Going Global with Security
falcongaze™

SecureTower™

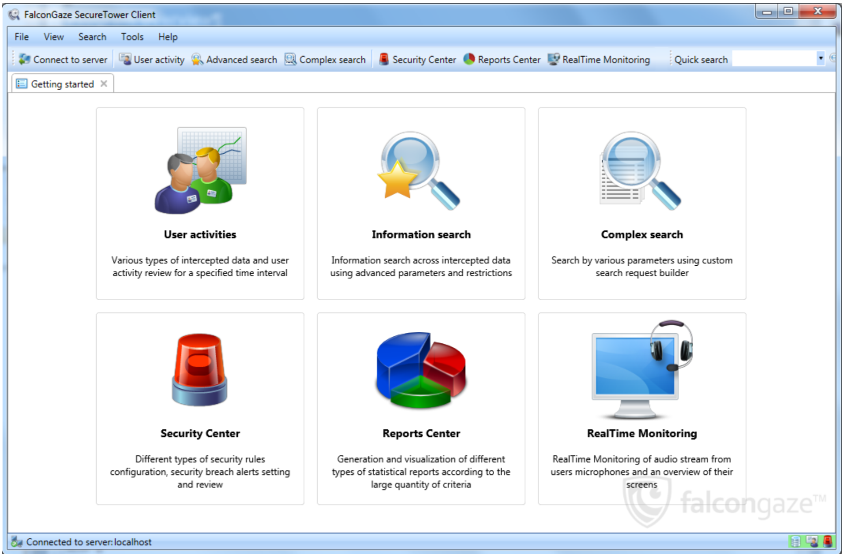
User Guide

Table of Contents

1 Program overview

SecureTower is a complex software product for ensuring internal information security through interception and analysis of network traffic, data, transferred to external devices or local/network printers and clipboard contents.

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.



User activities

Various types of intercepted data and user activity review for a specified time interval

Information search

Information search across intercepted data using advanced parameters and restrictions

Complex search

Search by various parameters using custom search request builder

Security Center

Different types of security rules configuration, security breach alerts setting and review

Reports Center

Generation and visualization of different types of statistical reports according to the large quantity of criteria

RealTime Monitoring

RealTime Monitoring of audio stream from users microphones and an overview of their screens

Connected to server: localhost

The client module of the program provides user with large possibilities of data search, identifying a user in breach of the information security policy, as well as monitoring network activities of certain employees of the organization to evaluate their performance and proper use of their working time.

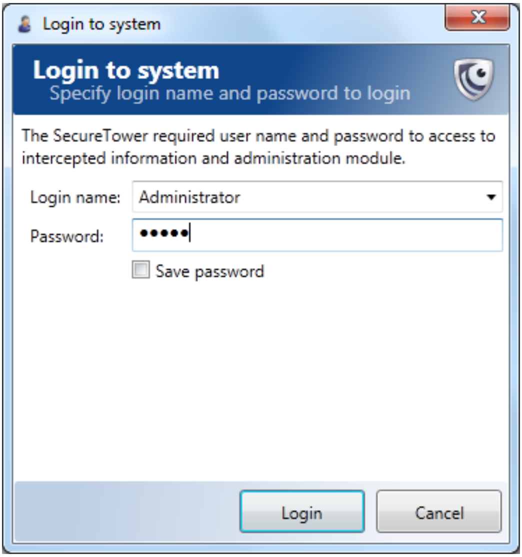
Besides information search and user activity view, security officer can configure **Security Center** settings and delivery of data security breach notifications and use **Reports Center** functionality with FalconGaze **SecureTower** Client Console to build automatic graphical reports based on all kinds of statistical data obtained by the system. Moreover, monitoring of audio stream from user's microphones and video from workstations desktops can be performed in real-time mode.

2 Getting started. Connecting to the server

Access to the Client console

In case you use **SecureTower** internal authentication mode (refer to section ***Setting user authentication mode*** of the *Administrator Guide*), after launching the Client console the user will be required to enter the name and password that have been set for him to access the system. In case you use authentication based on Windows Active Directory accounts, the user will be identified based on the Active Directory account he is currently working under in Windows, so no additional steps will be required. Upon successful logon to the system, the user will only have the privileges set for his group (refer to section *User cards* of this manual and section ***Managing user groups and access rights*** of the *Administrator Guide*).

Note: *While logging in a letters register should be taken into account both for login name and password.*



Login to system

Login to system
Specify login name and password to login

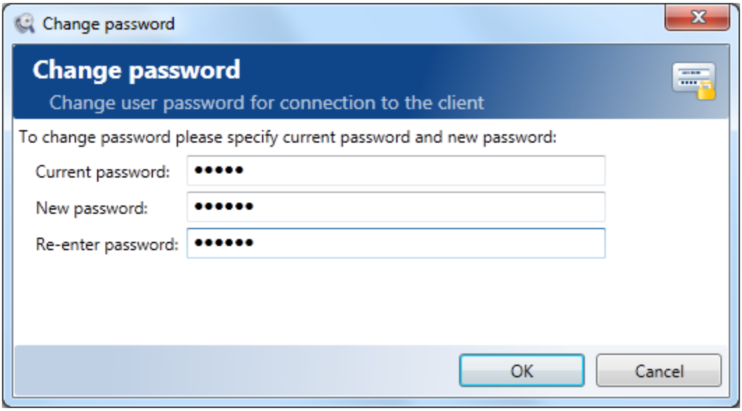
The SecureTower required user name and password to access to intercepted information and administration module.

Login name: Administrator

Password: •••••

□ Save password

To increase security purposes, the administrator may oblige user to change password on next logon. In this case the user will see the following window after he enters his current password.



Change password

Change password
Change user password for connection to the client

To change password please specify current password and new password:

Current password: •••••

New password: ••••••

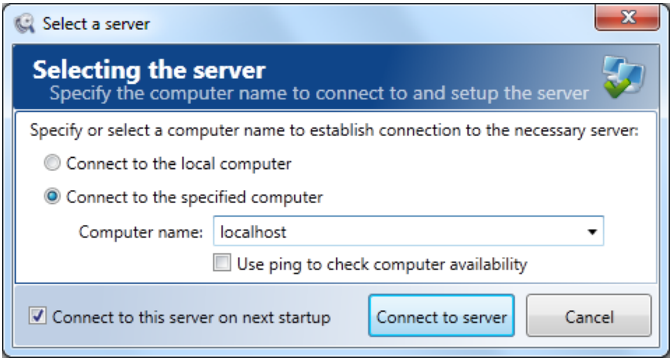
Re-enter password: ••••••

To change the password, the user must enter current password, then the new password twice, and click OK. The password change dialog box can be opened later through the main menu of the Client console (**Tools – Change login password**).

Connecting to the server

Attention! *To support functionality of the client application, the search server that provides database search and access functions must be accessible.*

1. Before starting with the client console, the user should select the server with the search subsystem installed and connect to it. This may be done in the **Select a server** dialogue box that automatically pops up on the main program screen upon the first start.



Select a server

Selecting the server

Specify the computer name to connect to and setup the server

Specify or select a computer name to establish connection to the necessary server:

○ Connect to the local computer

● Connect to the specified computer

Computer name: localhost

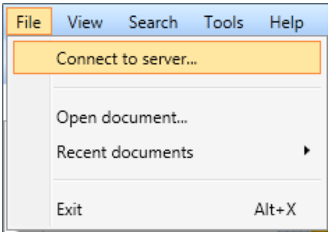
□ Use ping to check computer availability

☑ Connect to this server on next startup

2. If the search subsystem is installed on a local computer, select the **Connect to the local computer** option. If the search subsystem is installed on a remote computer, select the **Connect to the specified server** option and enter its name or IP address.

3. After connecting to the server, you can start working with the client console. If you want to have the program connect to the specified server automatically upon the next startups, enable the **Connect to this server on next startup** option. If you do not have information about the server which should be connected to in order to work with the product, you can request server parameters from the system administrator.

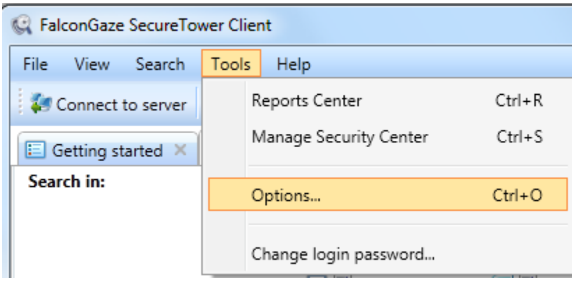
4. If you need to connect to another server, click **Connect to server** on the program toolbar or click this command on the **File** menu.



3 Quick tips for results viewing

Search results viewing

To adjust any result display settings on the **Tools** menu, click **Options**.



In the **Program options** window, you can select or clear the following check boxes:

Option	Description
Open already opened documents in a new tab	Upon being clicked in a search result list, user activity window or security center, the previously viewed documents will be opened in a new tab. Please note that window duplication is possible with this option enabled, meaning that the same search result will be opened in several windows.
Auto preview the first result in the list of found documents	In any search result list, the first result will be automatically previewed, with this option enabled.
Automatically navigate to the first found word in the document	If this option is enabled, any document that is opened in a **Search results** tab or the **Security Center** window will be automatically scrolled down to the first word that matches your search query.
Remember the last save location for the save results list	The last selected location will be used to save search results by default.
Open Security Center notification in a new tab	Select this check box to open security rule notification list in a new tab. Unless it's clear the notifications list will be opened in a current tab by default.

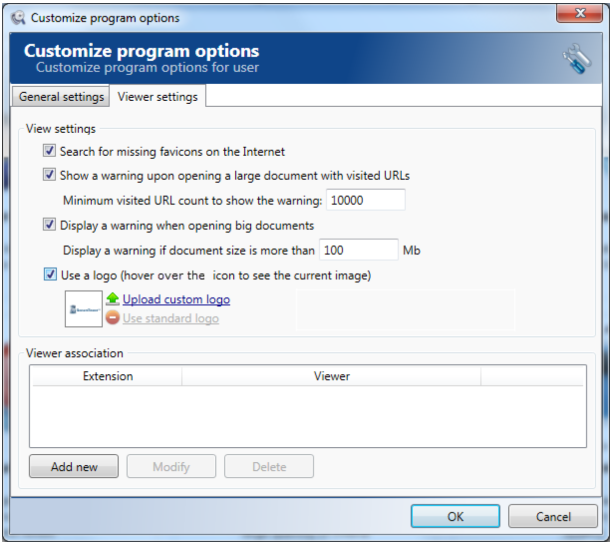
Option	Description
Build user activity report upon user selection	If this check box is selected, a user activity report will be built upon clicking the user name in the users list of User Activity tab.
Resolve IP addresses to computer name	This check box selection enables including IP address information into search results. Herewith, IP address resolving is recommended to be disabled if DHCP server is used in a local network. Compliance between IP and host name is fixed in the moment of interception and may be irrelevant for the moment of inspection.
Replace "Unknown user" text with contact information	Select this check box to enable automatic replacement of unknown user identifier with available contact information such as Active Directory user account (if existed), network contact information (email, messengers ID and so on in consistence with activity type) or intercepted IP address. The "Unknown user" phrase indicates that the user card for this user was not found in the program database.

One can specify the program interface view scale and a default save location for RealTime Monitoring results.

Setting plug-ins for viewing files with non-standard extensions

The application might not recognize some extensions of intercepted files and documents, so the user may specify plug-ins to view files with certain extensions and save such settings in the program. To do this:

1. Go to the **Viewer association** tab of the **Customize program options** window and click **Add new**.



Customize program options

Customize program options

Customize program options for user

View settings

☑ Search for missing favicons on the Internet

☑ Show a warning upon opening a large document with visited URLs

Minimum visited URL count to show the warning: 10000

☑ Display a warning when opening big documents

Display a warning if document size is more than 100 Mb

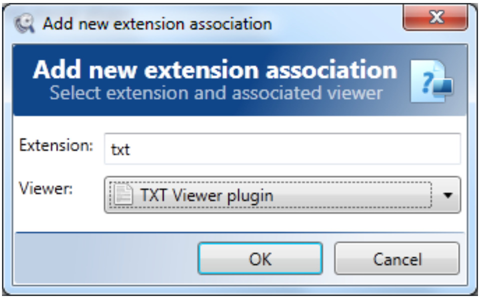
☑ Use a logo (hover over the icon to see the current image)

Viewer association

Extension	Viewer

2. In the **Extension text** box of the **Add new** extension association window, type the extension that you want to configure a viewer for, and in the **Viewer** drop-down list, select the appropriate plug-in for viewing files with the specified extension.

3. Click **OK**.



Add new extension association

Add new extension association

Select extension and associated viewer

Extension: txt

Viewer: TXT Viewer plugin

4. The newly added association will be displayed in the list of associations.

5. To modify viewer settings for a specific extension, select the respective association in the list and click **Modify**. In the **Modify** extension association window, enter the necessary changes and click **OK**.

6. To delete some association, select the respective association in the list and click **Delete**. In the action confirmation dialogue window, click **Yes**.

7. To save the settings, click **OK** in the **Customize program options** window.

The following options for results viewing optimization can be configured as well :

Option	Description
Search for missing favicons on the Internet	The favicon for the website will be added automatically while results presenting.
Show a warning upon opening a large document with visited URLs	The program will warn you if the search result document contains too many URLs which may take more time to load.
Minimum visited URL count to show the warning	In this entry field, you can specify the minimum number of URLs on which a warning will be shown.
Display a warning when opening big documents	The system will display a warning when you try to open a large document, which may take much time
Display a warning if document size is more than ...	One can set the size of a document being opened (in MB) to display a warning.
Use a logo	If the option is active the SecureTower logo will be used in the header of the output files by default upon saving monitoring and search results. Hover over the icon to view the currently used logo in the original size. To upload the custom logo click **Upload custom logo** and specify the necessary image file. Uploaded image will be used bu default. Note, that maximum image size is 256x128. If the image size is larger the image will be compressed upon upload process. To use the standard SecureTower logo instead the custom click **Use standard logo**. If the option is deactivated the results files will be saved without logo at all.

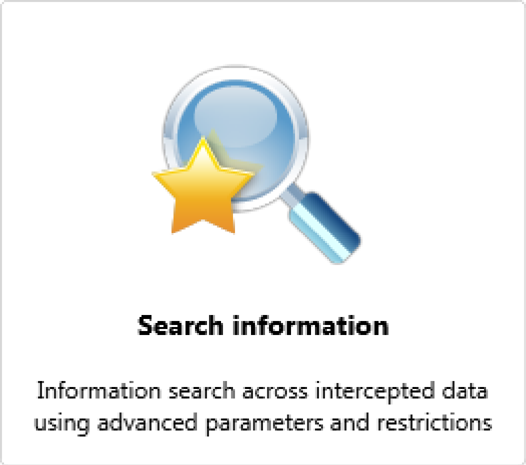
4 Search

One of the most important functions of the client module is a possibility of searching the information contained in the product database. There are two main search modes: “simple” and “advanced”. While the first mode, search is based on all intercepted information, including document attributes (however, the search may be restricted by the information type). In the second case, the search request may be specified with additional parameters.

4.1 Advanced search

An advanced search provides more precise and relevant search results. In the advanced search window, you can carry out a search through specifying additional search conditions and parameters. For example, you can search by the specified words or phrases only, or restrict the search by time and date of data interception, e-mail address, certain user, message subject, etc. You can specify certain search parameters for each type of required data individually (for e-mail, instant messages, web, and files).

To perform an advanced search, click in the **Search information** area on the program start page or click **Open new advanced search window** on the **Search** menu.



Search information

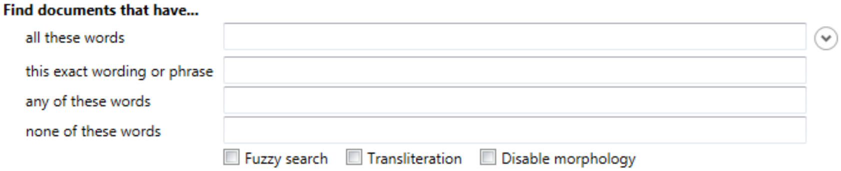
Information search across intercepted data using advanced parameters and restrictions

Access to advanced search are also is available by clicking **Advanced Search** on the console toolbar.

You will be redirected to the new tab in which you will be able to specify advanced search parameters. The advanced search window contains a search request field and additional parameters fields. To start the search, after entering all the necessary parameters for search request, click **Search** under the **Results limit** button.

4.1.1 Full-text search conditions

The program can perform searching operation using various search conditions: search of documents that have all specified words in the query, a specific word or phrase or any of specified words entered. Also, excluding the documents that contain certain words from the search is possible.



Find documents that have...

all these words

this exact wording or phrase

any of these words

none of these words

□ Fuzzy search □ Transliteration □ Disable morphology

These conditions are applied if the text field with the corresponding condition is filled with a word or phrase for the search request. For example, to search the document that contains the exact phrase, you should enter this phrase in the text field in front of the **Find documents with exact word or phrase** condition.

Search condition	Guidelines
Find documents with **all words** from the query	Enter words or phrases that should be in the target documents in the **all these words** text box. The search results will contain documents with all words specified in the query. While searching by all entered words, you can set additional search parameters: - **Word proximity**. Searching for all entered words taking into account of their proximity in the text. For example, if value 5 is set, the system will display documents containing the words of the search query, only if there are not more than 5 other words between them. - **Strict word order**. If this option is enabled, the system will display documents containing the words of the search query in the exact same order as they were entered into the search field.
Find documents with the **exact word or phrase**	Enter a word or phrase that should be in target documents in the **exact wording or phrase** text box. The search results will show the documents that contain this exact phrase you entered.
Find documents with **any words** from the query	Enter words or phrases that should be in the target documents in the **any of these words** text box. The search results will show the documents that contain any of the words you have

Search condition	Guidelines
	specified.
Find documents with **absence of words** from the query	Enter words or phrases that should not be in the target documents in the **none of these words** field. The search results will not show the documents that contain the words you specified.

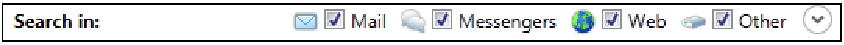
Additional search options applied to all text fields of the query:

- **Fuzzy search** – enables searching for words resembling the ones entered. Activation of this parameter may be helpful when searching for keywords in instant messengers (as the results will also include mistyped keywords), in the documents processed by optical recognition systems (as this will enable detection of keywords with incorrectly recognized symbols), etc. If 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 irrelevant search results.
- **Transliteration** – transliteration is a feature that is only applied to the Russian language and used to search for Cyrillic words transliterated with Latin symbols.
- **Disable morphology** – provides "exact concurrence" search. In common cases the morphology of the language is taken into account upon search processes, but in some cases it may lead to a big quantity of unexpected results. Enabling this option may be useful if it is necessary to find target documents with original words form that were specified.

***Note**: All search fields support double-quoted phrases to search for exact match (except for "this exact wording or phrase" field, where double quote marks will not affect the search results).*

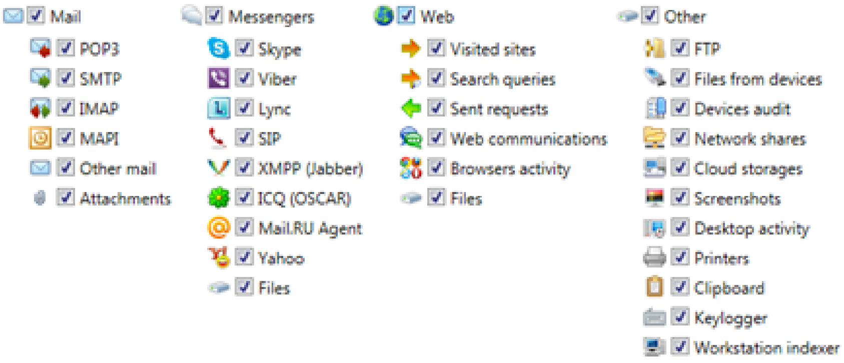
4.1.2 Search by data type

To specify the search context, select one or several types of data which should be searched (search within e-mail data, instant messengers, visited web-pages, transferred files) by selecting the check boxes related to the data sources in the **Search in** section.



