent in their entirety (without Preview).*

License server information

In the license server information section of the Endpoint agents control window you are to specify the parameters of access to **SecureTower** license server.

Specify the server address and port used to connect to it in the corresponding fields. Follow recommendations from [Setting up connection to the license server](#).

13.2 IP filter settings

To set up traffic filtering upon ICAP interception, click the **IP filters** tab and click **Enable IP filtering rules**. You can specify IP addresses or ranges that you want to allow or deny intercepting traffic from.

Configure exclusions as described in [IP filter settings for agent settings profile](#).

13.3 HTTP filter settings

To configure interception of data transmitted over HTTP(S) protocol via proxy server, click **HTTP filters** tab of the **ICAP server** window and select the check box of the corresponding option.

For more information about interception configuring, see the [HTTP settings](#) chapter.

13.4 Data blocking

SecureTower ensures blocking of data transferred using HTTP/HTTPS through a proxy server.

Blocking rules can be set up for both the HTTP POST and the GET requests by means of corresponding blocking rules. HTTP GET blocking is intended to deny network users visits of specified insecure web sites. HTTP POST blocking enables control and blocking of any Internet activity such as posting in web chats, social networks conversations, activity of malware programs and so on.

To block traffic through a proxy server:

1. Click the **Data blocking** tab of the **ICAP server** window.
2. To activate blocking mode, add a new blocking rule or group of rules. To familiarize with blocking rule creation and configuring, see the recommendations for data blocking by endpoint agent (the [Data blocking](#) chapter of this guide).
3. To switch on the rule, select the related check box (if not selected) in the list of rules.

In the **Data blocking** tab the root **Blocking rules** group is created by default and unavailable for deleting. One can create other groups or single rule within the **Blocking rules** group. Groups and rules can be created at any hierarchy level as well.

When created and switched on, blocking rules are applied to all intercepted information transferred over HTTP. herewith, all requests with attachments will be intercepted and analyzed by ICAP server to find content that meet search conditions of blocking rules. If the data transferred over HTTP(S) meet one or more rules, the transfer will be blocked. In this case, the user will get an error message: "Content is not available due to corporate security policy!" in his web browser window.

Note: To receive notifications about activity of blocking rules, add corresponding security rule in Security Center of **SecureTower** Client Console (for more information, see **General security rule** chapter of User Guide).

13.5 ICAP statistics

To view detailed data on connections and network activity as a statistics report in a real-time mode, select the **Statistics** tab of the **ICAP server** page.

In the **Statistics** window, the following information is provided: **Current amount of connections**, **Current size** and **amount of requests** and **Uptime** of ICAP server for each moment of time. The statistics is presented in the graphs form with the amount of the respective intercepted data for a certain time interval (see [Calculating statistics for a specified interval](#) for details).

14 Configuring image recognition

The high-tech image recognition **SecureTower** module allows system to recognize the text in the intercepted images with following data analysis. This functionality is useful at situations when the transmission of scanned confidential documents is used. The **SecureTower** system tool works equally well with PDF и DjVu and any format of graphic information, whether it is the JPG, BMP, TIFF format or any other. The module recognizes data not only in English but also in foreign languages, this enables system to carry out content analysis with all the features of morphology.

Image recognition server uses built-in recognition plugin by default to perform optical characters recognition. Beside built-in plugin the system provides integration with ABBYY FineReader.

It is recommended to configure an image recognition plugin settings to increase a recognition process efficiency.

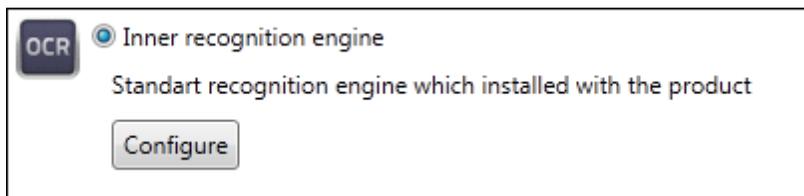
To configure the recognition plugin settings and to familiarize with server statistics, click the **Image recognition** tab in the left sidebar of the program's main window.