Search in: ☑ Mail ☑ Messengers ☑ Web ☑ Other

To specify detailed parameters of data sources to search, click the unfold button .



- ☑ Mail
  - ☑ POP3
  - ☑ SMTP
  - ☑ IMAP
  - ☑ MAPI
  - ☑ Other mail
  - ☑ Attachments
- ☑ Messengers
  - ☑ Skype
  - ☑ Viber
  - ☑ Lync
  - ☑ SIP
  - ☑ XMPP (Jabber)
  - ☑ ICQ (OSCAR)
  - ☑ Mail.RU Agent
  - ☑ Yahoo
  - ☑ Files
- ☑ Web
  - ☑ Visited sites
  - ☑ Search queries
  - ☑ Sent requests
  - ☑ Web communications
  - ☑ Browsers activity
  - ☑ Files
- ☑ Other
  - ☑ FTP
  - ☑ Files from devices
  - ☑ Devices audit
  - ☑ Network shares
  - ☑ Cloud storages
  - ☑ Screenshots
  - ☑ Desktop activity
  - ☑ Printers
  - ☑ Clipboard
  - ☑ Keylogger
  - ☑ Workstation indexer

By selecting/clearing the corresponding options, you may limit the data types for search to the following types:

- for **e-mail**: search for e-mails transferred via **POP3, SMTP, IMAP, MAPI** protocols (these options include mail sent and received using e-mail client applications and captured using centralized interception or by agents at endpoints), other mail (this option includes mail captured by the **SecureTower** Mail Processing Server by integration with corporate mail servers), or search for e-mail attachments;

- for **messengers**: search for correspondence via **ICQ (OSCAR protocol), Skype,SIP, XMPP (Jabber), Viber, Mail.Ru Agent, Yahoo IM, Microsoft Lync** or search for files transmitted over instant messengers;

- for **Web (HTTP)**: search for **visited sites**, **search queries**, **sent requests** (this option includes web mail, posts in blogs, Web forms filled, etc.), net activity via **web browsers**, chat **conversation in social networks** and forums or search for **files** downloaded/uploaded via HTTP;

- for other information type: search for files transferred over **FTP** protocol, copied to **external devices, cloud storage** or **network shares**, **printed** on local/network printers, user **desktop screenshots**, as well as **desktop activity** and **devices usage** statistic, **keylogger** data and **clipboard** content, and incidents of coincidence with **files from files hashes bank** detection.

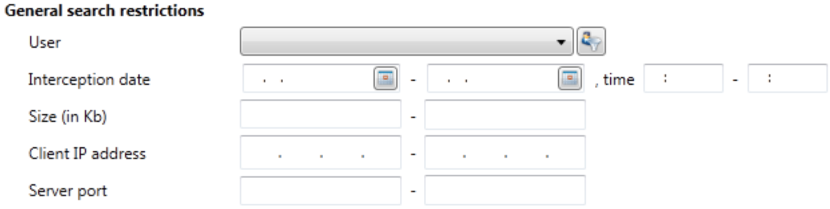
Note: *Clicking the central mouse button (scroll wheel) on any of the four major data types (Mail, Messengers, Web, Files) will select/clear all of the options check boxes.*

4.1.3 The number of shown results

Results limit 500 results ▾

By default, the program provides 500 most relevant search results. You can set another limit for the number of search results provided by the program by selecting the desired value in the **Results limit** drop-down list**.**

4.1.4 General search restriction parameters



General search restrictions

User

Interception date . . - . . , time : - :

Size (in Kb) -

Client IP address . . . - . . .

Server port -

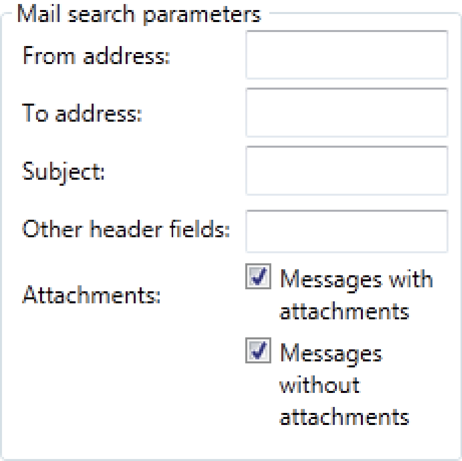
Search restriction	Guidelines
by user name	If you want to search for the information for a certain network user, select the necessary user on the **User** menu by clicking the drop-down arrow.
by date and time of data interception	To get results on the data intercepted within a certain period of time, enter the necessary value range in the **Interception date** field or select the corresponding dates in the drop-down window opened by clicking **the calendar icon**. To specify the time interval of data interception, enter the necessary value range in the **time** field. *If only the first field is filled, the search will be made starting from the specified date and further on without any limitation. If only the second field is filled, the search will be conducted starting from an indefinite moment in the past up to the specified date.* To remove search restriction by the specified date, click the cross in the right corner of the corresponding date field. ***Note**: Search restriction by time is not applicable for IM conversations; only search restriction by date is valid for this type of data.*
by document size (in KB)	If you want to restrict the search by file and data size, enter the necessary value range in the **Size (in KB)** field. If only one field is filled, the search will be made within all the data regardless of their size. ***Note**: This type of restriction is allied only for physical files. It is not valid for IM conversations.*
by local IP address and remote server port	If you want to restrict the search by local IP address, enter the necessary value range in the **Local IP address** field. To

Search restriction	Guidelines
	specify the remote port range, enter the necessary values in the **Remote port** field. *If only one field is filled, the search will be made within all the data regardless of their IP address or port.*

4.1.5 Search parameters for different data types

SecureTower system allows user to obtain the most relevant search results for each type of the intercepted data. To increase an accuracy of search results set up available parameters for each data type.

4.1.5.1 Mail search parameters



Mail search parameters

From address:

To address:

Subject:

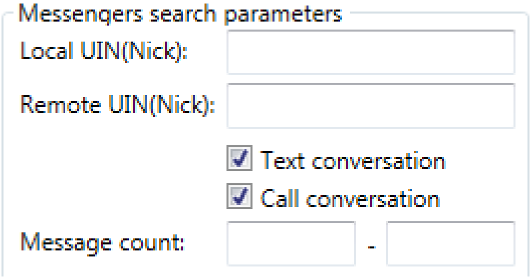
Other header fields:

Attachments: ☑ Messages with attachments ☑ Messages without attachments

Mail search parameters	Guidelines
Search by the sender address	If you want to restrict the search by the sender address, specify the necessary e-mail address in the **From address** field in the **Mail search parameters** section.
Search by the recipient address	If you want to restrict the search by the recipient address, specify the necessary e-mail address in the **To address** field in the **Mail search parameters** section.

Mail search parameters	Guidelines
Search by subject	If you want to restrict the search by a message subject, specify the subject of the message you want in the **Subject** field in the **Mail search parameters** section.
Search by other header data	If you want to restrict the search by other header data, specify the necessary information in **Other header** fields in the **Mail search parameters** section.
Find mails with attachments	To search within e-mail messages that have attachments, select the **Messages with attachments** check box in the **Mail search parameters** section.
Find mails without attachments	To search within e-mail messages that do not have attachments, select the **Messages without attachments** check box in the **Mail search parameters** section.

4.1.5.2 Messengers search parameters



Messengers search parameters

Local UIN(Nick):

Remote UIN(Nick):

☑ Text conversation

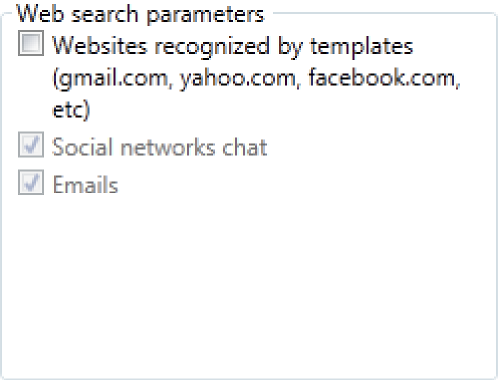
☑ Call conversation

Message count: -

Messenger search parameters	Guidelines
Search by local user account (UIN, nick, user name, etc.)	If you want to restrict the search by a local user account, specify the necessary user information in the **Local UIN (Nick)** field in the **Messengers search parameters** section.
Search by remote user account (UIN, nick, user name, etc.)	If you want to restrict the search by a remote user account, specify the necessary user information in the **Remote UIN (Nick)** field in the **Messengers search**

Messenger search parameters	Guidelines
	parameters section.
Find text conversations only	To search within the text conversation only select the **Text conversation** check box in the **Messengers search parameters** section.
Find call conversations only	To search within the call conversation only select the **Call conversation** check box in the **Messengers search parameters** section.
Find conversations with a certain number of messages	To restrict the search by a number of messages exchanged within a conversation, specify the necessary value range in the **Message count** field in the **Messengers search parameters** section (For example, from 1 to 50). ***Note**: If only one field is filled, the search will be made within all the conversations regardless of the number of messages.*

4.1.5.3 Web search parameters



Web search parameters

☐ Websites recognized by templates (gmail.com, yahoo.com, facebook.com, etc)

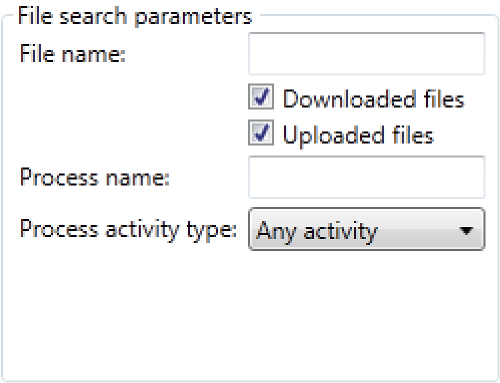
☑ Social networks chat

☑ Emails

Web parameter	Function
Web sites templates	For a more user-friendly presentation of data intercepted over HTTP protocol, **SecureTower** system features several data

Web parameter	Function
	templates. Such templates are available for most popular websites through which users can exchange information (in the form of messages, emails, posts and comments on blogs, forums, etc.): facebook.com (including chat rooms and message), gmail.com, blogger.com, livejournal.com, hotmail.com, myspase.com, linkedin.com, twitter.com, loveplanet.com, various forums (if their address contains the word «forum»), web messengers, etc. To search only for data exchanged via the sites for which such templates are available, select the check box of corresponding option in the advanced search parameters.
Social networks chat	To search only for data exchanged via social networks such as Facebook, Odnoklassniki, Vk, Twitter select the **Social networks chat** option.
Emails	To search only for mail exchanged via web interface select the **Emails** option.

4.1.5.4 File search parameters



File search parameters

File name:

☑ Downloaded files

☑ Uploaded files

Process name:

Process activity type: Any activity

The program enables interception of files and documents that network users transfer in instant messengers, as well as post and upload on the visited web-resources over the HTTP and FTP protocols. Such documents may be of various formats: text, graphic, audio files, archives, etc.

Note: *This section of the* ***Advanced search*** *window does not allow user to set parameters for searching files that were sent or received as mail attachments. To specify search parameters for mail attachments, go to the* *Mail search parameters* *section of the* ***Advanced search*** *window.*

Files may be transferred by one of the following ways:

- Within an instant messenger conversation (ICQ, Skype, Viber, SIP)
- Uploaded to or downloaded from an HTTP-server (to a user page of social network, forum, or blog)
- Uploaded to removable mass storage devices or network shares
- Uploaded to or downloaded from an FTP-server (to read more about the FTP protocol, go to section *Viewing files transferred over FTP protocol*)

The program enables interception and viewing both sent and received files.

The program enables monitoring of application activity on users workstations as the part of the desktop activity monitoring as well. The start, stop or any type of activity data is available for search and viewing.

Search by file name	To search within files with a certain name, enter the name of the desired file in the **File name** field in the **File search parameters** section.
Search by received files	To search within the received files only, select the **Downloaded files** check box in the **File search parameters** section.
Search by sent files	To search within the sent files only, select the **Uploaded files** check box in the **File search parameters** section.
Search by process name	To search within processes with a certain name, enter the name of the desired process in the **Process name** text box in the **File search parameters** section.
Search by activity type	To search within processes with a certain type of activity only click the one in the **Process activity type** list in the **File search parameters** section.

4.2 Quick serch

To obtain a general search result:

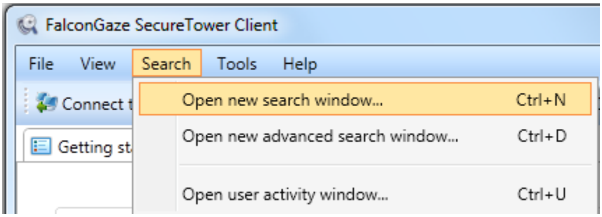
Type a search request in the **Quick search** input field located in the program toolbar.

While quick search procedure a full-text search throughout intercepted data without possibility of search options tune is executed.

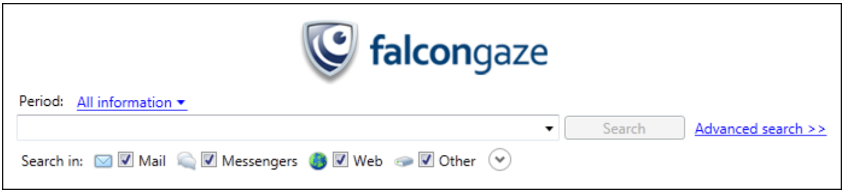
4.3 Simple search

To make a “simple” full-text search:

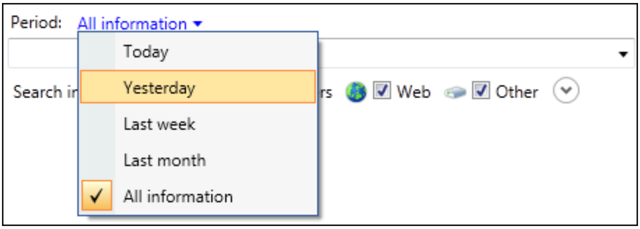
1. On the **Search** menu, click **Open new search window**.


FalconGaze SecureTower Client
File
View
Search
Tools
Help
Connect t
Getting st
Open new search window... Ctrl+N
Open new advanced search window... Ctrl+D
Open user activity window... Ctrl+U

2. Enter the words or phrases field by which you want to execute a full-text search in the search. If you put a word or phrase in double quotes, the system will execute an exact-match search. Otherwise, the program will execute search by one of the words entered (the OR operator) with the language morphology taken into account. To specify the search context, select one or several data types within which the search will be executed (search within e-mail, messengers, web, or/and files).



3. With the **Period** drop-down menu, you can restrict your search by the specifying exact time period of data interception. Only the data that were intercepted within the specified period will be included in search results.



4. Specify necessary search parameters and click **Search**.

- Go to advanced search by clicking the **Advanced Search** link if it’s necessary (for more information, see *Advanced Search*).

4.4 Complex search

Complex search allows user to create rules of search operations based on the text content of the captured data, IP-addresses (local or remote), the specified port (local or remote), user name, data size, data type, and date of interception.

To start with the complex search within the intercepted network traffic, click in the **Complex search** area or click the corresponding button on the toolbar of the client console window. Access to complex search is available from the **Search** menu as well.

From the **Complex search** window the various conditions of search operations are available for configuring as well as the list of favorites search queries which can be used as templates further.

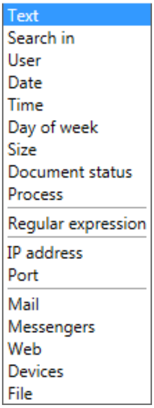
4.4.1 Creating a search request

Data can be searched by a certain text or a regular expression in the intercepted data, IP address (as well as local or remote), by the specified port (as well as local or remote), by a user name, by the size of data, by the type of data and by the interception date.

1. 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 will be created instead.

2. 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.

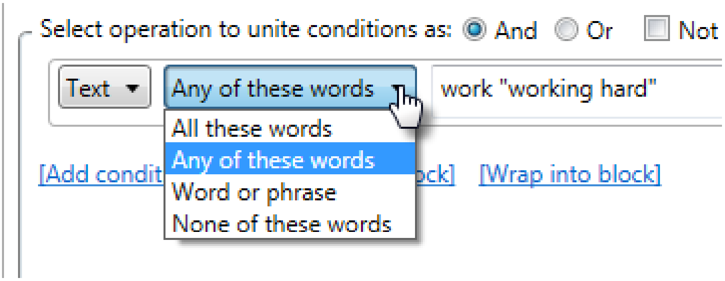
Condition types are available in the drop-down list opened by clicking the **Text** button.



For various search conditions different relevant operations can be specified.

For the 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.

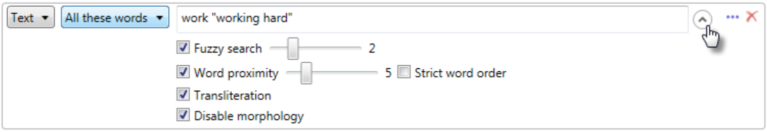

Select operation to unite conditions as: ● And ○ Or □ Not

Text ▾ | Any of these words ▾ | work "working hard"

All these words
Any of these words
Word or phrase
None of these words

[Add condit ... ck] [Wrap into block]

Besides, you can specify additional conditions of keywords search by clicking the unfold button ⌄ to the right of the text field:


Text ▾ | All these words ▾ | work "working hard"

☑ Fuzzy search 2
☑ Word proximity 5 □ Strict word order
☑ Transliteration
☑ Disable morphology

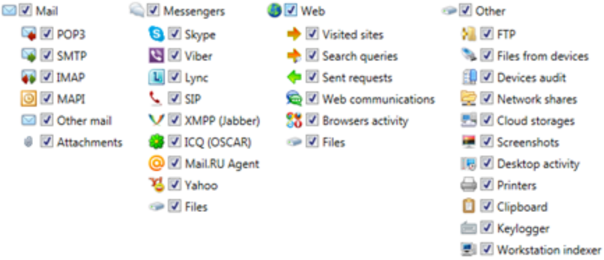
- **Fuzzy search** - search for mistyped or similar words. If this option is checked, you can set a threshold, i.e. the extent to which the words detected in the traffic flows can differ from the ones entered into the text field. It is not recommended to set a high value of this parameter when searching for short words, as it may enhance search results inaccuracy.
- **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 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 rule 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.
- **Disable morphology** – provides "exact concurrence" search. In common cases the morphology of the language is taken into account upon search processes, but in some cases it may lead to a big quantity of unexpected

results. Enabling this option may be useful if it is necessary to find target documents with original words form that were specified

Upon configuring the text search conditions the symbols "**?**" and "*****" are allowed.

Search by data types (Search in option)

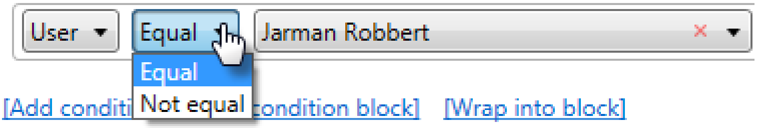
Search in the information sent or received via e-mail, instant messengers, Web (HTTP protocol), as well as sent and received files and other data types.



- ☑ Mail
  - ☑ POP3
  - ☑ SMTP
  - ☑ IMAP
  - ☑ MAPI
  - ☑ Other mail
  - ☑ Attachments
- ☑ Messengers
  - ☑ Skype
  - ☑ Viber
  - ☑ Lync
  - ☑ SIP
  - ☑ XMPP (Jabber)
  - ☑ ICQ (OSCAR)
  - ☑ Mail.RU Agent
  - ☑ Yahoo
  - ☑ Files
- ☑ Web
  - ☑ Visited sites
  - ☑ Search queries
  - ☑ Sent requests
  - ☑ Web communications
  - ☑ Browsers activity
  - ☑ Files
- ☑ Other
  - ☑ FTP
  - ☑ Files from devices
  - ☑ Devices audit
  - ☑ Network shares
  - ☑ Cloud storages
  - ☑ Screenshots
  - ☑ Desktop activity
  - ☑ Printers
  - ☑ Clipboard
  - ☑ Keylogger
  - ☑ Workstation indexer

Search by users

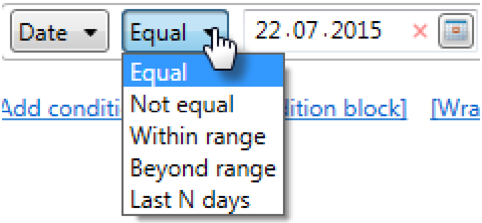
To search by user specify one of the following conditions: **Equal** (search for information transferred by the specified user) or **Not equal** (search for information transferred by all users except specified).



User ▼ Equal ▼ Jarman Robbert ✕ ▼

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 any day except the specified period) and Last N days (including the current day).



Search by time and day of week

To search by time you can specify conditions similar to search by date.

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

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**).

Document status

The system mark every intercepted document with a specific status. There are four document statuses which can be used for search:

- **Encrypted** - To search for encrypted data, select the **Encrypted** option in the menu and select the **Encrypted information detected or access to the information restricted** check box . If this option is switched on, the system will generate and send notifications every time it detects encrypted data (this could be password-protected archives, MS Word or MS excel documents, etc.). If this option is disabled, the system will only analyze unencrypted data and ignore encrypted documents;
- **Decrypted** - data transferred over SSL and which was decrypted by the agent select the **Decrypted** option;
- **Corrupted** - data which was corrupted upon transfer or initially use this option;

- **Blocked** - data which was blocked by the blocking rules due to the security policies.
- **Upper-level** - data which was transferred by itself (not as s part of a parents document) use this option.
- **Direction: received** or **sent** - data transferred in the particular direction (outgoing or incoming to user data).

To search with specified status condition select the **YES/NO** compliance parameter. If the Yes parameter is selected search results will contain only the documents with specified status.

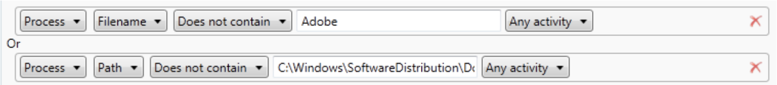
Attention! *"Blocked" status isn't attached to HTTP GET requests to access the web sites prohibited by blocking rules. The fact of prohibition web sites visit don't meet the "Blocked" status search condition and will not be displayed among the search results.*

Search by process parameters

To perform search for process by its name, application window title and execution file path select the **Process** option from the conditions type list.

While searching by executor attributes conditions **Contains**(search for process with selected attribute) or **Does not contains** (search for all process except selected attribute) may be set. Besides, the **Start** or the **Stop** of activity, both ones and **Any activity** of process with selected attributes may be detected.

Filtering search result on full network path parameter could be useful to exclude software update processes from analysis or to perform activity control for processes from one vendor.



Process ▾ Filename ▾ Does not contain ▾ Adobe Any activity ▾ ✕

Or

Process ▾ Path ▾ Does not contain ▾ C:\Windows\SoftwareDistribution\D Any activity ▾ ✕

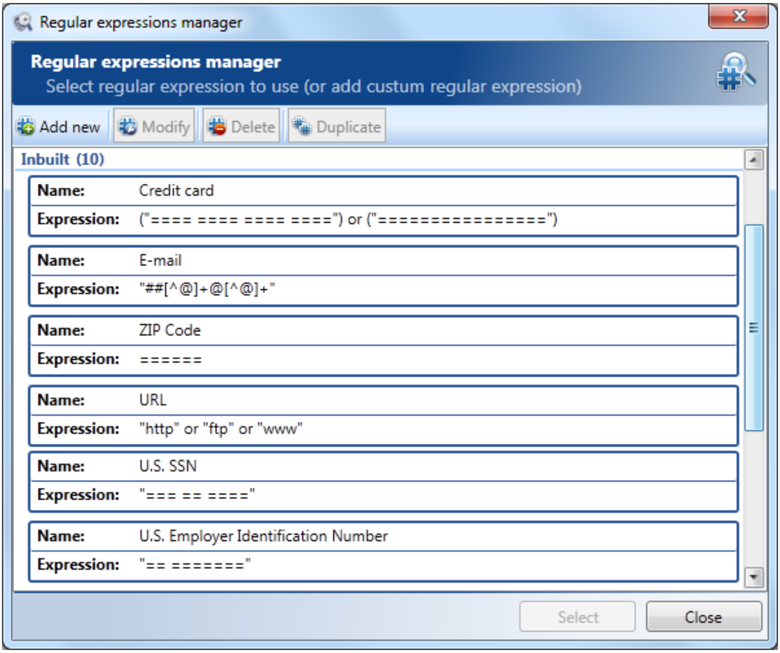
The complex condition for all processes which does not contain the "Adobe" word in executor name and processes except Windows update software are figured above.

Regular expression

Regular expression searching provides a way to search for advanced combinations of characters. Regular expressions may be used to search for certain type of documents such as credit cards, e-mail messages, zip codes, etc.

To create a rule to search by a regular expression, in the drop-down list of search conditions, select **Regular expression**, and in the text box provided enter the necessary values or select one of the available presets by clicking the Tools button ... next to the text box. Having selected the necessary regular expression, click

Select.



Regular expressions manager

Select regular expression to use (or add custum regular expression)

Inbuilt (10)

Name:	Credit card
Expression:	("==== ==== ==== ====") or ("================")
Name:	E-mail
Expression:	"##[^@]+@[^@]+"
Name:	ZIP Code
Expression:	======
Name:	URL
Expression:	"http" or "ftp" or "www"
Name:	U.S. SSN
Expression:	"=== == ===="
Name:	U.S. Employer Identification Number
Expression:	"== ======="

A regular expression included in a search request must be quoted and must begin with ##.

Examples:

```
Apple and "##199[0-9]"
```

```
Apple and "##19[0-9]+"
```

This version of the product uses TR1 regular expressions. For more information on TR1 regular expressions, for more information, see: *http://msdn.microsoft.com/en-us/library/bb982727.aspx*.

Limitations:

1. A regular expression must match a single whole word. For example, a search for "##app.*ie" would not find "apple pie".
2. Only letters are searchable. Characters that are not indexed as letters are not searchable even using regular expressions, because the index does not contain any information about them.
3. Because the index does not store information about line breaks, searches that include begining-of-line or end-of-line regular expression criteria (^ and $) will not work.

Performance:

A regular expression is like the * wildcard character in its effect on search speed: the closer to the front of a word the expression is, the more it will slow searching. "Appl.*" will be nearly as fast as "Apple", while ".*pple" will be much slower.

Searching for numbers:

Using “=”character is faster than regular expressions for matching patterns of numbers. For example, to search for a social security number, you should use "=== == ====" instead of the equivalent regular expression. Please note that in this case you do not need to begin the request with ##.

Searching by IP addresses or ports

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 the e-mail traffic

When searching in the email 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 SMTP e-mails that contain/do not contain the specified expression in fields of "MAIL From:" and "RCPT To:" protocol commands);
- **messages with attachments** (search for e-mails that include/do not include

attached files).

Search in the messengers traffic

When searching in the messengers traffic, you can set the following parameters:

- **local UIN (nick)** (search for conversations in IMs where the UIN (nick) of the local user contains/does not contain the specified expression);
- **remote UIN (nick)** (search for conversations in IMs where the UIN (nick) of the remote user contains/does not contain the specified expression);
- **local user info** (search for conversations in IMs where the additional user info fields of the local user account contain/do not contain the specified expression);
- **remote user info** (search for conversations in IMs where the additional user info fields of the remote user account contain/do not contain the specified expression);
- **conversations with files** (search for conversations in IMs where the users exchanged/did not exchange any files);
- **message count** (search for conversations in IMs containing the specified number of messages (in a range)).

Search for specific files by their names or extensions

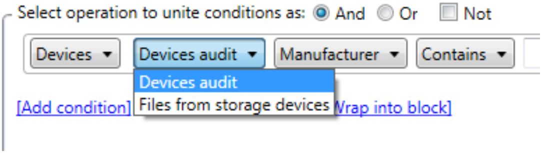
In case you choose to search for files based on their names, you can select one of the two further options – **Equal** or **Not equal** – to search for files with the specified name or any files except having the specified name (the name should be entered into the text field on the right)

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 by devices

To search on data related to devices with specific parameters use the **Devices** condition and set the type of devices control data. Two types are available for choice: **devices audit** and **intercepted from devices** data.

To search any information in the data transferred to external devices or any data about devices usage specify a devices attribute.


Select operation to unite conditions as: ● And ○ Or □ Not

To determine an attribute of external devices connected to computers on which agents are installed, go to the **SecureTower Administrator Console**.

Select the **Agents schema** tab in the **Endpoint agent control center** window and copy the necessary devices attributes (for more information, see the *Monitoring endpoint agents status chapter of the **Administrator Guide***).

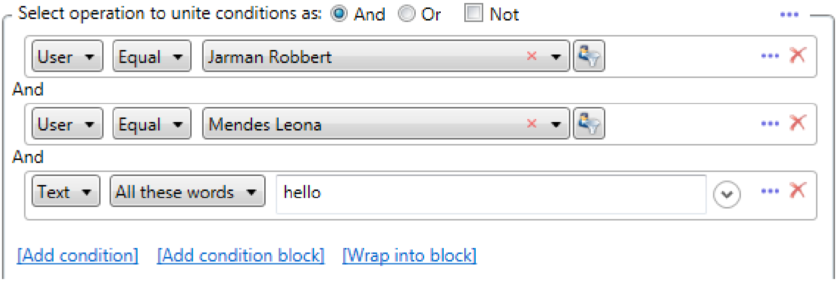
Insert from clipboard or enter the value of the selected parameter into a data entry field to complete. To receive the most relevant results set the maximum number of known parameters in search conditions.

Search conditions

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**, select the **And** radio button.
- 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, select the **OR** radio button.

***Note**: For example, upon creating several search conditions (by text, first user name and second user name), the search may be conducted either subject to all of these conditions at the same time or subject to one of the listed search conditions (in accordance with the selected "AND" or "OR" operation applied to these conditions). In the first case (see picture below), security officers will receive a notification on some chat, conversation or e-mail exchange between these two users that contains the specified text.*



Select operation to unite conditions as: ● And ○ Or □ Not

User | Equal | Jarman Robbert

And

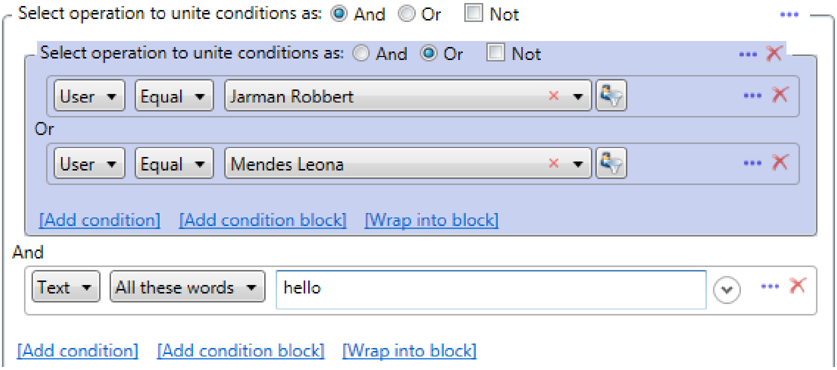
User | Equal | Mendes Leona

And

Text | All these words | hello

In the second case – they will get either any information related to the first user, or any information related to the second user, or any information that contains the specified text.

To make sure that the notification informs the security officer not only of the conversation between the specified users, but also of conversations of each of them with other users, one should create a condition and a condition block and apply both of the operations to them ("AND" and "OR"). The condition may include the searched text, and the block – the names of the first and the second users. The block conditions should be united by the "OR" operation, while the block and the condition should be united by the "AND" operation. In such a case, notifications will be sent if the program detects some information containing the specified text either for the first user or for the second user.



Select operation to unite conditions as: ● And ○ Or □ Not

Select operation to unite conditions as: ○ And ● Or □ Not

User | Equal | Jarman Robbert

Or

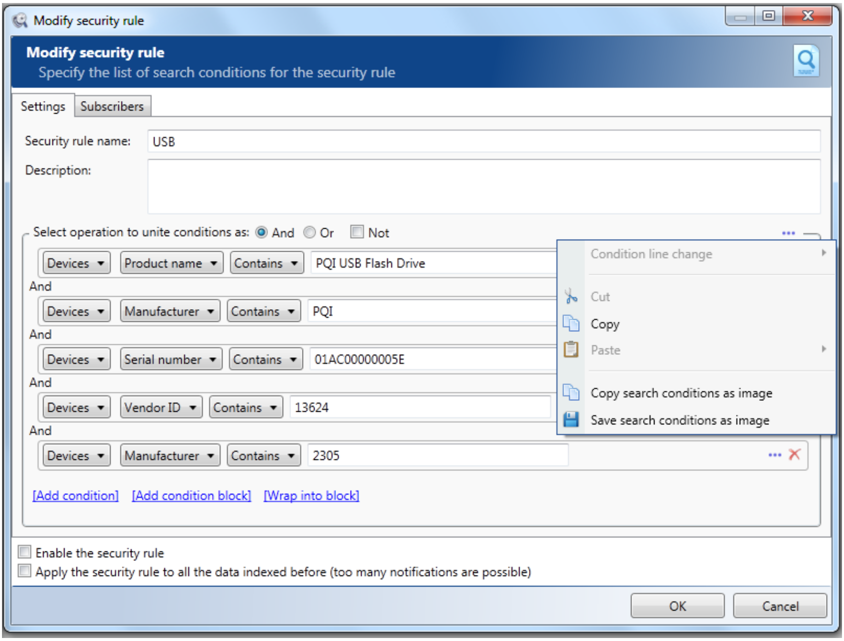
User | Equal | Mendes Leona

And

Text | All these words | hello

Advanced procedures for search conditions

To work with advanced procedures left click the **Tools** icon ••• and select a necessary one from the list.



Modify security rule

Modify security rule
Specify the list of search conditions for the security rule

Security rule name: USB

Description:

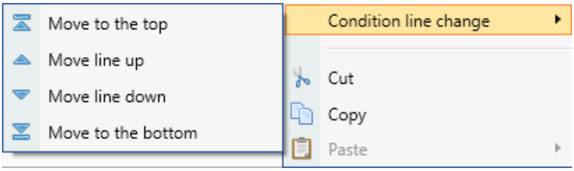
Select operation to unite conditions as: ● And ○ Or □ Not

Devices	Product name	Contains	PQI USB Flash Drive
And			
Devices	Manufacturer	Contains	PQI
And			
Devices	Serial number	Contains	01AC00000005E
And			
Devices	Vendor ID	Contains	13624
And			
Devices	Manufacturer	Contains	2305

□ Enable the security rule
□ Apply the security rule to all the data indexed before (too many notifications are possible)

Changing condition line

A search condition line or block line position can be changed within parent block.



To change the item line point to **Conditions line change**, and then click one of available actions.

Cut

Select the **Cut** procedure to remove selected item from the parent block body and copy it to clipboard as a part of the system code. After applying this operation the **Paste** procedure is available for item that was cut within any rule in the Client console.

Copy

Select the **Copy** procedure to copy selected item to clipboard as a part of the system code. After applying this operation the **Paste** procedure is available for item that was copy within any rule in the Client console.

Paste

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** .

Copy search condition as image

This procedure is useful in cases if it is necessary to provide user without SecureTower access with image of condition content.

Select the **Copy search condition as image** procedure to copy the root block of search conditions to clipboard as screenshot of block body.

This procedure is available for the root block only.

Save search condition as image

This procedure is useful in cases if it is necessary to provide user without SecureTower access with image of condition content.

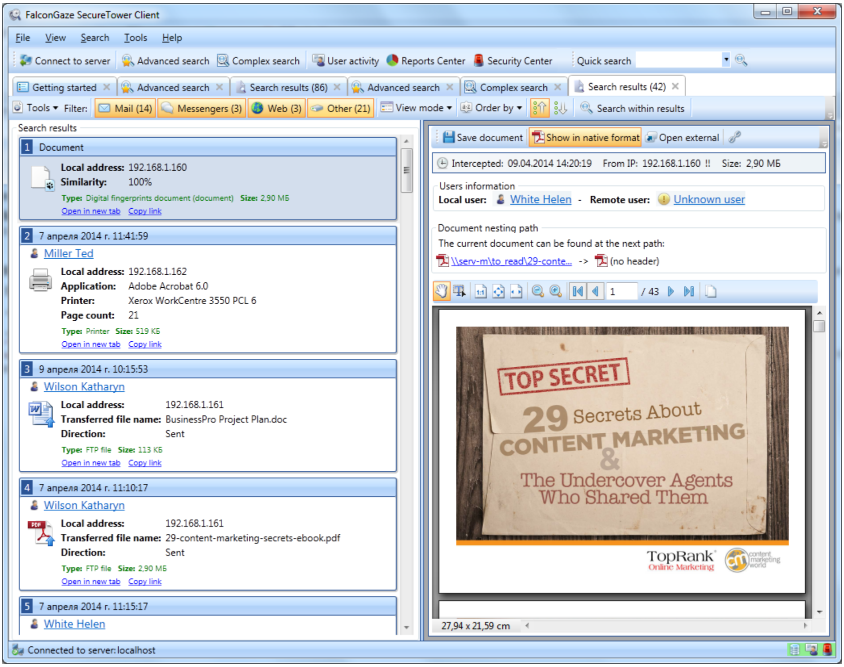
Select the **Save search condition as image** procedure to save the root block of search conditions to clipboard as .png format file with screenshot of block body. Select network path in the dialog window and click **Ok** to finish saving procedure.

This procedure is available for the root block only.

4.4.2 Operating with search request

There are several operations available from the **Complex search** window toolbar:

1. **Search with current request** - click to start search with current search conditions. The list of search results with intercepted data which correspond to the current search request will be displayed in the newly opened **Search results** window.



Search results

1 Document

Local address: 192.168.1.160
Similarity: 100%
Type: Digital fingerprints document (document) **Size:** 2,90 МБ
Open in new tab Copy link

2 7 апреля 2014 г. 11:41:59
Miller Ted
Local address: 192.168.1.162
Application: Adobe Acrobat 6.0
Printer: Xerox WorkCentre 3550 PCL 6
Page count: 21
Type: Printer **Size:** 519 КБ
Open in new tab Copy link

3 9 апреля 2014 г. 10:15:53
Wilson Katharyn
Local address: 192.168.1.161
Transferred file name: BusinessPro Project Plan.doc
Direction: Sent
Type: FTP file **Size:** 113 КБ
Open in new tab Copy link

4 7 апреля 2014 г. 11:10:17
Wilson Katharyn
Local address: 192.168.1.161
Transferred file name: 29-content-marketing-secrets-ebook.pdf
Direction: Sent
Type: FTP file **Size:** 2,90 МБ
Open in new tab Copy link

5 7 апреля 2014 г. 11:15:17
White Helen

Intercepted: 09.04.2014 14:20:19 From IP: 192.168.1.160 !! Size: 2,90 МБ

Users information
Local user: White Helen - **Remote user:** Unknown user

Document nesting path
The current document can be found at the next path:
\\serv-m\to_read\29-conte... -> (no header)

27,94 x 21,59 cm

Connected to server:localhost

2. **Show favorite** - click to display the **Favorite** list. The **Favorite** list will be displayed in the right part of the **Complex search** window (for more information, see *Favorites*).

3. **Save\Load** - click and select the one from the options:

   - Click **Load search rule** to import REQ format file with the search conditions previously saved.

   - Click **Save search rule** to save the search conditions of the currently edited request to REQ format file.