Configure the OCR process in the **Common information** tab window:

1. Select the OCR plugin and configure it as described either in [Setting up built-in plugin](#) or [ABBYY settings](#).
2. Specify the database to be recognized (see [Setting up data storages](#)).
3. Specify the port number for server settings configuring in the **API options** section.
4. Set the license parameters to provide access to the license server. Follow recommendations from [Setting up connection to the license server](#).

To view online statistics of the server operation, click the **Statistics** tab of the **Image recognition** window (see [Image recognition statistics](#) for details).

14.1 Setting up built-in plugin



To perform image recognition the specific built-in recognition engine is used in the **SecureTower** system. It provides the system with optical character recognition functionality for following recognized text analysis.

Attention: *By default the built-in recognition engine does not support PDF recognition. To recognize PDF documents download the GhostScript distribution from <http://nicomsoft.com/files/ocr/ghostscript.htm>.*

Install GhostScript on the same server where Recognition Server is already installed. If your

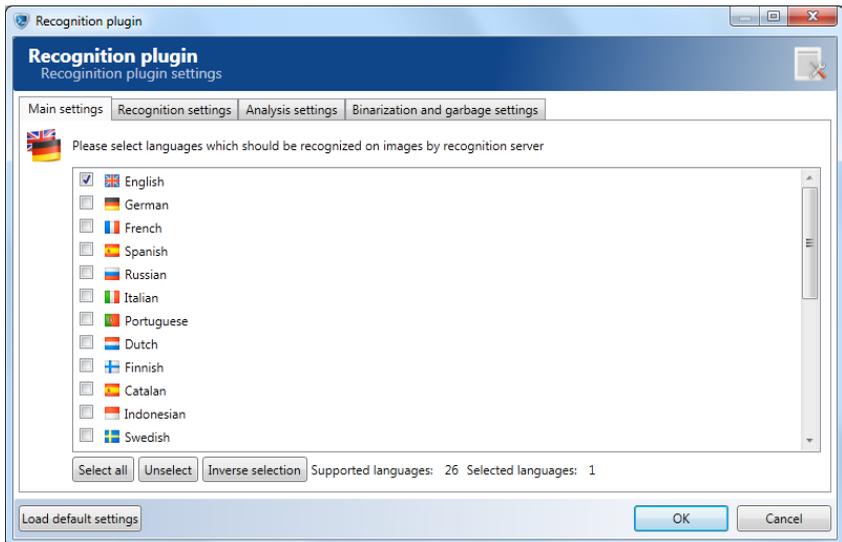
application is 64-bit, download and install 32-bit version of GhostScript and then download and install 64-bit version. Reboot the server after Ghostscript install.

Configuring the plugin for particular needs is a very important step. Different tasks may require different recognition settings, that is why it is possible to achieve best results only if the recognition plugin is configured properly.

To enable recognition and configure plugin settings check on corresponding option and click **Configure**. To manage recognition options, click the relevant tabs of the **Recognition plugin** window . To use default settings click **Load default settings** in the bottom left - hand corner of the **Recognition plugin** window.

Main settings

Select the **Main settings** tab to set languages of intercepted text fragments that should be recognized.



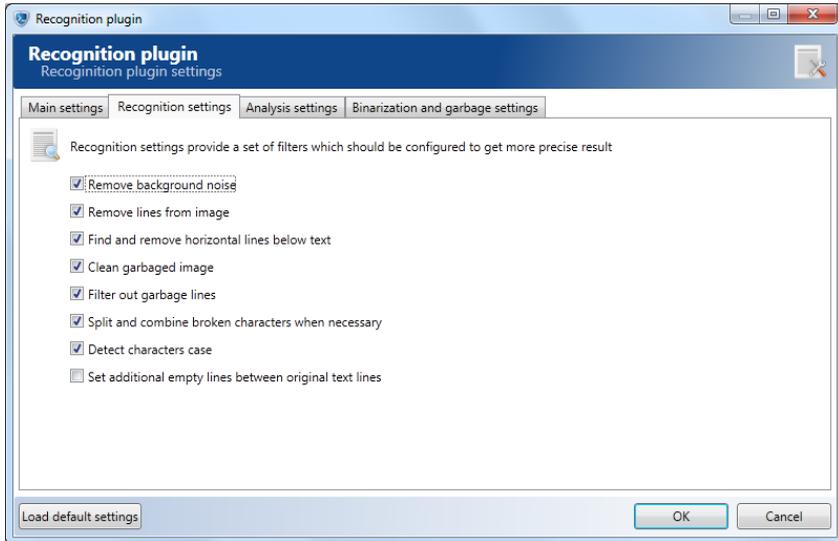
To choose the language you need check the related check box or use one of the selection buttons:

- Click **Select all** to choose all languages from the list.
- Click **Unselect** to cancel previous choice.
- Click **Inverse selection** to cancel previous choice and to choose unselected languages from the list simultaneously.

Notes: At least one language must be enabled. It is possible to select more than one language for recognition. Do not enable many languages if you need to recognize only one, several enabled languages may decrease recognition quality and require more operating memory and CPU time.

Recognition settings

Recognition settings provide a set of filters which should be configured to get more precise result.



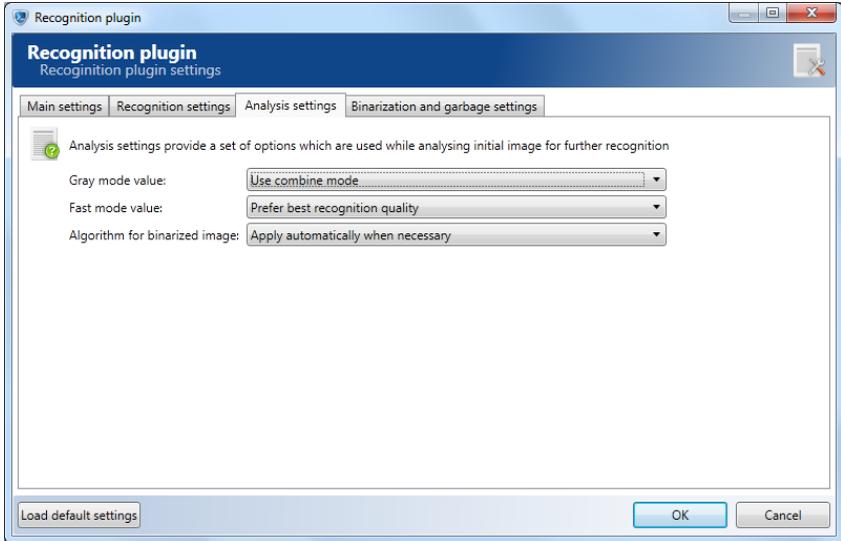
Following options are accessible for activation:

- **Remove background noise** - removes background noise if checked. This option is very useful for images with dotted background.
- **Remove lines from image** - enables search and removing of lines during optical character recognition step to handle text, that was formatted as table or was inserted in frame, properly if checked.
- **Find and remove horizontal lines below the text** - enables search and removing of horizontal lines below the text during optical character recognition step to handle underlined words properly if checked.
- **Clean garbaged image** - applies a smart algorithm to clean garbaged image.
- **Filter out garbage lines** - filters out garbage lines if checked.
- **Split and combine broken characters when necessary** - increases a precision of recognition and text analysis if checked.
- **Detect characters case.**

- **Set additional empty lines between original text lines** - helps to save equal space between lines in processed text during recognition step.

Analysis settings

Analysis settings provide a set of options which are used while analyzing initial image for further recognition.



1. Select one of image preprocessing modes from the **Gray mode value** drop-down list:
 - **Load all images in 8bit gray mode** - loads all images in 8bit gray mode, it requires less memory and faster.
 - **Load all images in 24bit color mode** - loads all images in full color.
 - **Use combine mode** - uses 8bit gray mode for gray and black-white images and use 24bit color mode for color images.
2. Select one of recognition criteria from the **Fast mode value** drop-down list:
 - **Prefer best recognition quality.**
 - **Prefer maximum recognition speed.**
 - **Super fast recognition mode.**
3. Select one of image binarization algorithm modes from the **Algorithm for binarized image** drop-down list:
 - **Apply automatically when necessary.**
 - **Do not apply.**

- **Apply always.**

Binarization and garbage settings

Binarization settings provide a set of options which are used during image binarization process.