4. **Add to favorite** - click to save the current search request to the **Favorite** list. The currently edited search rule will be added to the **Favorite** list and then can be used for quick access during search request creation (for more information, see *Favorites*).

4.4.3 Favorites

The newly created rule *[can be added to the Favorite list]* and can be used for quick access during search request creation. The list contains all rule with user combined search requests which were added to Favorite.

The favorites are accessible for viewing and using during search rules creation in the **Complex search** window. To view a favorite rule structure and search performing select the necessary rule in the list and click **Open** on the Favorite area ribbon toolbar.

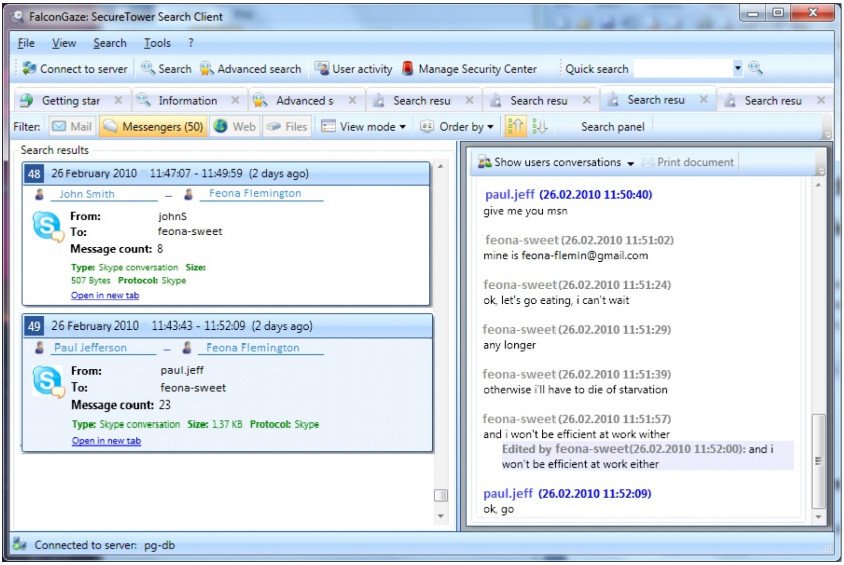
To change the name of a favorite rule select the necessary rule in the list and click **Modify** on the favorite area ribbon toolbar

To delete the search rule from the **Favorite** list select the necessary rule in the list and click **Modify** on the favorite area ribbon toolbar.

5 Viewing search results

Search results open in a separate tab and are ordered by relevance (“relevance” is the degree to which the result found matches the query). Upon a simple search, the application will provide 100 most relevant results. The advanced search allows user to obtain a larger number of results shown.

Once you switch to the **Search results** tab, you will see the results found for your search request. In the left pane of the search results window, the search results list is displayed. In the right pane of the window, a preview for the selected search result is available.



48 26 February 2010 11:47:07 - 11:49:59 (2 days ago)

John Smith – Feona Flemington

From: johnS
To: feona-sweet
Message count: 8
Type: Skype conversation **Size:** 507 Bytes **Protocol:** Skype
Open in new tab

49 26 February 2010 11:43:43 - 11:52:09 (2 days ago)

Paul Jefferson – Feona Flemington

From: paul.jeff
To: feona-sweet
Message count: 23
Type: Skype conversation **Size:** 1,37 KB **Protocol:** Skype
Open in new tab

paul.jeff (26.02.2010 11:50:40)
give me you msn

feona-sweet (26.02.2010 11:51:02)
mine is feona-flemin@gmail.com

feona-sweet (26.02.2010 11:51:24)
ok, let's go eating, i can't wait

feona-sweet (26.02.2010 11:51:29)
any longer

feona-sweet (26.02.2010 11:51:39)
otherwise i'll have to die of starvation

feona-sweet (26.02.2010 11:51:57)
and i won't be efficient at work wither
Edited by feona-sweet(26.02.2010 11:52:00): and i won't be efficient at work either

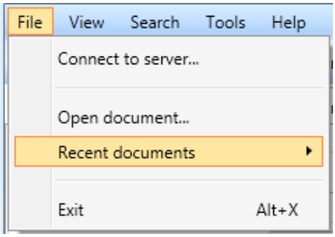
paul.jeff (26.02.2010 11:52:09)
ok, go

Connected to server: pg-db

Double click a result entry in the list to open it in the new tab.

Viewing recent documents

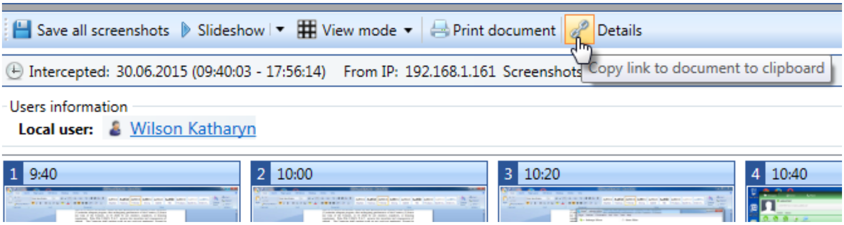
To view the recently viewed documents (mail messages, instant messages, intercepted files, etc.), on the **File** menu in the program toolbar, point to **Recent documents** and select the necessary document.



Sharing a link to a document

To share some document with other users of the security officer console, click the **Copy link** button in the right corner on the toolbar of the search results window. This action will generate the document's link which you can paste into any communication program window for others to use it.

This link is the identification of the intercepted document in internal **SecureTower** format, for example, `fgst://PG59|e20915ab-dc80-4d61-84a2-1c863330bedf|dc4fa057-f1d4-44fa-ab6d-28a898be34cd/-1062731486/S-1-5-21-2369683944-1213016059-2822112797-2876/2a983ce9-e706-45c4-83fc-3b3e06d02c7a/`.



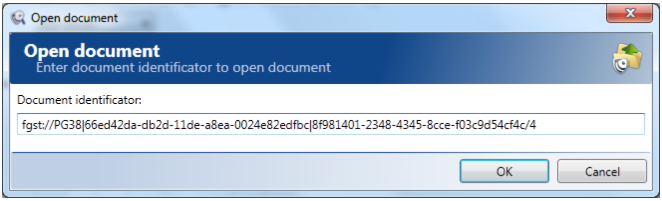
Intercepted: 30.06.2015 (09:40:03 - 17:56:14) From IP: 192.168.1.161 Screenshots

Local user: Wilson Katharyn

This kind of links can be used to facilitate subsequent search of the document in **SecureTower** database

Viewing a link to a document

To open the document the link to which another console user has provided to you, go to the **File** menu on the program toolbar and click **Open document**. Copy the link to the clipboard, paste it into the text box of the **Open document** window and click **OK.**



Open document
Enter document identificator to open document

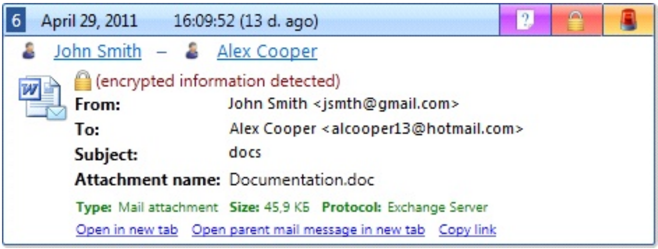
Document identificator:
fgst://PG38|66ed42da-db2d-11de-a8ea-0024e82edfbc|8f981401-2348-4345-8cce-f03c9d54cf4c/4

User interface navigation tips

If the client console window is collapsed, some items on toolbar can be hidden. In this case click the "**More Tools**" icon ⋮ on the toolbar to access hidden elements.

5.1 Search results list

Sometimes the headers of the search results entry in the results list may contain additional symbols.



6 April 29, 2011 16:09:52 (13 d. ago)

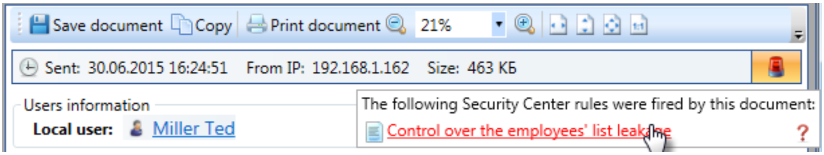
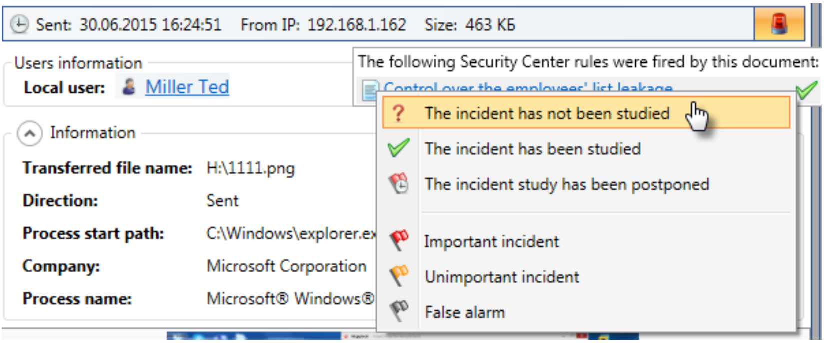
John Smith – Alex Cooper

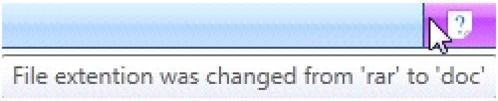
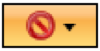
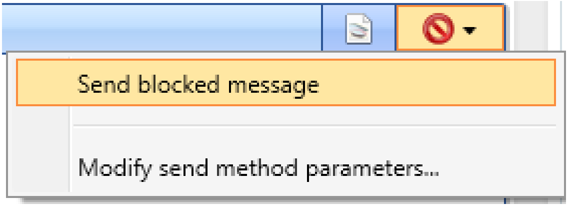
(encrypted information detected)

From: John Smith <jsmth@gmail.com>
To: Alex Cooper <alcooper13@hotmail.com>
Subject: docs
Attachment name: Documentation.doc

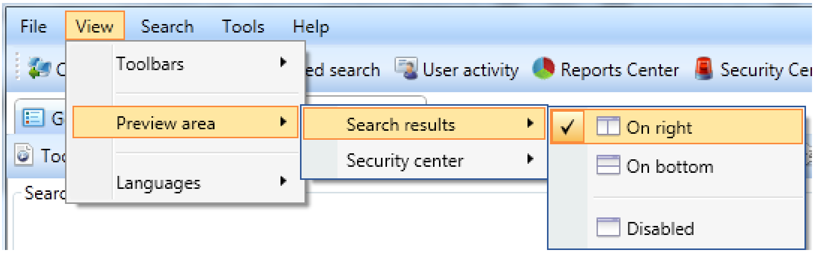
Type: Mail attachment Size: 45,9 КБ Protocol: Exchange Server

Symbol	Meaning
🚨	This symbol means that the transferring this document triggered a security rule. Move the cursor over the symbol to see a pop-up hint with the name of the rule triggered and the incident status in the Security Center.

Symbol	Meaning
	 Sent: 30.06.2015 16:24:51 From IP: 192.168.1.162 Size: 463 КБ Users information Local user: Miller Ted The following Security Center rules were fired by this document: Control over the employees' list leakage Click the security rule name to see all incidents triggering this rule. The Security Center window will be opened in the new tab with all incidents triggered this rule. Hover over the incident status icon to change it: - Left-click the icon for quick choice. Repeat the action until the necessary status will not be set. - Right-click the icon and click the necessary status option on the context menu. Sent: 30.06.2015 16:24:51 From IP: 192.168.1.162 Size: 463 КБ Users information Local user: Miller Ted The following Security Center rules were fired by this document: Control over the employees' list leakage Information Transferred file name: H:\1111.png Direction: Sent Process start path: C:\Windows\explorer.ex Company: Microsoft Corporation Process name: Microsoft® Windows® ? The incident has not been studied ✓ The incident has been studied The incident study has been postponed Important incident Unimportant incident False alarm See also: *Security notifications review*.
🔒	This symbol means that encrypted information has been detected in the transferred data. This may be a password-protected archive, MS Word or MS Excel document, etc. In case the file names in the password-protected archive were not encrypted, they will be displayed in the right part of the window.
?	This symbol means that the extension of the transferred file has been changed. In this case, the information about the original file format will be displayed in the right part of the window.

Symbol	Meaning
	 File extention was changed from 'rar' to 'doc' Move the cursor over this symbol to see a pop up tip indicating the original and new file extension.
	This symbol means that information inclosed in transferred data is prohibited for transfer by blocking rule. In this case, the information about the triggered blocking rule will be displayed in the right part of the window. Move the cursor over this symbol to see a pop up tip indicating the rule name. Click the block symbol to open the list of operations that available for this document.  To send blocked message it is necessary to configure send method parameters. To configure send method parameters, chose a necessary one from the list and proceed as described in *Configuring security notifications delivery*. When configuration is done, select the **Send blocked message** check box to permit transfer of this document.

You can always disable or change the location of the search preview tab. To do this on the **View** menu, point to **Preview area**, and select the necessary command.



Save and export procedure

Search results can be saved to external file - on the **Search results** toolbar click the **Tools** menu. Select one of the available way to save the results.

- Click **Export results list** to save list of results to the single file. The file format can be set directly from the Save dialog window: Microsoft Excel (XLS and XLSX) with or without icon storing, CSV, XML. The results list will be stored in table form with headers and attributes.
- Click **Save all results** to save all results (corresponding documents) as single separate files organized in the folder.

Note 1*: CSV or "XLS(X) without icon" formats are highly recommended if the number of results is significant .*

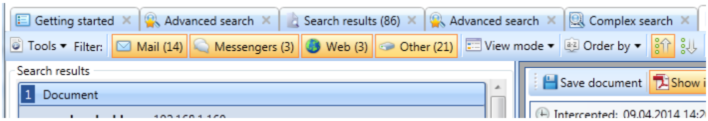
Note 2*: Plugins emails, PC activity, printed documents and screenshots are available for save mode configuring. Other type of results will be saved in there initial format.*

Updating search results

While the results are inspecting, their relevance may become out of date due to the database updates. To view the most relevant results on the **Tools** menu click **Update search results**.

5.1.1 Sorting a search results list

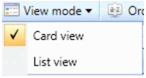
On the Search results window toolbar, you will see various filters by which you can sort the provided search results: by data types (e-mail, instant messages, web, files). The toolbar is context-sensitive, automatically displaying the functions relevant to what you are doing at the moment. Functions that cannot be used in the current context are dimmed.

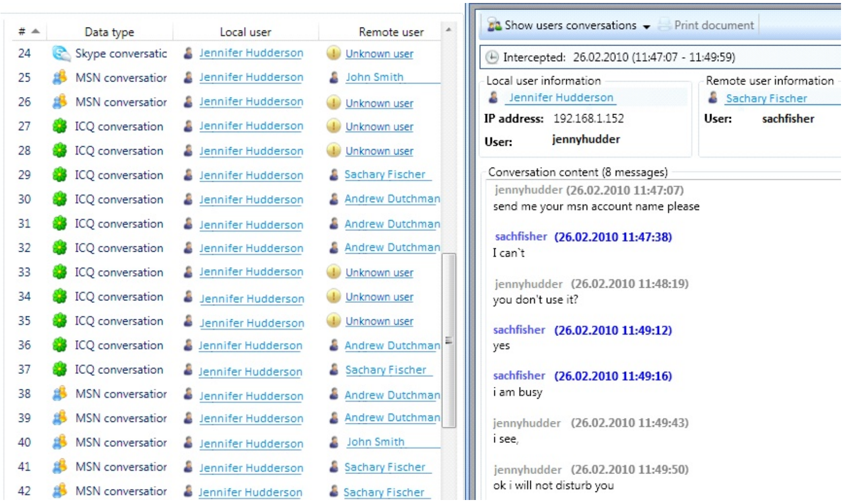


Quick tips:

- To refine your search results, you can exclude certain results from being displayed by clicking the buttons responsible for displaying the corresponding types of data. For example, if you want to see instant messenger conversations only, you can deselect the **Mail**, **Web** and **Others** buttons . You can always return the rest of the results by clicking those buttons again

- To change the view mode, click **View mode** and then click the necessary mode. Search results may be presented in a list (as shown below) or in a card view mode.





#	Data type	Local user	Remote user
24	Skype conversatic	Jennifer Hudderson	Unknown user
25	MSN conversatior	Jennifer Hudderson	John Smith
26	MSN conversatior	Jennifer Hudderson	Unknown user
27	ICQ conversation	Jennifer Hudderson	Unknown user
28	ICQ conversation	Jennifer Hudderson	Unknown user
29	ICQ conversation	Jennifer Hudderson	Sachary Fischer
30	ICQ conversation	Jennifer Hudderson	Andrew Dutchman
31	ICQ conversation	Jennifer Hudderson	Andrew Dutchman
32	ICQ conversation	Jennifer Hudderson	Andrew Dutchman
33	ICQ conversation	Jennifer Hudderson	Unknown user
34	ICQ conversation	Jennifer Hudderson	Unknown user
35	ICQ conversation	Jennifer Hudderson	Unknown user
36	ICQ conversation	Jennifer Hudderson	Andrew Dutchman
37	ICQ conversation	Jennifer Hudderson	Sachary Fischer
38	MSN conversatior	Jennifer Hudderson	Andrew Dutchman
39	MSN conversatior	Jennifer Hudderson	Andrew Dutchman
40	MSN conversatior	Jennifer Hudderson	John Smith
41	MSN conversatior	Jennifer Hudderson	Sachary Fischer
42	MSN conversatior	Jennifer Hudderson	Sachary Fischer

Intercepted: 26.02.2010 (11:47:07 - 11:49:59)

Local user information
Jennifer Hudderson
IP address: 192.168.1.152
User: jennyhudder

Remote user information
Sachary Fischer
User: sachfisher

Conversation content (8 messages)

jennyhudder (26.02.2010 11:47:07)
send me your msn account name please

sachfisher (26.02.2010 11:47:38)
I can`t

jennyhudder (26.02.2010 11:48:19)
you don't use it?

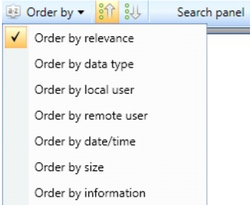
sachfisher (26.02.2010 11:49:12)
yes

sachfisher (26.02.2010 11:49:16)
i am busy

jennyhudder (26.02.2010 11:49:43)
i see,

jennyhudder (26.02.2010 11:49:50)
ok i will not disturb you

- To order the search results by any parameter, click **Order by** and click the necessary parameter on the submenu. You can also have them presented in a ascending or descending order by clicking the **Ascending sort** button ⇧ or the **Descending sort** button ⇩.


Order by ▾ ⇧ ⇩ Search panel

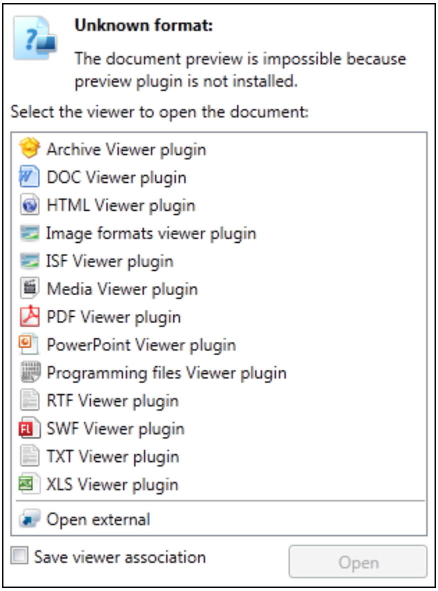
✓ Order by relevance
Order by data type
Order by local user
Order by remote user
Order by date/time
Order by size
Order by information

5.2 Viewing various data type

The program enables inspection of all the intercepted documents without necessity to open them with external applications. For example, a PDF document may be displayed both in the program and with the Adobe Acrobat Reader application. An archive can also be viewed inside of the program or opened in an external application.

The program chooses the most appropriate view mode for each document format to avoid having to view documents with external applications. For example, e-mails are displayed with all the main attributes (subject, to, etc.), message body and the list of attachments.

If the program doesn't recognize the format of the document found, it will prompt the user to select one of the built-in plugins of applications intended for viewing this document formats.


Unknown format:

The document preview is impossible because preview plugin is not installed.

Select the viewer to open the document:

Archive Viewer plugin
DOC Viewer plugin
HTML Viewer plugin
Image formats viewer plugin
ISF Viewer plugin
Media Viewer plugin
PDF Viewer plugin
PowerPoint Viewer plugin
Programming files Viewer plugin
RTF Viewer plugin
SWF Viewer plugin
TXT Viewer plugin
XLS Viewer plugin

Open external

□ Save viewer association

Open

To associate selected plug-in with specified files extension, select the **Save viewer**

association check box. You can modify the plug-in settings, as well as add new extension associations in the **Customize program options** window (**Tools – Options...**).

The search list can include both the complicated format documents (an e-mail, a chat history, etc.) and the simple ones (such as files attached to an e-mail or transferred over ICQ). The program provides different functions for each type of documents. For example, upon viewing a file found, one can switch to viewing the e-mail message it was attached to.

See also: *Quick tips for results viewing*.

For the certain type of data the viewer provides a panel with set of context-sensitive tools listed below.

Viewer instrument panel provides the following command:	
✋	"Hand" tool to navigate through the document;
T	Select tool for text selection;
1:1 ⊡ ↔	View size buttons: - view in actual size; - fit whole page into window; - fit page into window by width;
⊖ ⊕	View size buttons for accurate adjustment of page size for viewing;
⏮ ◀ 1 / 1 ▶ ⏭	Indication of current page and number of pages in the document with navigation buttons to jump to first/previous/next/last page;
🗋	Page thumbnails button to display thumbnails of all pages in the left part of the viewer window.

5.2.1 Web-traffic data (HTTP) viewing

Web-traffic may contain queries sent to a remote web-server over HTTP or visited URLs. Network users can not just visit and view internet pages, but also post some information in the visited web-resource. For example, they can add data in social networks, send messages in forums, blogs, or upload files, documents, archives, etc.

There are following HTTP traffic types:

- **Visited web-addresses** (URLs) in internet (HTTP)
- **Requests or data sent** to a remote web-server (HTTP POST): For example, sent text

messages in social networks, blogs, forums, submitted search requests.

- **Files uploaded** to a remote web-server (HTTP POST file): For example, files (photos, pictures, text documents, archives, etc.) uploaded to a user page in a social network, forum, blog.

Note*: If the blocking rule was triggered by HTTP(S) data transferring the search result will be marked with the blocking symbol* 🚫▾ *(* for more information, see *Data blocking chapter of the Administrator Guide and the Viewing notifications in Security Center chapter of this guide.*

Visited URLs (HTTP)

In the web-traffic data window, you will see an information block with the date and time of data interception, **local user** and a window with the list of **visited URLs**. There is a date and time of an URL visit provided in front of each URL. You can follow any of the links in this list in order to view the content of the visited resource. For each user in search results in the left pane of the program window, a preview of all the visited links is available in the right pane of the program window.

Saving	To save the list of visited URLs, click **Save** on the preview area toolbar. In the save dialogue window, specify the folder where you want to save the list of visited URL, and click **Save**. The document will be saved in the HTML format.
Printing	To print the search results click **Print** on the preview area toolbar.
Grouping by domain	To group the search results by domain name click the **Group** button on the preview area toolbar.
Link to the document	To copy a particular URL hover over it in the list of visited URLs and left-click. On the appeared context menu, click **Copy**. To copy all the URLs displayed in the list click **Copy all** on the context menu.

Data sent to a web-server (HTTP POST)

In the HTTP POST data window, you will see information blocks with the date and time of data interception, **local user**, data sent (the address of the remote web-server to which the data were uploaded, their format, size, transfer date, etc.) and the data content window.

Viewing	The content of the sent data and request parameters to a remote web-server are available in the **Content** area.
Saving	To save the content of the sent request, click **Save** on the preview area toolbar. In the save dialogue window, specify the folder where you want to save the list of visited URL, and click **Save**. The document will be saved in the XML format.
HTTP header viewing	To open HTTP POST header data click **Show HTTP-header** on the preview area toolbar. The header data will be opened in the new window.
Link to the document	To copy a particular URL hover over it in the list of visited URLs and left-click. On the appeared context menu, click **Copy**. To copy all the URLs displayed in the list click **Copy all** on the context menu.

Files uploaded to a web-server (HTTP POST file)

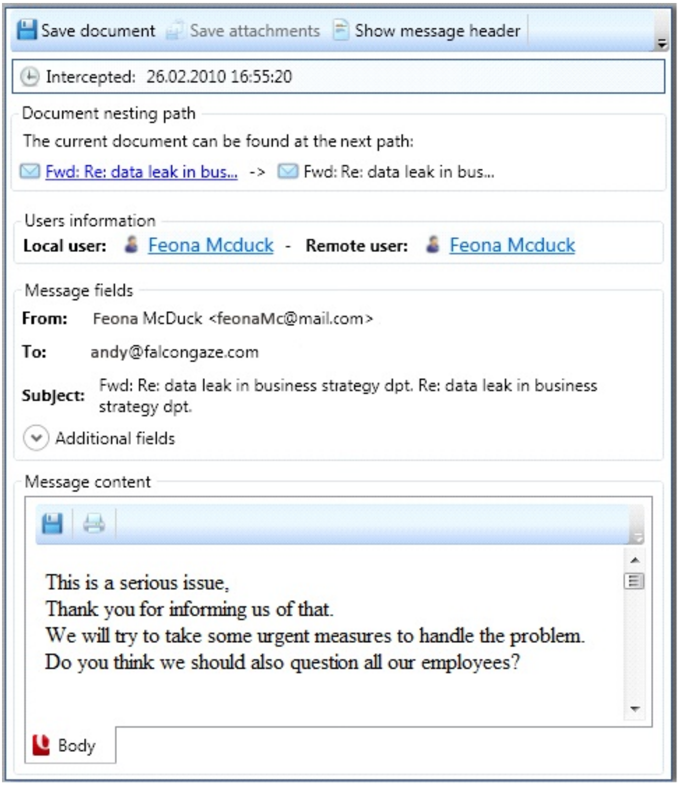
In the HTTP POST file window, you will see information blocks with the date and time of data interception, **local user**, data nesting path and the data content window. In this case, the remote user is represented by a web-server to which the file found was uploaded. If you click the link provided in the data nesting path, you will see the details of the request to a remote web-server (the address of the server, data format, size, transfer date, etc.).

Viewing	The content of the data sent and request parameters are available in the **Content** window. To view the search content with another program, click **Open external** on the toolbar of the search result window. The document will be opened in the application intended for processing this file format.
Saving	To save the file, click **Save** on the toolbar of the search result window. In the save dialogue window, specify the folder where you want to save the list of visited URL, and click **Save**. The document will be saved in the format in which it was transferred.

5.2.2 Viewing e-mails (POP3, IMAP, SMTP, MAPI)

In the e-mail data window, you will see information blocks with the date and time of data interception, local and remote users, main mail attributes (to, from, subject), additional fields and the message content window.

***Note**: Messages transferred over SMTP and activated any blocking rule will be marked with block icon . For more information*, see ***Data blocking** of the Administrator Guide and Viewing notifications in Security Center in this Guide.*



Intercepted: 26.02.2010 16:55:20

Document nesting path

The current document can be found at the next path:

Fwd: Re: data leak in bus... -> Fwd: Re: data leak in bus...

Users information

Local user: Feona Mcduck - **Remote user:** Feona Mcduck

Message fields

From: Feona McDuck <feonaMc@mail.com>

To: andy@falcongaze.com

Subject: Fwd: Re: data leak in business strategy dpt. Re: data leak in business strategy dpt.

Additional fields

Message content

This is a serious issue,
Thank you for informing us of that.
We will try to take some urgent measures to handle the problem.
Do you think we should also question all our employees?

Viewing e-mail information:

To view the message header, click **Show message header** on the preview area toolbar. The message header text will open in a new window.

To view the session parameters (protocol, local and remote ports, local IP address, incoming/outgoing server, etc.), expand the **Additional fields**. To hide these parameters, collapse the field.

To view the mail message content with another program, click **Open external** on the preview area toolbar of the search result window. The mail message will be opened in the application intended for processing the MSG file format (Microsoft Outlook, Thunderbird, etc.).

Viewing e-mail content:

Viewing e-mail content is available in the **Message content** window, the **Body** tab.

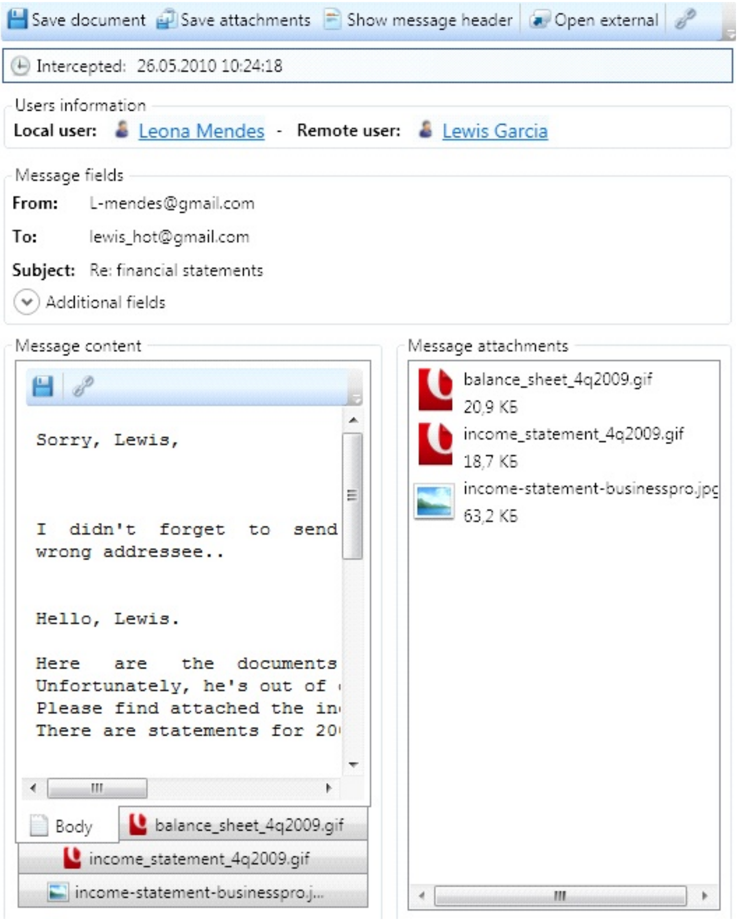
Viewing e-mail attachments :

If there are any e-mail attachments, the corresponding tabs are displayed at the bottom of the **Message content** window. By switching between these tabs, you can view the desired attachment or file. The list of e-mail attachments is also displayed in the right part of the e-mail data window in the **Message attachments** window. All the functions described below are available in the context menu opened by right-clicking one of the attachments in this window.

To open the attachment with a specialized application, click **View document in native format viewer** on the toolbar of the **Message content** window. This document will open in the search result window.

To view the attachment in a new tab, click **Open in a new tab** on the toolbar of the **Message content** window.

To view the attachment with another program, click **Open external** on the toolbar of the **Message content** window. The attachment will be opened in the application intended for processing this file format.



Intercepted: 26.05.2010 10:24:18

Local user: Leona Mendes - **Remote user:** Lewis Garcia

From: L-mendes@gmail.com

To: lewis_hot@gmail.com

Subject: Re: financial statements

```
Sorry, Lewis,


I didn't forget to send
wrong addressee..


Hello, Lewis.

Here are the documents
Unfortunately, he's out of
Please find attached the in
There are statements for 20
```

balance_sheet_4q2009.gif
20,9 КБ

income_statement_4q2009.gif
18,7 КБ

income-statement-businesspro.jpg
63,2 КБ

Saving an e-mail message:

To save an e-mail message with all its attachments, click **Save** on the preview area toolbar. In the save dialogue window, specify the folder where you want to save the e-mail message, and click **Save**. The document can be saved in selected format : HTML, MS Outlook (*msg) or its initial format.

To save the message body of the intercepted message, click **Save document to file** 💾 on the preview area toolbar of the **Message content** window. In the save dialogue window, specify the folder where you want to save the e-mail message, and click **Save**. The document can be saved in one of the listed format: HTML, MS Outlook, TXT as well as in its initial format.

Saving e-mail attachments:

To save *the content of all the mail attachments*, click **Save attachments** on the preview area toolbar. In the save dialogue window, specify the folder where you want to save the e-mail message, and click **Save**. Each attachment will be saved in the format it was transferred.

To save a *certain attachment*:

- select this attachment by opening the tab with its name in the **Message content** area, and click **Save document to file** on the toolbar of the **Message content** area

OR

- right-click the corresponding attachment in the **Message attachments** area and click **Save file as** on the context menu. In the save dialogue window, specify the folder where you want to save the e-mail message, and click **Save**. The attachment will be saved in the format it was transferred.

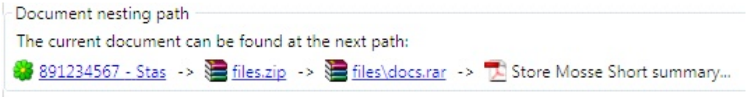
5.2.3 Viewing complex data formats (attachments, archives, files)

The program enables interception and viewing mail attachments that contain complex data formats. Complex format information represents documents that include data of other formats (for example, an e-mail message may be a reply to another e-mail message that, in its turn, contains an archive with files of various formats, etc.). Thus, a chain of various nesting levels of documents is formed, and the program intercepts, processes and enables viewing each of the documents included into this chain. For example, upon viewing an e-mail message found that is a reply to another e-mail message, one can switch to viewing the latter, including all its attachments, archives and their content.

Note*: The program enables identification of password-protected archives and other documents (including MS Word, MS Excel files, etc.). In this case the information about an intercepted document will contain a special symbol* 🚨*. The program enables viewing the list of files in a password-protected archive if the file names are not encrypted.*

In the complex format data window, you will see information blocks with the date and time of data interception, data nesting levels, local and remote users and the document content window.

The remote user may be represented by a server.



Document nesting path

The current document can be found at the next path:

891234567 - Stas -> files.zip -> files\docs.rar -> Store Mosse Short summary...

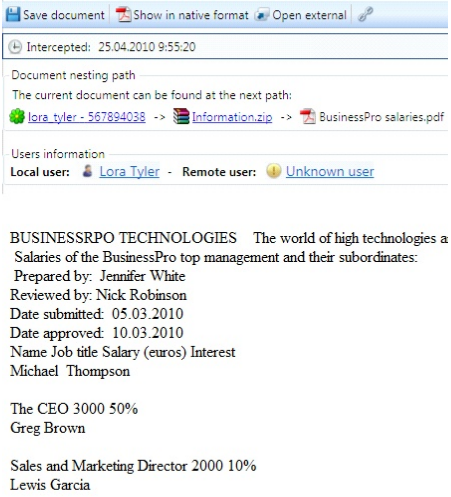
Viewing files

The content of the found document the format of which is recognized by the program is

]

displayed in the search result window.

***Note**: The program identifies file format based on its content, but not extension. Therefore, in case of deliberate file extension change by user, the program will identify the original file format.*



Intercepted: 25.04.2010 9:55:20

Document nesting path

The current document can be found at the next path:

lora_tyler - 567894038 -> Information.zip -> BusinessPro salaries.pdf

Users information

Local user: Lora Tyler - **Remote user:** Unknown user

BUSINESSRPO TECHNOLOGIES The world of high technologies a

Salaries of the BusinessPro top management and their subordinates:

Prepared by: Jennifer White

Reviewed by: Nick Robinson

Date submitted: 05.03.2010

Date approved: 10.03.2010

Name Job title Salary (euros) Interest

Michael Thompson

The CEO 3000 50%

Greg Brown

Sales and Marketing Director 2000 10%

Lewis Garcia

To view the document with another program, click **Open external** on the preview area toolbar. The document will be opened in the application intended for processing this file format.

Viewing archives

Upon viewing archives, the list of files contained in this archive will be provided. Such files are also available for viewing. For this, double-click the corresponding document with a mouse.

In case the archive is password-protected, a special symbol 🔒 will be displayed. If the file names in the archive are not encrypted, the file list will be displayed.

Viewing files of other nesting levels

In the data nesting levels information box, you can view the location of the document found in the chain of files of different nesting level and format (for example, you can see an e-mail message in which the document was found; the archive that contains the file found, etc.).

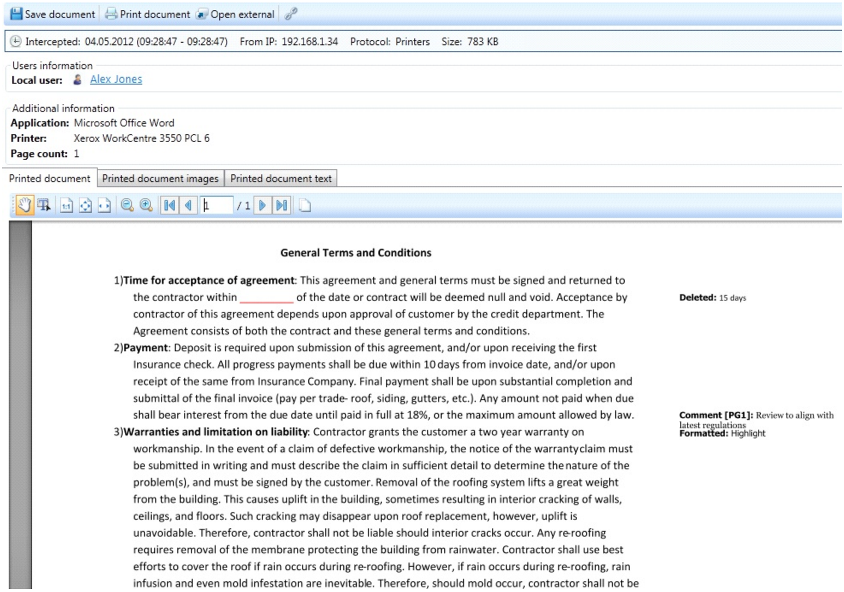
You can switch to viewing any of the documents by clicking the corresponding link in the chain of data nesting levels (see the *Data nesting levels* window).

Saving

To save the content of the document, click **Save** on the preview area toolbar. In the save dialogue window, specify the folder where you want to save the e-mail message, and click **Save**. Each attachment will be saved in the format it was transferred.

5.2.4 Viewing printed files

SecureTower system enables intercepting documents sent to local and network printers. Intercepted documents are stored in the database and displayed to the user in PDF format as text and/or graphic.



Intercepted: 04.05.2012 (09:28:47 - 09:28:47) From IP: 192.168.1.34 Protocol: Printers Size: 783 KB

Users information
Local user: Alex Jones

Additional information
Application: Microsoft Office Word
Printer: Xerox WorkCentre 3550 PCL 6
Page count: 1

General Terms and Conditions

1)**Time for acceptance of agreement**: This agreement and general terms must be signed and returned to the contractor within ________ of the date or contract will be deemed null and void. Acceptance by contractor of this agreement depends upon approval of customer by the credit department. The Agreement consists of both the contract and these general terms and conditions.

2)**Payment**: Deposit is required upon submission of this agreement, and/or upon receiving the first Insurance check. All progress payments shall be due within 10 days from invoice date, and/or upon receipt of the same from Insurance Company. Final payment shall be upon substantial completion and submittal of the final invoice (pay per trade- roof, siding, gutters, etc.). Any amount not paid when due shall bear interest from the due date until paid in full at 18%, or the maximum amount allowed by law.