Binarization settings

Binarization settings provide a set of options which are used while image binarization

Black factor: (10) 0 255

Space factor: (1,0) 0.1 10

Simple factor: (0) 0 1000

Simple threshold: (255) 0 255

Light factor: (0,4) 0.1 1

1. Specify a value for each binarization factor in the **Binarization settings** zone:

- **Black factor** - advanced black/white pixels factor. Default value is "10.0"..
- **Space factor** - factor of the space between words. Default value is "1.0".
- **Simple factor**: "0" - adaptive space detection is used. "1"..."1000" - directly specifies space size, in pixels. Default value is "0".
- **Simple threshold**: "0"..."254" - simple binarization with specified threshold is used. "255" - intellectual adaptive binarization is used. Default value is "255".
- **Light factor** - is used to adjust final threshold during intellectual adaptive binarization. Default value is "0.4".

Garbage settings provide a list of garbage parameters which are used for noise filtration.

Garbage settings

Garbage settings provide a list of garbage parameters which are used for noise filtration

Big garbage minimum width: (0) 0 10000

Big garbage minimum height: (0) 0 10000

Small garbage maximum width: (0) 0 100

Small garbage maximum height: (0) 0 100

2. Specify a value for each garbage parameters in the **Garbage settings** zone:

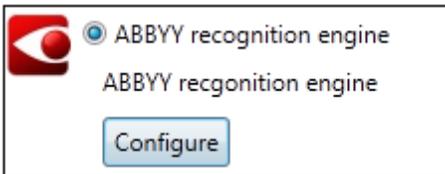
- **Big garbage minimum width**: "0" - does not do anything. "1"..."10000" - removes big

garbage with specified minimal width, in pixels. Default value is "0".

- **Big garbage minimum height:** "0" - does not do anything. "1"..."10000" - removes big garbage with specified minimal height, in pixels. Default value is "0".
- **Small garbage maximum width:**"0" - does not do anything. "1"..."100" - removes small garbage with specified maximum width, in pixels. Default value is "0".
- **Small garbage maximum height:** "0" - does not do anything. "1"..."100" - removes small garbage with specified maximum height, in pixels. Default value is "0".

Click **OK** to finish with recognition plugin configuring or **Cancel** to cancel all action that was done.

14.2 ABBYY settings



To perform image recognition the possibility of integration with ABBYY FineReader is implemented in **SecureTower**.

Configuring the plugin for particular needs is a very important step. Different tasks may require different recognition settings, that is why it is possible to achieve best results only if the recognition plugin is configured properly.

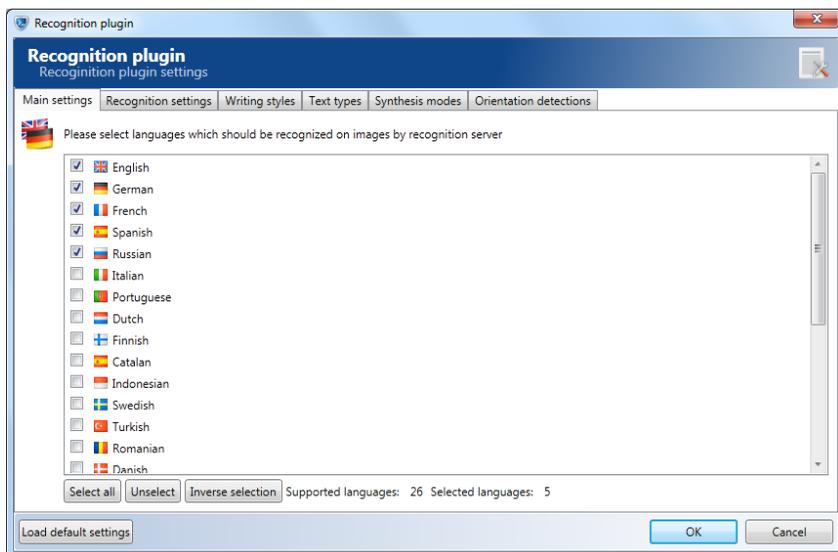
To enable recognition and configure plugin settings check on corresponding option and click **Configure**. If the plugin is not installed by default click **Buy license** and continue configuring after the plugin installation is done.

Use corresponding tabs of the Recognition plugin window to manage recognition options.

To use default settings click **Load default settings** in the Recognition plugin window.

Main settings

Select the **Main settings** tab to set languages of intercepted text fragments that should be recognized. The plugin supports 26 languages: Bulgarian, Catalan, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Hungarian, Indonesian, Italian, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, Turkish .



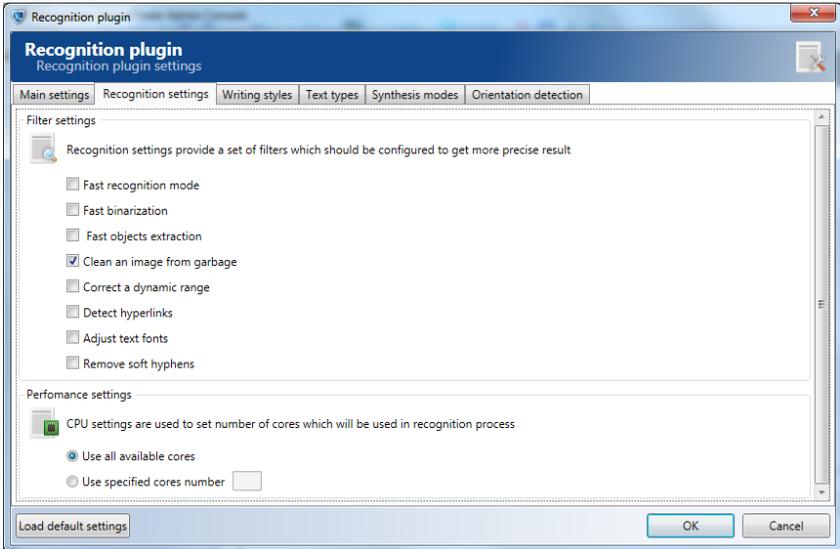
To choose the language you need select the related check box or use one of the selection buttons:

- Click **Select all** to choose all languages from the list.
- Click **Unselect** to cancel previous choice.
- Click **Inverse selection** to cancel previous choice and to choose unselected languages from the list simultaneously.

Notes: *At least one language must be enabled. It is possible to select more than one language for recognition. Do not enable many languages if you need to recognize only one, several enabled languages may reduce recognition quality and require more operating memory and CPU time.*

Recognition settings

Recognition settings provide a set of options which should be configured to get more precise result.



Following options are accessible for activation:

- **Recognition fast mode** - provides 2 - 2.5 times faster recognition speed at the cost of a moderately increased error rate (1.5 - 2 times more errors). We do not recommend using this mode to recognize small image fragments (for example, fragments which consist of only one line or word) because the time advantage will be insignificant.
- **Fast binarization** - ABBYY FineReader Engine will use algorithms for fast image binarization, however binarization quality may deteriorate.
- **Fast objects extraction** - objects extraction is a process which detects additional objects (for example, garbage, texture, small text areas of low quality) on an image before recognition. If this option is checked, objects extraction will speed up, but its quality may deteriorate.
- **Remove garbage from image** - specifies if garbage (excess dots that are smaller than a certain size) is to be removed from the image during objects extraction.
- **Correct dynamic range** - if this property is checked, image colors will be corrected so that the background is white and the text is black, or vice versa, which improves image quality. Recognition, however, will slow down.
- **Detect hyperlinks** - hyperlinks are detected during page synthesis.
- **Adjust text fonts** - specifies whether the set of fonts, which are used during

document synthesis by default, should be extended with the fonts suitable for complex script languages if necessary. If the value of this property is checked and the recognized text contains words in complex script languages, the advanced fonts will be included into the set of fonts, which are used during document synthesis by default.