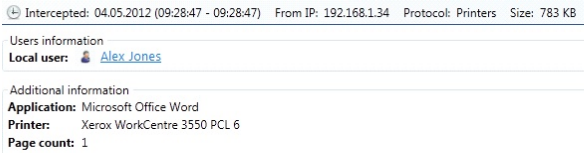
3)**Warranties and limitation on liability**: Contractor grants the customer a two year warranty on workmanship. In the event of a claim of defective workmanship, the notice of the warrantyclaim must be submitted in writing and must describe the claim in sufficient detail to determine thenature of the problem(s), and must be signed by the customer. Removal of the roofing system lifts a great weight from the building. This causes uplift in the building, sometimes resulting in interior cracking of walls, ceilings, and floors. Such cracking may disappear upon roof replacement, however, uplift is unavoidable. Therefore, contractor shall not be liable should interior cracks occur. Any re-roofing requires removal of the membrane protecting the building from rainwater. Contractor shall use best efforts to cover the roof if rain occurs during re-roofing. However, if rain occurs during re-roofing, rain infusion and even mold infestation are inevitable. Therefore, should mold occur, contractor shall not be

Deleted: 15 days

Comment [PG1]: Review to align with latest regulations
Formatted: Highlight

Command available for a printed document on the preview area toolbar:

- **Save** (saving intercepted document locally into a PDF file and as HTML for printed document text);
- **Print** (sending intercepted document for printing directly from **SecureTower** user interface);
- **Open external** (opening intercepted document in a PDF viewing application);
- The **Copy link** button for copying a link to intercepted document to clipboard (for more information, see *Viewing search results*).



Intercepted: 04.05.2012 (09:28:47 - 09:28:47) From IP: 192.168.1.34 Protocol: Printers Size: 783 KB

Users information

Local user: Alex Jones

Additional information

Application: Microsoft Office Word

Printer: Xerox WorkCentre 3550 PCL 6

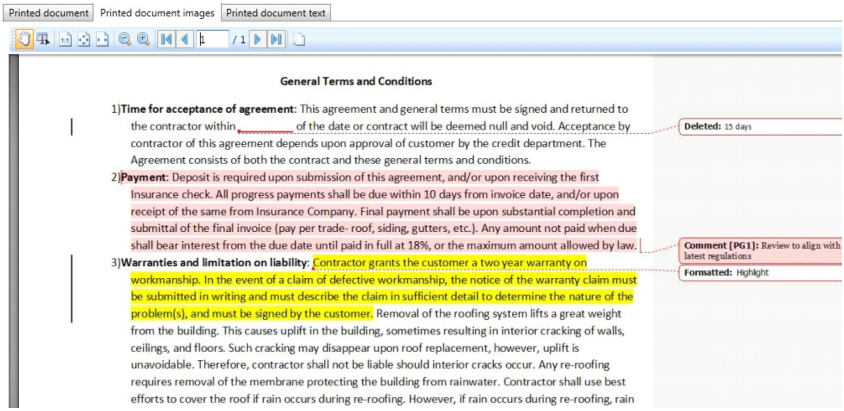
Page count: 1

Details of intercepted documents include:

- date and time of interception;
- IP address of the sender
- protocol this document was intercepted over (in this case – Printers);
- size of the document;
- application the document was sent from;
- printer the document was sent to;
- number of pages.

Subject to the format of the document, the application it was sent from, the printer and other factors, the intercepted document can be available for display as text and/or graphic.

Printed document tab displays intercepted information as text formatted as the original.



General Terms and Conditions

1)**Time for acceptance of agreement**: This agreement and general terms must be signed and returned to the contractor within ____ of the date or contract will be deemed null and void. Acceptance by contractor of this agreement depends upon approval of customer by the credit department. The Agreement consists of both the contract and these general terms and conditions.

2)**Payment**: Deposit is required upon submission of this agreement, and/or upon receiving the first Insurance check. All progress payments shall be due within 10 days from invoice date, and/or upon receipt of the same from Insurance Company. Final payment shall be upon substantial completion and submittal of the final invoice (pay per trade- roof, siding, gutters, etc.). Any amount not paid when due shall bear interest from the due date until paid in full at 18%, or the maximum amount allowed by law.

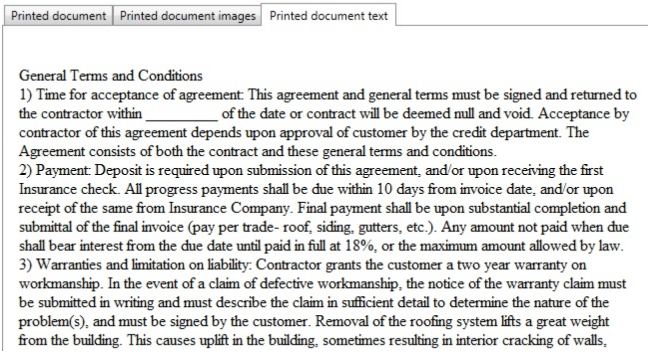
3)**Warranties and limitation on liability**: Contractor grants the customer a two year warranty on workmanship. In the event of a claim of defective workmanship, the notice of the warranty claim must be submitted in writing and must describe the claim in sufficient detail to determine the nature of the problem(s), and must be signed by the customer. Removal of the roofing system lifts a great weight from the building. This causes uplift in the building, sometimes resulting in interior cracking of walls, ceilings, and floors. Such cracking may disappear upon roof replacement, however, uplift is unavoidable. Therefore, contractor shall not be liable should interior cracks occur. Any re-roofing requires removal of the membrane protecting the building from rainwater. Contractor shall use best efforts to cover the roof if rain occurs during re-roofing. However, if rain occurs during re-roofing, rain

Deleted: 15 days

Comment [PG1]: Review to align with latest regulations

Formatted: Highlight

Printed document images tab displays intercepted information in graphic format (as images).



General Terms and Conditions
1) Time for acceptance of agreement: This agreement and general terms must be signed and returned to the contractor within __________ of the date or contract will be deemed null and void. Acceptance by contractor of this agreement depends upon approval of customer by the credit department. The Agreement consists of both the contract and these general terms and conditions.
2) Payment: Deposit is required upon submission of this agreement, and/or upon receiving the first Insurance check. All progress payments shall be due within 10 days from invoice date, and/or upon receipt of the same from Insurance Company. Final payment shall be upon substantial completion and submittal of the final invoice (pay per trade- roof, siding, gutters, etc.). Any amount not paid when due shall bear interest from the due date until paid in full at 18%, or the maximum amount allowed by law.
3) Warranties and limitation on liability: Contractor grants the customer a two year warranty on workmanship. In the event of a claim of defective workmanship, the notice of the warranty claim must be submitted in writing and must describe the claim in sufficient detail to determine the nature of the problem(s), and must be signed by the customer. Removal of the roofing system lifts a great weight from the building. This causes uplift in the building, sometimes resulting in interior cracking of walls,

Printed document text tab displays intercepted information as simple unformatted text.

5.2.5 Viewing conversations in IMs (OSCAR, Viber, Jabber, Skype, SIP, Lync)

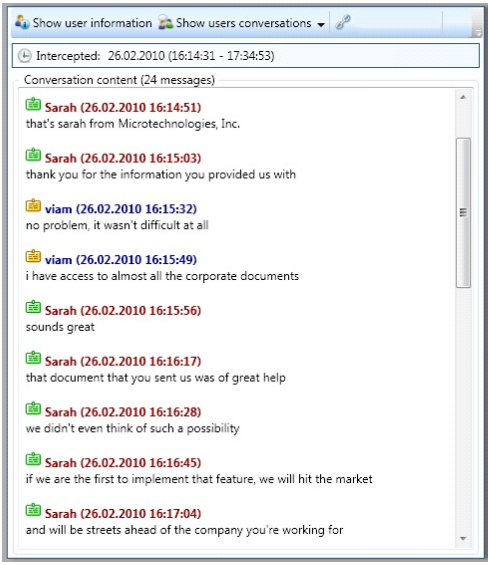
The program can intercept messages and data exchanged in instant messengers, including files transferred with the help of these programs, sender and receiver information (user accounts, UINs, avatars, contact information), conversation time, etc.

Upon viewing a conversation between certain users, one can switch to viewing all the conversations between these users for the specified period of time or all the conversations of one of these users in the current instant messenger program.

In the IM conversation window, you will see information blocks with the date and time interval of the intercepted conversation, local and remote users (user names, ICQ UINs, accounts, contact information, IP addresses, avatars, etc.) and the conversation content window.

Viewing conversations

The conversation can be viewed in the **Conversation content** area.



Intercepted: 26.02.2010 (16:14:31 - 17:34:53)

Conversation content (24 messages)

Sarah (26.02.2010 16:14:51)
that's sarah from Microtechnologies, Inc.

Sarah (26.02.2010 16:15:03)
thank you for the information you provided us with

viam (26.02.2010 16:15:32)
no problem, it wasn't difficult at all

viam (26.02.2010 16:15:49)
i have access to almost all the corporate documents

Sarah (26.02.2010 16:15:56)
sounds great

Sarah (26.02.2010 16:16:17)
that document that you sent us was of great help

Sarah (26.02.2010 16:16:28)
we didn't even think of such a possibility

Sarah (26.02.2010 16:16:45)
if we are the first to implement that feature, we will hit the market

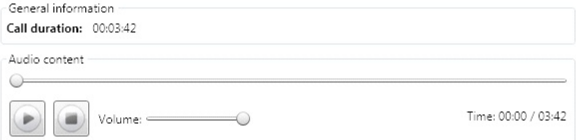
Sarah (26.02.2010 16:17:04)
and will be streets ahead of the company you're working for

Viewing SMS sent from Skype

An SMS text is available in the **Content** area. The remote user information will include a mobile phone number to which the message was sent.

Listening to a Skype voice call to a Skype user

A voice call record can be played in the **Audio content** area. The **General information** area displays the duration of the call.


General information

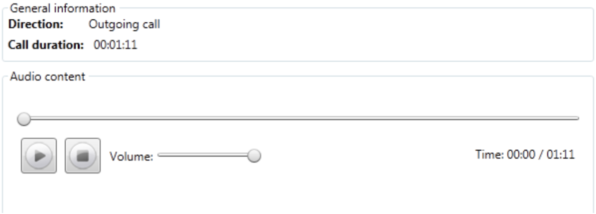
Call duration: 00:03:42

Listening to a Skype and voice call to a mobile or land line phone

The voice call record can be played in the **Audio content** area. The remote user information will include the number of a mobile or land line phone to which the call was made. The **General information** area displays the call duration, its cost and rate applicable for this type of calls.

Listening to any type of SIP voice call

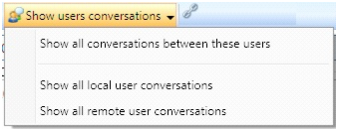
A voice call record can be played in the **Audio content** area. The **General information** area displays the duration of the call.



General information
Direction: Outgoing call
Call duration: 00:01:11

Viewing all the conversations between users

1. To view all the conversations between the users, click **Show user conversations** on the preview area toolbar and click **Show all conversations between these users**.



Show users conversations
Show all conversations between these users
Show all local user conversations
Show all remote user conversations

The results with all the conversations between these users in the current IM program will open in a new tab.

2. To view all the conversations of the local user, click **Show user conversations** on the preview area toolbar and click **Show all local user conversations**.

The results with all the conversations of this user in the current IM program will open in a new tab.

3. To view all the conversations of the remote user with the local ones, click **Show user conversations** on the preview area toolbar and click **Show all remote user conversations**.

The results with all the conversations of this user in the current IM program will open in a new tab.

***Note**: When viewing Skype or SIP conversations, there is one more function available – viewing all voice calls in Skype for the current users with the same collection of commands: viewing all calls made between the two current users, viewing all calls of the current local user and viewing all calls made by the current remote user to any local users.*

Saving an IM conversation

To save the conversation to a file, click **Save** on the preview area toolbar. In the save dialogue window, specify the folder where you want to save the conversation, and click **Save**. The conversation will be saved in the RTF format.

Printing an IM conversation

To print the intercepted IM conversation, click **Print** on the toolbar. In the new window select a printer and click **Print**.

Viewing transferred files

If there were any files transferred within a conversation, these files will be displayed in the **Conversation content** area. The list of files transferred will also be displayed in the right part of the IM conversation window, in the **Transferred files** area.

You can open any file transferred in a new tab. For this, select the necessary file in the **Transferred files** area, open the context menu by right-clicking the file and click **Open in new tab**.

Saving transferred files

To save the file transferred, select the corresponding file in the **Transferred files** area, open the context menu by right-clicking the file and click **Save file as**. The file will be saved in the format in which it was transferred.

5.2.6 Viewing files transferred in IMs (OSCAR, Jabber, Skype, SIP, Viber)

The program enables intercepting and viewing files transferred with instant messenger programs. Upon viewing a transferred file, one can switch to viewing the conversation within which this file was transferred.

In the transferred file window, you will see information blocks with the date and time of data interception, data nesting levels, local and remote users and the document content window.

To read about working with transferred files, go to *Viewing complex data formats (attachments, archives, transferred files)*.

5.2.7 Viewing files transferred over FTP protocol

Network users can download files from or upload to a remote server over the FTP protocol. FTP is a protocol designed for transferring files in computer networks. The program enables intercepting and viewing files both downloaded from and uploaded to an FTP-server.

In the transferred file window, you will see information blocks with the date and time of data interception, data nesting levels, local and remote users and the document content window. In this case, the remote user is represented by an FTP-server to/from which the file was uploaded/downloaded.

To read about working with files transferred over the FTP protocol, go to the *Viewing complex data formats (attachments, archives, transferred files)* section.

5.2.8 Viewing files copied to a storage device

Network users can copy files to a storage device (USB flash drive, hard disk drive, optical and floppy disc). The program enables interception and viewing files transferred to storage devices.

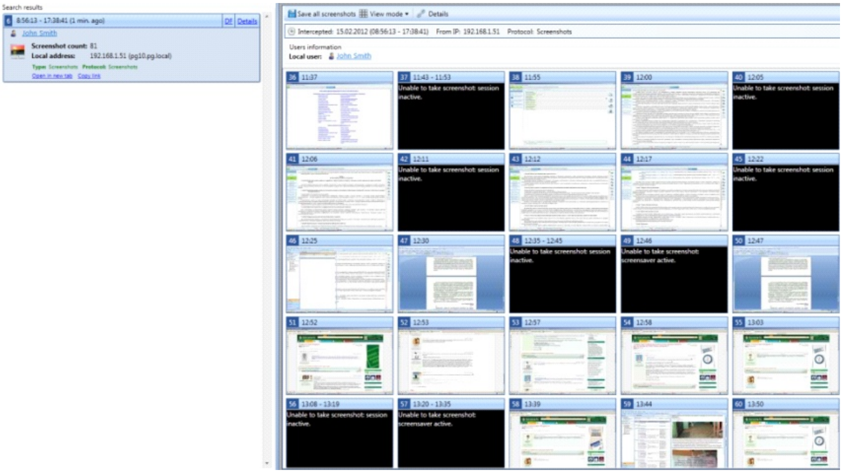
In the transferred file window, you will see information blocks with the date and time of data interception, file size, local user, device parameters such as device type, manufacturer, serial number, product ID, vendor ID and the document content window.

In cases when the size of transferred file is more than maximum size specified for shadow copying , the search result will be marked with corresponding alert symbol. Only the file's size and name as well as time of transfer and local user data will be available for inspection.

To read about working with files transferred to a portable storage, go to section *Viewing complex data formats (attachments, archives, transferred files)*.

5.2.9 Viewing user screenshots

When you click the **Screenshots** link in the user’s workday snapshot page (refer to section *Viewing daily network activity of a certain user*) or perform search through user screenshots (refer to section *Search by data type*), a search results window will open displaying the gallery of all screenshots taken on the selected user’s work station at specified time.



Search results

6 8:56:13 - 17:38:41 (1 min. ago)

John Smith

Screenshot count: 81

Local address: 192.168.1.51 (pg10.pg.local)

Type: Screenshots Protocol: Screenshots

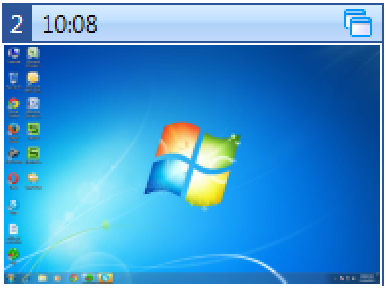
Intercepted: 15.02.2012 (08:56:13 - 17:38:41) From IP: 192.168.1.51 Protocol: Screenshots

Users information

Local user: John Smith

DF
Details
Open in new tab
Copy link
Save all screenshots
View mode
Details
36 11:37
37 11:43 - 11:53
Unable to take screenshot: session inactive.
38 11:55
39 12:00
40 12:05
Unable to take screenshot: session inactive.
41 12:06
42 12:11
Unable to take screenshot: session inactive.
43 12:12
44 12:17
45 12:22
Unable to take screenshot: session inactive.
46 12:25
47 12:30
48 12:35 - 12:45
Unable to take screenshot: session inactive.
49 12:46
Unable to take screenshot: screensaver active.
50 12:47
51 12:52
52 12:53
53 12:57
54 12:58
55 13:03
56 13:08 - 13:19
Unable to take screenshot: session inactive.
57 13:20 - 13:35
Unable to take screenshot: screensaver active.
58 13:39
59 13:44
60 13:50

The left part of the window contains information about the user (or users) and the computer the screenshots were taken at, as well as the information on the number and time of screenshots. The right part of the window is a preview area that contains a gallery with the thumbnails of all screenshots with their numbers, snapshot time and conditions: by timer - ◎, by new window - ❐, by PrtScr - ★.

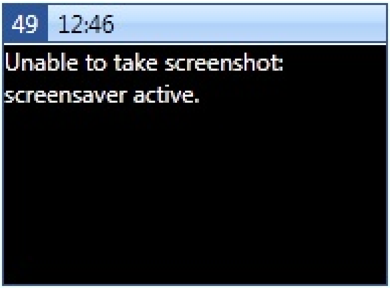


To filter the displayed screenshots in the gallery:

1. Click the **Screenshot type** drop-down arrow.
2. On the **Screenshot type** list, click the necessary type to select or to clear (if necessary).

Error messages

In case **SecureTower** failed to take a screenshot on the endpoint at a certain moment, a black box will be displayed in place of such screenshot with an indication of the reason which prevented the system from taking that screenshot.



Unable to take screenshot: screensaver active.

The 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.

Viewing mode

To set the mode of screenshots appearance in the viewing area, on the **View mode** menu:

- Click **Picture** to display a scaled-up thumbnails in the viewing area. This mode is also available when you click a thumbnail. Click the **Gallery** icon to switch from the picture view to gallery.

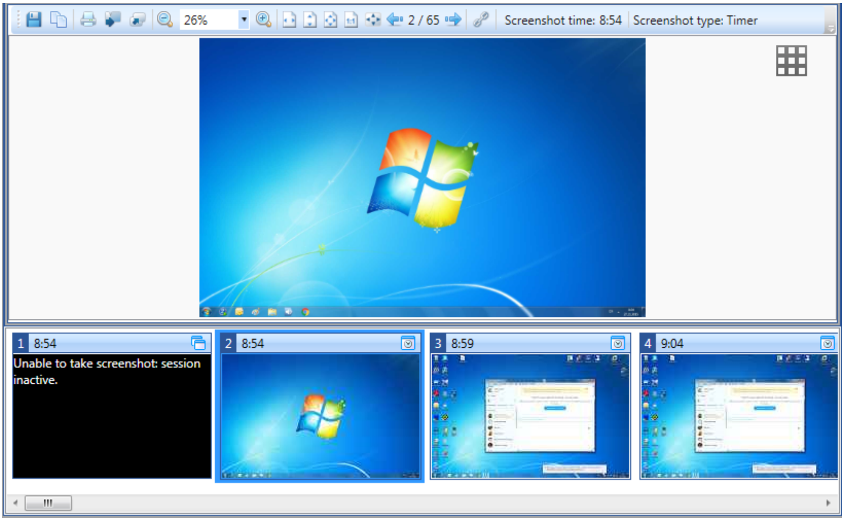
- Click **Gallery** to view all thumbnails of screenshots simultaneously (this mode is selected by default).