- **Remove soft hyphens** - tells ABBYY FineReader Engine to remove optional hyphens when exporting recognized text to the output file.

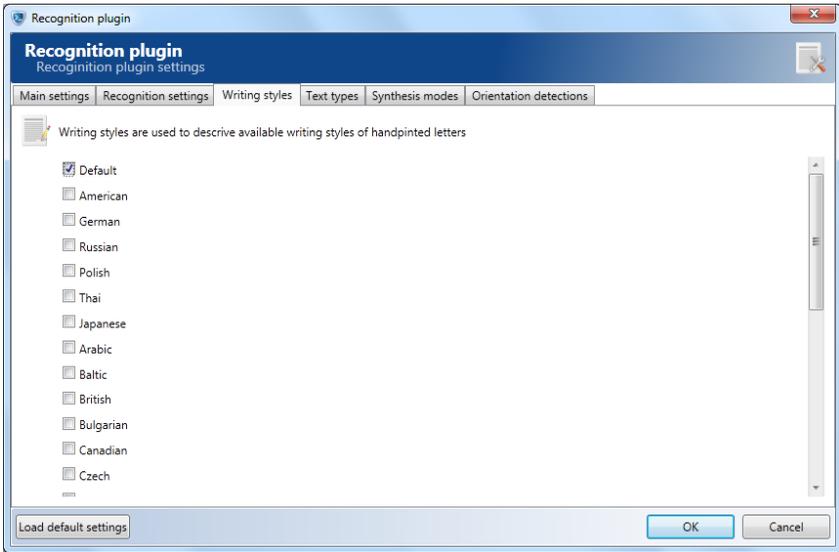
The performance of the recognition server can be configured as well. Select the one from the available processor operating mode:

- **All available cores** - all the available cores will be used during image recognizing to reach the most possible performance.
- **Specified cores number** - support rational distribution of the load on a physical server (where the recognition server is installed). Herewith, the maximum available cores number will be used if the specified number exceeds the real one.

Writing styles

Writing styles options are used to describe available writing styles of hand printed letters.

By default the writing style is selected depending on the current language of the operating system. One can specify the different user styles from available if necessary.



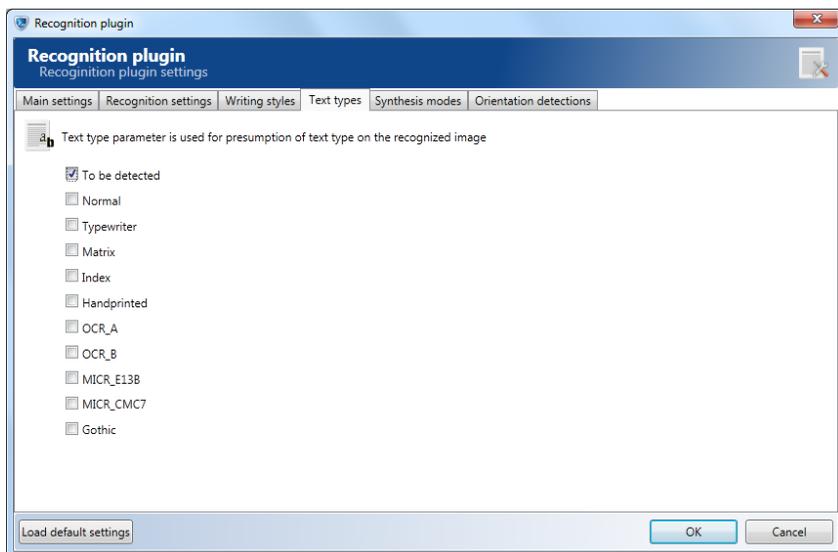
Text types

The **Text types** values denote the possible text types which should be used for recognition process.

ABBYY FineReader Engine will choose from the parameters specified in the **Text types** tab what type should be used while image recognizing. For example, if it is set to Normal or Index, ABBYY FineReader Engine will assume that the text contains only common typographic text and digits written in a ZIP-code style, ignoring all other variants.

ABBYY FineReader Engine can automatically detects the type of a recognized piece of text. When auto detection is on, ABBYY FineReader Engine will first try to detect the type of text. During auto detection, ABBYY FineReader Engine runs preliminary recognition for all of the text types specified in the **Text types** tab. The preliminary OCR results are then compared, ABBYY FineReader Engine selects the type with the best preliminary results and runs the recognizer for this type.

To set auto detection on or to set another one or several types of text select the related check boxes.



To be detected - This value tells ABBYY FineReader Engine to automatically detect the type of the text.

Normal - This value corresponds to a common typographic type of text

Typewriter - This value tells ABBYY FineReader Engine to presume that the text on the recognized image is typed on a typewriter.

Matrix - This value tells ABBYY FineReader Engine to presume that the text on the recognized image is printed on a dot-matrix printer

Index - This constant corresponds to a special set of characters including only digits written in ZIP-code style.

Hand printed - This value corresponds to hand printed text. It may look as follows:

OCR_A - This value corresponds to a mono spaced font, designed for Optical Character Recognition. Largely used by banks, credit card companies and similar businesses.

OCR_B - This value corresponds to a font designed for Optical Character Recognition.

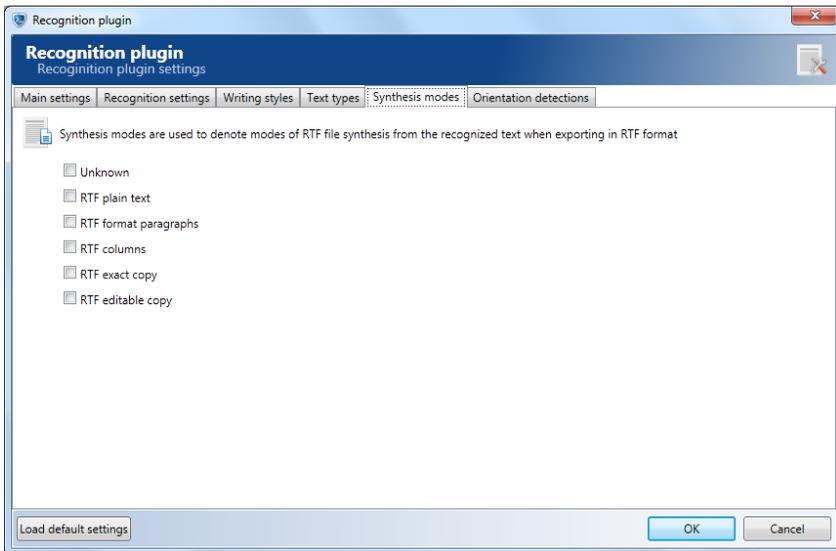
MICR_E13B - This value corresponds to a special set of characters including only digits and A, B, C, D characters printed in magnetic ink. MICR (Magnetic Ink Character Recognition) characters are found in a variety of places, including personal checks.

MICR_CMC7 - This value corresponds to a special set of characters, which includes only digits and A, B, C, D, E characters, written in MICR barcode font (CMC-7).

Gothic - This value tells ABBYY FineReader Engine to presume that the text on the recognized image is printed with the Gothic type.

Synthesis mode

Synthesis modes are used to denote modes of RTF file synthesis from the recognized text when exporting in RTF format.



Unknown - the mode of file synthesis is not defined.

RTF plain text - the text in output file is formatted in a single column. Frames are not used. Paragraphs are retained, while types and sizes of fonts are not retained.

RTF format paragraphs - paragraphs and fonts types and sizes are retained. The text formatting inside paragraphs is not retained.