To view all screenshots in the slide show mode, click **Slideshow** button, then click the relevant drop-down arrow and select the interval of transition between slides.

Working with picture mode

If the **Picture** mode is selected two additional commands for thumbs panel layout and panel width settings appear on the toolbar:

1. Click **Thumbs panel layout** and select the necessary layout pattern for panel with thumbs of screenshots.
2. To specify the size in thumbs for panel width or height, click the **Thumbs per line** drop-down arrow, and then click the necessary number.



Screenshot time: 8:54 Screenshot type: Timer

Unable to take screenshot: session inactive.

The screenshot toolbar contains the following buttons:

- **Save document to file** - click to save the picture to file;
- **Copy** - click to copy the picture to clipboard;
- **Print** - click to print the picture;
- **Open at new tab** - click to open the picture in a new tab in Client Console;
- **Open external** - click to open the picture with default image viewer;

- **zoom tools** 47% - click a relevant button to zoom in or zoom out the picture or select the scale value from the drop-down list;
- **Original size** 1:1 - click to open the picture in original size as it was captured.
- **Fullscreen** - click to switch to full screen mode;
- scale tools - click to fit the image to viewing area;
- navigation tools 129 / 207 - use to navigate within the pictures;
- **Copy link** (for more information, see Viewing search results chapter).

Some of the options listed above are available from the image context menu as well.

Saving screenshots

The screenshots can be saved as the set of single image files in the PNG format, as single video-file in AVI format, as PDF document or as HTML file with baggage files folder.

To save all the screenshots of a selected user day to a selected format, on the viewing area toolbar click **Save** and configure saving settings in the **Save screenshots** window.

In the newly opened window both the user activity and information screenshot types can be selected for displaying separately or simultaneously as well as the date range can be set.

1. To view only the screenshots for the certain time range, specify it in the corresponding field. By default there is the time interval between the first and the last screenshots. Click the **Delete** icon in these fields to clear their from the current values. To apply the specified time filter click **Filter**. To return to default settings click **Reset filter**.

2. To display certain type screenshots, select the corresponding check box:

- Select **Show user activity screenshots** to display screenshots with captured user activity on it in the view area .
- Select **Show information screenshots** to display screenshots with system alert information.

3. To select screenshots for saving, select the check box next to the relevant thumb. Use scroll bar to view all content of the viewing area. The selection buttons can be used as well:

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

4. To display selected for saving items only click **Show selected screenshots**.

The information about total, shown and selected items number is displayed under viewing area.

5. To select an output file format choose one from the **Save screenshots as** list.

6. To complete saving click **Save**.

Printing screenshots

To print the screenshots of a selected user day click **Print**.

In the newly opened window both the user activity and information screenshot types can be selected for displaying separately or simultaneously as well as the date range can be set.

1. To view only the screenshots for the certain time range specify it in the corresponding field. By default there is the time interval between the first and the last screenshots. Click the **Delete** icon ✖ in these fields to clear their from the current values. To apply the specified time filter click **Filter**. To return to default settings click **Reset filter**.

2. To display certain type screenshots select the corresponding check box:

- Select **Show user activity screenshots** to display screenshots with captured user activity on it in the view area .
- Select **Show information screenshots** to display screenshots with system alert information.

3. To select screenshots for saving check the check box next to corresponding thumb. Use scroll bar to view all content of the view area. One can also use the selection buttons below the list:

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

4. To display selected for saving items only click **Show selected screenshots**.

Information about total, shown and selected items number is displayed under viewing area.

5. To select an output file format click one from the **Save screenshots as** list.

6. To complete saving click **Save**. To cancel choice was made and to return to screenshots viewing click cancel.

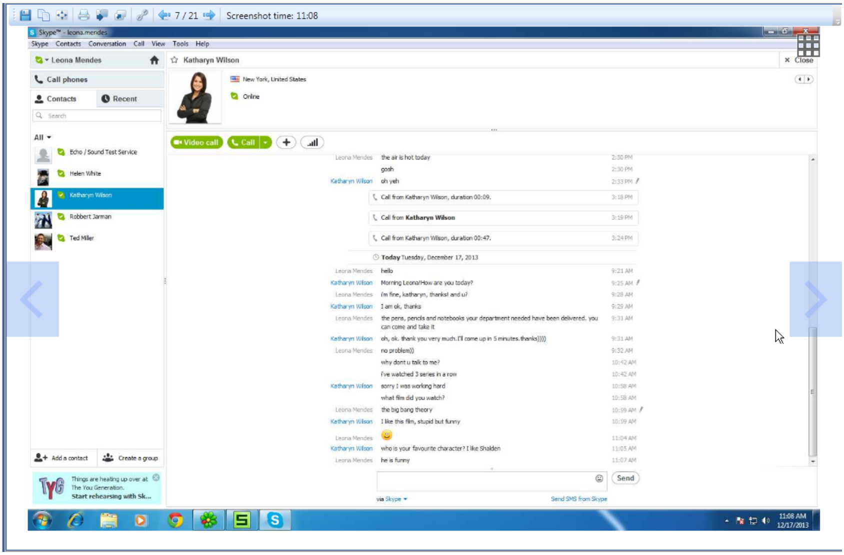
7. To configure printing parameters choose one from available in the **Print options** list:

- Select the **Print pictures on separate pages** check box to print one picture per page.
- Select the **Print pictures on one page** check box to print several pictures on one page. The number of pictures per page is not fixed and depends on pictures size. To ensure pictures identification with date and number check the corresponding option.

8. To print selected screenshots click **Print**.

Viewing tips

- Use the navigation buttons which are available upon hovering over the view zone borders to navigate through pictures.



```
Leona Mendes     the air is hot today                                   2:30 PM
                 gosh                                                   2:30 PM
Katharyn Wilson  oh yeh                                                 2:33 PM
                 Call from Katharyn Wilson, duration 00:09.             3:18 PM
                 Call from Katharyn Wilson                              3:19 PM
                 Call from Katharyn Wilson, duration 00:47.             3:24 PM
                 Today Tuesday, December 17, 2013
Leona Mendes     hello                                                  9:21 AM
Katharyn Wilson  Morning Leona!How are you today?                       9:25 AM
Leona Mendes     i'm fine, katharyn, thanks! and u?                     9:28 AM
Katharyn Wilson  I am ok, thanks                                        9:29 AM
Leona Mendes     the pens, pencils and notebooks your department needed have been delivered. you
                 can come and take it                                   9:31 AM
Katharyn Wilson  oh, ok. thank you very much.I'll come up in 5 minutes.thanks))))   9:31 AM
Leona Mendes     no problem))                                           9:32 AM
                 why dont u talk to me?                                 10:42 AM
                 i've watched 3 series in a row                         10:42 AM
Katharyn Wilson  sorry I was working hard                               10:58 AM
                 what film did you watch?                               10:58 AM
Leona Mendes     the big bang theory                                    10:59 AM
Katharyn Wilson  I like this film, stupid but funny                     10:59 AM
Leona Mendes     😊                                                     11:04 AM
Katharyn Wilson  who is your favourite character? I like Shalden        11:05 AM
Leona Mendes     he is funny                                            11:07 AM
```

- To zoom the currently viewing screenshot mouse over it and double-click. Use the navigation keys to drug the screenshot within the view zone.
- To zoom in/out the screenshot press and hold Ctrl and scroll the mouse wheel.
- To navigate through the screenshot, when viewing in the full screen mode, use the combination of pressed Ctrl + navigation keys (right/left).
- To open the picture in the original size, double-click it.

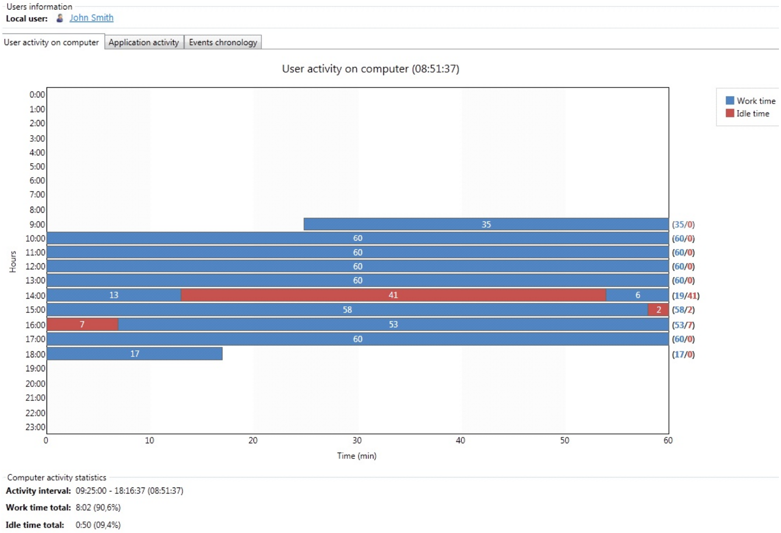
5.2.10 Viewing endpoint activity statistics

When you click the link "**N minutes activity**" in the user's workday snapshot page (refer to section *Viewing daily network activity of a certain user*) or perform search by desktop activity (refer to section *Search by data type*), a search results window will open displaying the information about the activity of a selected endpoint.

Endpoint activity statistics are displayed in three tabs - **User activity on computer**, **Application activity** and **Events chronology**.

User activity on computer

The first tab displays endpoint activity (blue) and idle (red) periods hour-by-hour. The length of the blue/red lines represents the duration of the corresponding computer state (indicated by the numbers of minutes in the lines). The period of user inactivity (absence of keystrokes, mouse movements and clicks), after which the system marks a computer as idle, is set in the ***SecureTower*** *Administrator Console* (default value being 5 minutes).

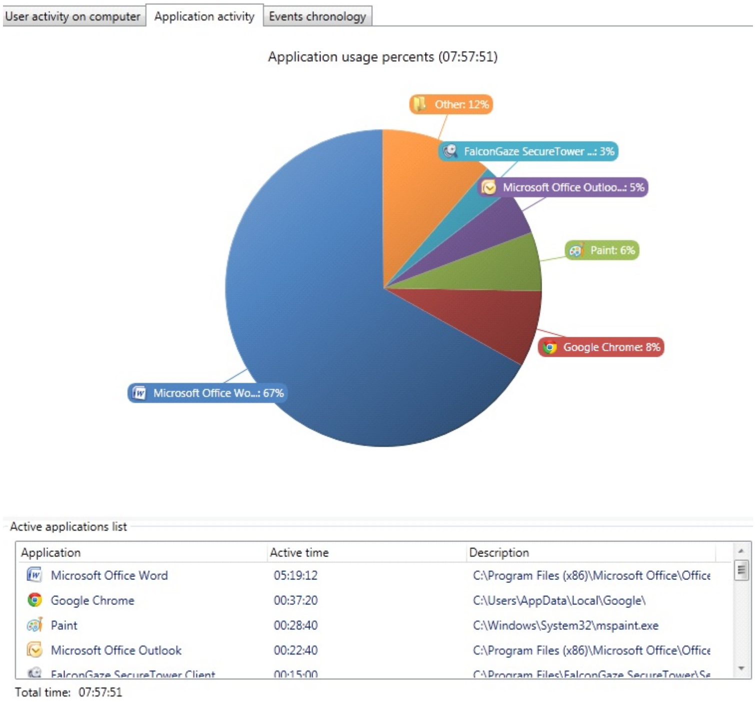

Users information
Local user: John Smith

Computer activity statistics
Activity interval: 09:25:00 - 18:16:37 (08:51:37)
Work time total: 8:02 (90,6%)
Idle time total: 0:50 (09,4%)

To view more detailed information about computer state, left-click the particular line on the diagram. The **Events chronology** tab will be opened with highlighted period of interest.

Application activity

The second tab displays a graph of application activity on the endpoint. The graph shows the applications run by the user, and the percentage of time the user was working with these applications.


User activity on computer
Application activity
Events chronology
Application usage percents (07:57:51)
Other: 12%
FalconGaze SecureTower ...: 3%
Microsoft Office Outloo...: 5%
Paint: 6%
Google Chrome: 8%
Microsoft Office Wo...: 67%
Active applications list

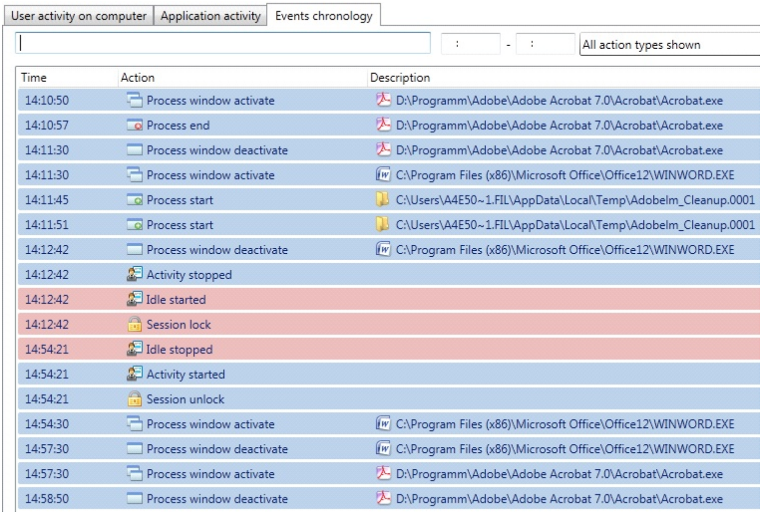
Application	Active time	Description
Microsoft Office Word	05:19:12	C:\Program Files (x86)\Microsoft Office\Office
Google Chrome	00:37:20	C:\Users\AppData\Local\Google\
Paint	00:28:40	C:\Windows\System32\mspaint.exe
Microsoft Office Outlook	00:22:40	C:\Program Files (x86)\Microsoft Office\Office
FalconGaze SecureTower Client	00:15:00	C:\Program Files\FalconGaze SecureTower\Se

Total time: 07:57:51

In the lower part of the window you can see a list of all applications run by the user, and the duration of their activity. **SecureTower** system starts counting the activity time of an application when the user activates the corresponding application window. When a user switches to another window, the system starts counting activity time for that application.

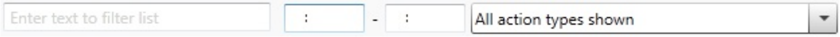
Events chronology

The **Events chronology** tab displays a list of all events on the selected endpoint (including start/stop of the activity and idle periods, start/termination of, activation/deactivation of application windows, etc.). The events during computer idle period are marked in red, the events in the active periods are marked in blue.



Time	Action	Description
14:10:50	Process window activate	D:\Programm\Adobe\Adobe Acrobat 7.0\Acrobat\Acrobat.exe
14:10:57	Process end	D:\Programm\Adobe\Adobe Acrobat 7.0\Acrobat\Acrobat.exe
14:11:30	Process window deactivate	D:\Programm\Adobe\Adobe Acrobat 7.0\Acrobat\Acrobat.exe
14:11:30	Process window activate	C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE
14:11:45	Process start	C:\Users\A4E50~1.FIL\AppData\Local\Temp\Adobelm_Cleanup.0001
14:11:51	Process start	C:\Users\A4E50~1.FIL\AppData\Local\Temp\Adobelm_Cleanup.0001
14:12:42	Process window deactivate	C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE
14:12:42	Activity stopped	
14:12:42	Idle started	
14:12:42	Session lock	
14:54:21	Idle stopped	
14:54:21	Activity started	
14:54:21	Session unlock	
14:54:30	Process window activate	C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE
14:57:30	Process window deactivate	C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE
14:57:30	Process window activate	D:\Programm\Adobe\Adobe Acrobat 7.0\Acrobat\Acrobat.exe
14:58:50	Process window deactivate	D:\Programm\Adobe\Adobe Acrobat 7.0\Acrobat\Acrobat.exe

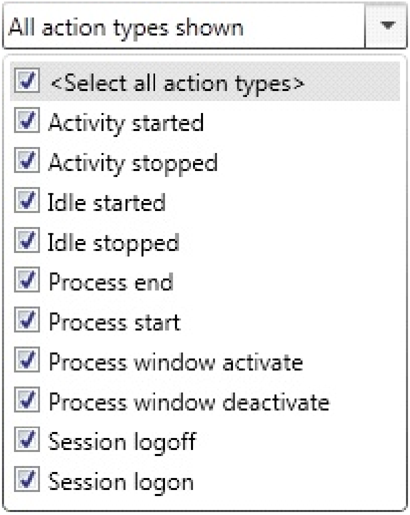
To search for a specific event in the list, you can enter the corresponding characters in the list filtering text field.



As you type, the list will only display the events having the entered combination of symbols in their **Description** field.

You can filter the events list by time. To do this, enter the time period into the boxes next to the text field.

Besides, you can configure the list to include only events of certain types. To do this, check the boxes next to the event types in the drop-down menu.



All action types shown

- ☑ <Select all action types>
- ☑ Activity started
- ☑ Activity stopped
- ☑ Idle started
- ☑ Idle stopped
- ☑ Process end
- ☑ Process start
- ☑ Process window activate
- ☑ Process window deactivate
- ☑ Session logoff
- ☑ Session logon

Saving reports data

To save endpoint activity data for the selected user click **Save** on the preview area toolbar:

- To save the report displayed in the currently opened tab click **Save current report**.
- To save all type of reports available for computer activity of the selected date click **Save all type of reports**.

Selected types of reports will be saved to the PDF file including the user data.

Printing reports

To print any report on computer activity for the selected user click **Print** on the preview area toolbar:

- To print the report displayed in the currently opened tab click **Print current report**.
- To print all type of reports available for computer activity of the selected date click **Print all type of reports**.

Selected types of reports will be printed on the specified printer.

5.2.11 Viewing clipboard content

When you click the link "**N copies to clipboard**" in the user's workday snapshot page (refer to section *Viewing daily network activity of a certain user*) or perform search by desktop activity (refer to section *Search by data type*), a window with search results will be opened. There one can inspect the list of copies contained in clipboard for specified time/ date interval.

5.2.12 Viewing files transferred to network shares

Network users can copy files to network shares. The program enables intercepting and viewing files transferred to network folder and discs that can be remotely accessed from another computer.

In the transferred file window, you will see information blocks with the date and time of data interception,file size and name, local user name, application parameters (network pass, name, vendor) and the document content window.

In cases when the size of transferred file is bigger than maximum size specified for shadow copying, the search result will be marked with corresponding alert symbol. Only the file's size and name as well as time of transfer and local user data will be available for inspection.

See also: *Viewing complex data formats (attachments, archives, transferred files)*.

5.2.13 Viewing cloud storages files

Users can transfer any kind of data using different cloud storage services. **SecureTower** provides a complex control of operations with cloud storages for both the desktop application and web services.

The data transferred to/from cloud storages is intercepted by making a shadow copy.

If the file size is more than specified in settings for maximum size available for shadow copying the size and name of the file, time and date of the operation and local user name will be displayed only

See also: *Viewing complex data formats (attachments, archives, transferred files)*.

5.2.14 Keylogger viewing

SecureTower provides complex information about users computer activity by using keystroke logging. All data about keystrokes and corresponding applications, date and time, user IP address are available from the Client console and can be analyzed automatically in Security center (in case of appropriate policies setup).

The following commands are available on the keylogger toolbar:

- **Print** - intercepted data can be printed directly from the Client console.