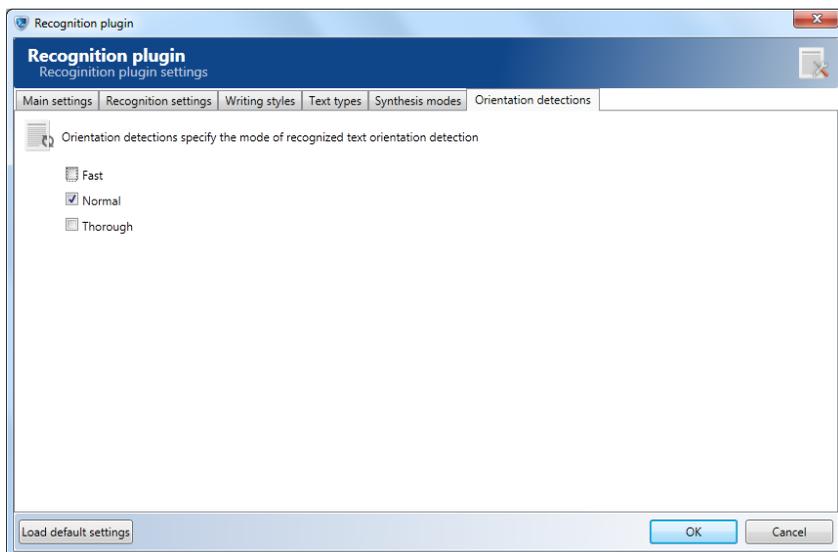
RTF columns - full formatting is retained using columns and frames.

RTF exact copy - produces a document that maintains the formatting of the original. This option is recommended for documents with complex layouts, such as promotion booklets. Note, however, that this option limits the ability to change the text and formatting of the output document.

RTF editable copy - produces a document that preserves the original format and text flow but enables easy editing.

Orientation detection

The page orientation is detected during page processing, and if it differs from normal, Engine automatically rotates the image. One can specify the mode of detection.



Fast mode - this mode provides the fastest speed of orientation detection at the cost of a moderately decreased quality.

Normal mode - the normal mode is an intermediate mode between thorough and fast modes/

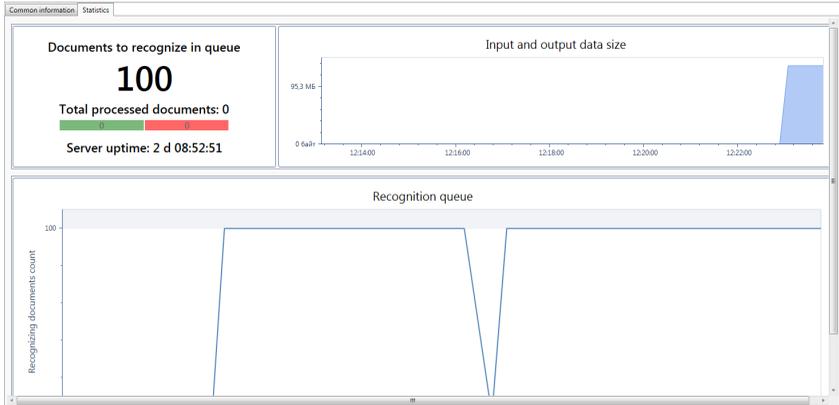
Thorough mode - this mode provides the best quality of orientation detection.

14.3 Setting up data storages

To configure parameters of data base that will be used as image source for recognition process, go to the **Data storages for the recognition process** section. Select one from existed data storages or create a new one as described in [Selecting data storage type](#).

14.4 Image recognition statistics

The current state of recognition processes is provided in the **Statistics** tab window. All of the data are updated and provided in the real time.



The following parameters can be found in the window:

- **Documents to recognize in queue:** the total number of documents in recognition queue at the moment.
- **Total processed documents:** the total number of documents processed by the server since the last start (restart). Upon restart all the data will be reset. The number is considered as the sum of successfully recognised (shown in green) and unrecognized (in red) due to any reasons documents.
- **Server uptime:** The total time of server activity since the last start. Upon restart all the data will be reset.

The **Input and output data size** section depicts the ratio of recognized text size to the total size of documents processed during recognition since the last start (restart) in the real time mode. To see the values of data point to the necessary diagram area. Upon restart all the data will be reset.

The **Recognition queue** section depicts the changes of the processed documents number in the real time.