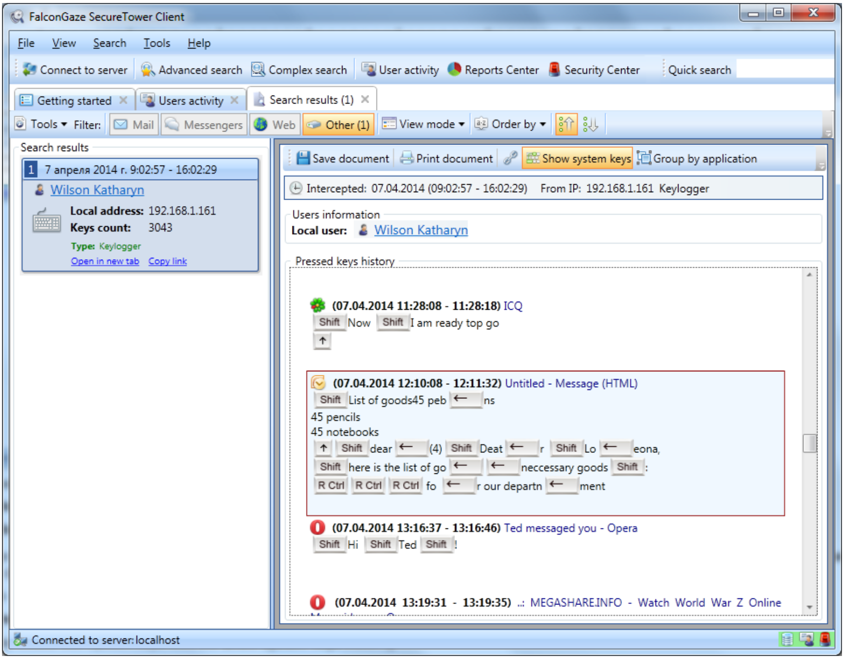
- **Save** - intercepted data can be saved to PDF file with user data and keylogger report.

- Use the **Copy link** button to copy to clipboard the link to this result.

- **Details** - access to the system properties of the document with intercepted data.

- **Copy messages** - intercepted data can be copied to clipboard.

To display results with system keys click **Show system keys** .



Search results

1 7 апреля 2014 г. 9:02:57 - 16:02:29

Wilson Katharyn

Local address: 192.168.1.161

Keys count: 3043

Type: Keylogger

Intercepted: 07.04.2014 (09:02:57 - 16:02:29) From IP: 192.168.1.161 Keylogger

Users information

Local user: Wilson Katharyn

Pressed keys history

(07.04.2014 11:28:08 - 11:28:18) ICQ

Shift Now Shift I am ready top go
↑

(07.04.2014 12:10:08 - 12:11:32) Untitled - Message (HTML)

Shift List of goods45 peb ← ns
45 pencils
45 notebooks
↑ Shift dear ← (4) Shift Deat ← r Shift Lo ← eona,
Shift here is the list of go ← ← neccessary goods Shift :
R Ctrl R Ctrl R Ctrl fo ← r our departn ← ment

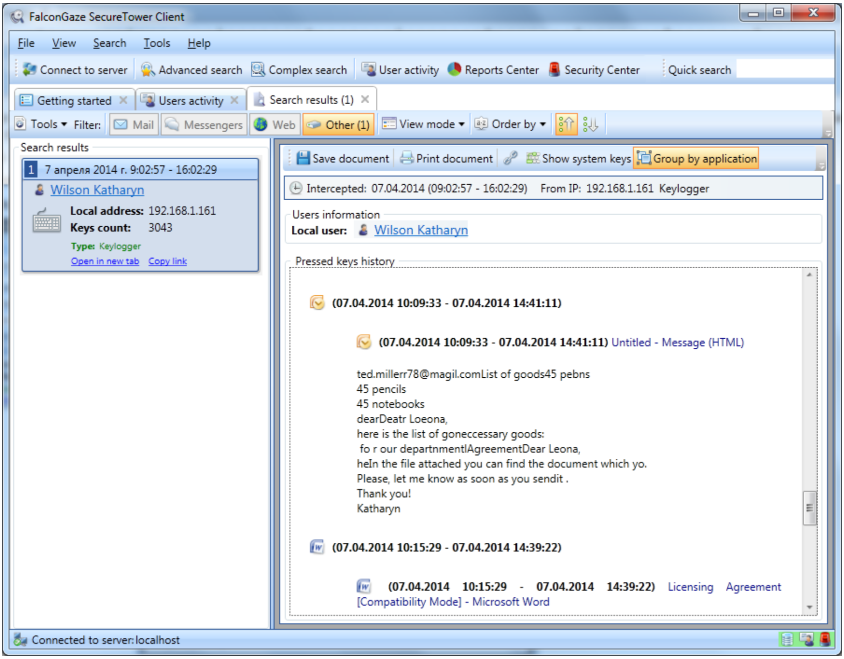
(07.04.2014 13:16:37 - 13:16:46) Ted messaged you - Opera

Shift Hi Shift Ted Shift !

(07.04.2014 13:19:31 - 13:19:35) .:: MEGASHARE.INFO - Watch World War Z Online

Connected to server: localhost

To sort intercepted data by application click **Group by applications**.



1 7 апреля 2014 г. 9:02:57 - 16:02:29

Wilson Katharyn

Local address: 192.168.1.161

Keys count: 3043

Type: Keylogger

Intercepted: 07.04.2014 (09:02:57 - 16:02:29) From IP: 192.168.1.161 Keylogger

Users information

Local user: Wilson Katharyn

Pressed keys history

(07.04.2014 10:09:33 - 07.04.2014 14:41:11)

(07.04.2014 10:09:33 - 07.04.2014 14:41:11) Untitled - Message (HTML)

ted.millerr78@magil.comList of goods45 pebns
45 pencils
45 notebooks
dearDeatr Loeona,
here is the list of goneccessary goods:
fo r our departnmentlAgreementDear Leona,
heln the file attached you can find the document which yo.
Please, let me know as soon as you sendit .
Thank you!
Katharyn

(07.04.2014 10:15:29 - 07.04.2014 14:39:22)

(07.04.2014 10:15:29 - 07.04.2014 14:39:22) Licensing Agreement [Compatibility Mode] - Microsoft Word

Note*: To control user activity in any application with the particular document content, set* ***Keylogger*** *for* ***Search in*** *condition and unite it with* ***Title*** *for* ***Process*** *condition while the complex search performing.*

5.2.15 Viewing device audit data

Devices audit

SecureTower enables monitoring and control of external devices usage. The number of connected devices, their types, connection duration, current condition of connection as well as local user and IP data are provided in the results window.

The following commands are available on the search results window toolbar:

- **Print** - intercepted data can be printed directly from the Client console.

- **Save** - intercepted data can be saved to RTF file with user data and audit report.

- The **Copy link** button 🔗 is used to copy to clipboard the link to this result.

- **Details** - access to the system properties of the document with intercepted data.

The audit data can be filtered in two different ways:

- Select or clear the check boxes on the **Devices types** area to filter results by device type;

- To search for a specific device in the results, on the audit window toolbar type the corresponding characters in the **Filter** text field. As you type, the list will only display the audit results with entered combination of symbols in their parameters fields.

File operations audit

SecureTower provide a control on users and processes file operations with: mass storage devices, local network shares, cloud storages.

In the search audit results window the list of all file operations with local user and serviced information are displayed. All items in the list for which the shadow copy was implemented link to their original documents that were intercepted

Note: *.Viewing files content is available if the shadow copy was taken for those files.*

To open the service information about an audit result select and click the corresponding row in the list. The service information with file name (path to file on the local disc), process data, file author, date and time of operation as well as other operation type sensitive data will be displayed on the **File properties** area.

To view the file content left-click it's name.

For more operation with file right-click it's and select the necessary operation from the file context menu. The following commands are available:

- **Open in new tab** - opens current document in a new tab in the Search Client console;

- **Open external** - is used to open the document with another program. The document will be opened in the application intended for processing this file format.

- **Save document** - intercepted data can be saved to file with user data and audit report.

- The **Copy link** button 🔗 to copy to clipboard the link to this result.

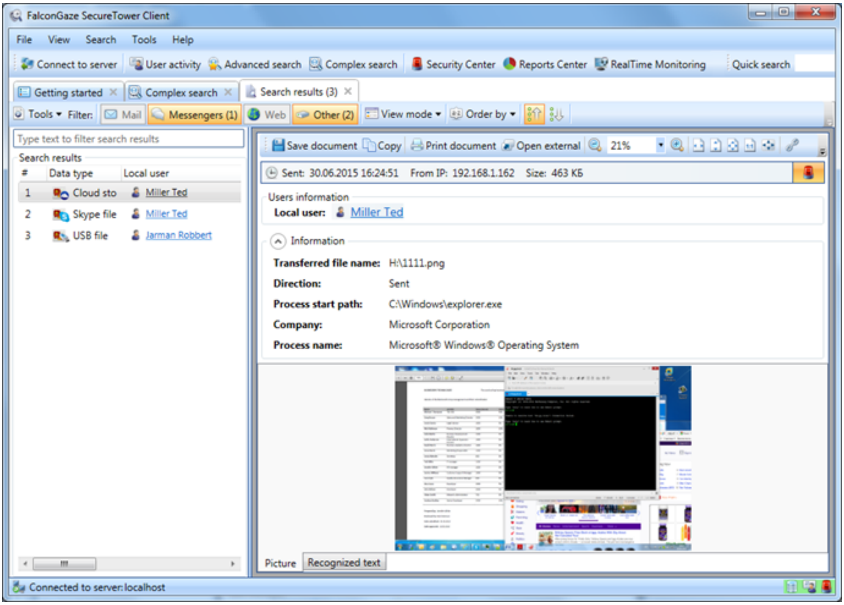
Note: *Scale the **Files audit information** section to expand the window when there are too many entries in the list.*

5.2.16 Viewing recognized text

The high-tech image recognition **SecureTower** module enables recognizing text on intercepted images with following data analysis. This functionality is useful at situations when the transmission of scanned confidential documents is widely used. The **SecureTower** system tool works equally well with any format of graphic information (whether it is the JPG, BMP, TIFF format or any other) or PDF files. The module recognizes data not only in English but also in foreign languages, this feature make it possible to carry out content analysis based on morphology.

There are two tabs in the recognized images result window:

- Select the **Picture** tab to display a recognized image in original format.



FalconGaze SecureTower Client
File View Search Tools Help
Connect to server User activity Advanced search Complex search Security Center Reports Center RealTime Monitoring Quick search
Getting started Complex search Search results (3)
Tools Filter: Mail Messengers (1) Web Other (2) View mode Order by
Save document Copy Print document Open external 21%
Picture Recognized text

Type text to filter search results

Search results

#	Data type	Local user
1	Cloud sto	Miller Ted
2	Skype file	Miller Ted
3	USB file	Jarman Robbert

Sent: 30.06.2015 16:24:51 From IP: 192.168.1.162 Size: 463 КБ

Users information

Local user: Miller Ted

Information

Transferred file name: H:\1111.png

Direction: Sent

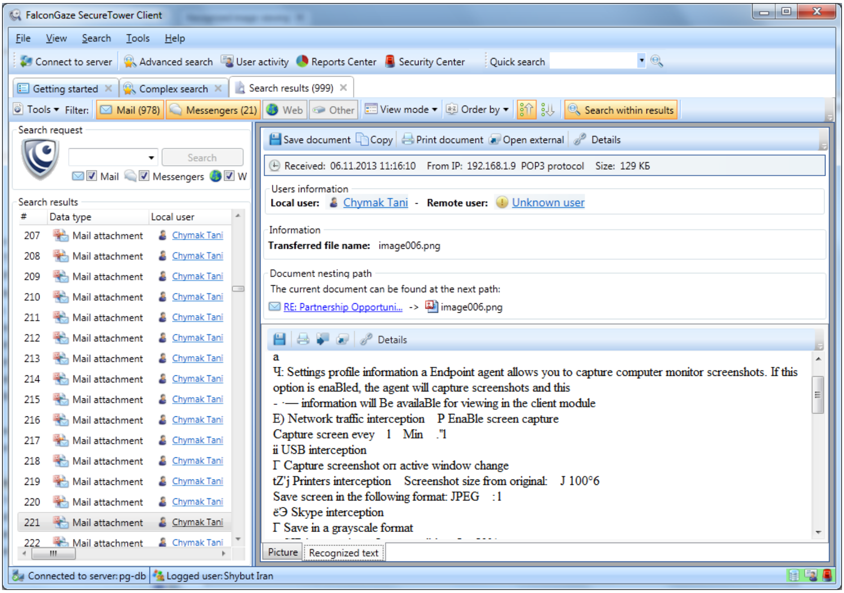
Process start path: C:\Windows\explorer.exe

Company: Microsoft Corporation

Process name: Microsoft® Windows® Operating System

Connected to server:localhost

- Select the **Recognized text** to display text recognized on the intercepted image. The text will be displayed without formatting.



FalconGaze SecureTower Client
File View Search Tools Help
Connect to server Advanced search User activity Reports Center Security Center Quick search
Getting started Complex search Search results (999)
Tools Filter: Mail (978) Messengers (21) Web Other View mode Order by Search within results
Save document Copy Print document Open external Details
Search request
Search
Mail Messengers W
Details
Picture Recognized text

Search results

#	Data type	Local user
207	Mail attachment	Chymak Tani
208	Mail attachment	Chymak Tani
209	Mail attachment	Chymak Tani
210	Mail attachment	Chymak Tani
211	Mail attachment	Chymak Tani
212	Mail attachment	Chymak Tani
213	Mail attachment	Chymak Tani
214	Mail attachment	Chymak Tani
215	Mail attachment	Chymak Tani
216	Mail attachment	Chymak Tani
217	Mail attachment	Chymak Tani
218	Mail attachment	Chymak Tani
219	Mail attachment	Chymak Tani
220	Mail attachment	Chymak Tani
221	Mail attachment	Chymak Tani
222	Mail attachment	Chymak Tani

Received: 06.11.2013 11:16:10 From IP: 192.168.1.9 POP3 protocol Size: 129 КБ

Users information

Local user: Chymak Tani - **Remote user:** Unknown user

Information

Transferred file name: image006.png

Document nesting path

The current document can be found at the next path:

RE: Partnership Opportuni... -> image006.png

```
a
Ч: Settings profile information a 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
E) Network traffic interception    P EnaBle screen capture
Capture screen evey    1    Min    ."1
ii USB interception
Г Capture screenshot oп active window change
tZ'j Printers interception    Screenshot size from original:    J 100°6
Save screen in the following format: JPEG    :1
ёЭ Skype interception
Г Save in a grayscale format
```

Connected to server:pg-db Logged user:Shybut Iran

5.2.17 Viewing browser activity

When you click the link “**N minutes activity**” in the user’s workday snapshot page (refer to section *Viewing daily network activity of a certain user*) or perform search by desktop activity (refer to section *Search by data type*), a search results window will be opened displaying the information about the user browser activity.

Browser activity statistics are displayed in two tabs - **Host statistics** and **Url activity chronology**.

The following commands are available on the browser activity window toolbar:

- **Print** - intercepted data can be printed directly from the Client console.

- **Save** - intercepted data can be saved to PDF file.

- **Details** - access to the system properties of the document with intercepted data.

- Use the **Copy link** button 🔗 to copy to clipboard the link to this result. The link is necessary for quick access to intercepted data within the **SecureTower** Client console (for more information, see *Viewing search results*).

Host statistics

The **Host statistics** tab represents information concerning the history of all websites visited by user and visit durations in the form of chart and table form.

The sites names on the chart are interactive and link to detailed information about user navigation via the corresponding web site.

Url activity chronology

The **Url activity chronology** tab in the common case represents the table with list of the all visited with help of browser web sites.

One can use the filter of the web pages list:

- To filter pages by web address type the corresponding characters in the **Filter** text field. As you type, the list will only display the results with entered combination of symbols in their url-address;

- To filter pages by time of interception type a time range in the corresponding cells.

Saving reports data

To save browser activity data for the selected user click **Save** on the preview area toolbar:

- To save the report displayed in the currently opened tab click **Save current report**.

- To save all type of reports available for computer activity of the selected date click **Save all type of reports**.

Selected types of reports will be saved to the PDF file including the user data.

Printing reports

To print any report on browser activity for the selected user click **Print** on the preview area toolbar:

- To print the report displayed in the currently opened tab click **Print current report**.
- To print all type of reports available for computer activity of the selected date click **Print all type of reports**.

Selected types of reports will be printed on the specified printer.

5.2.18 Viewing results of workstation indexing

SecureTower enables indexing the files systems of controlled workstations and performing control of coincidences between files on workstations and files from data bank with confidential files hashes. If the coincidence is detected, the system will make the corresponding records to **SecureTower** database of intercepted data.

The results of files systems control can be accessed upon search on **Workstation indexer** data type. The content of the files detected upon coincidences searching can be viewed in the console for each search result. To view the content, click **Open** in the result window.

5.3 Identifying senders and recipients in search results

Each search result (document) specifies local and remote users between which the data were exchanged. A remote user can be represented by a server (for example, for a document transferred over FTP protocol).

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, user SID, ICQ UINs, user accounts in IM programs, user names in social networks, etc.).

Note: User SID is a unique user ID in Active Directory. This ID is intercepted together with the information captured by monitoring agents. Upon importing users from Active Directory, the SID field in user cards is automatically filled in, so when you view any information intercepted by endpoint agents, for example, a Skype conversation, you will see the user full name (as they appear in their user card) together with their Skype user name or IP address which, alone, would be insufficient to correctly or accurately identify the user.

Originally, user database is formed and configured by an administrator in the *Administrator Console*. To read more about working with user cards, go to *Monitoring user network activity* of this **User Guide**.

Viewing sender/recipient information:

1. To view information about the user who sent or received certain data, click the link with their name in a search result box. If data were sent or received by a user with no

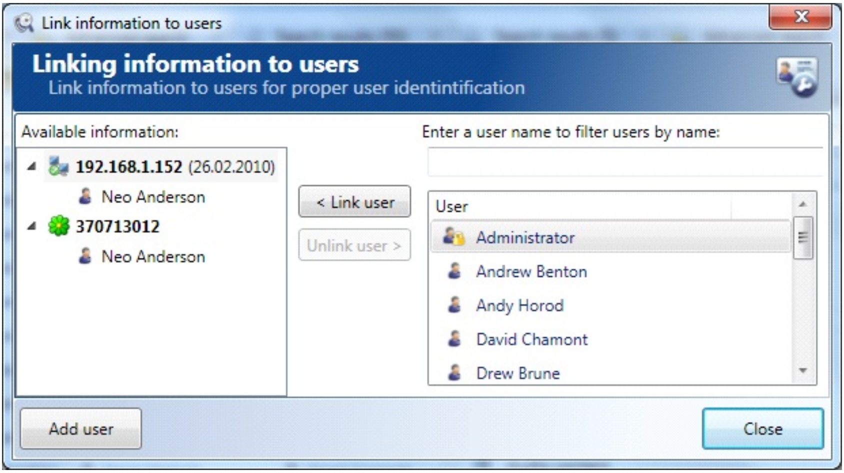
identification card assigned, this user line will say “Unknown user”.

Jennifer White – Unknown user

***Note**: If the interception service was started after some instant messenger conversation was initiated, it is possible that the intercepted information of the conversation parties will be incomplete. For example, for an ICQ conversation, only the remote user’s UIN can be intercepted. In that, for the local user only the IP address will be known. After some time elapses, the local user’s UIN can be extracted from traffic, and in this case the conversation will be deemed by the program as a conversation between other users, and, therefore, will be displayed in search results as a new conversation. Thus, a situation is possible in which the same conversation is presented by the program in several search results, with different conversation parties mentioned.*

2. If data were sent or received by the user with an identification card assigned, you will see the information linked to this user in a new window. To view and modify this user card, right-click the name of the user and click **View user card** on the context menu. User cards for any user from the list in the right part of the window can be viewed analogically.

   To read more about modifying user cards, go to *User cards*.



Link information to users

Linking information to users

Link information to users for proper user identintification

Available information:

- 192.168.1.152 (26.02.2010)
  - Neo Anderson
- 370713012
  - Neo Anderson

Enter a user name to filter users by name:

User
Administrator
Andrew Benton
Andy Horod
David Chamont
Drew Brune

Modifying user identification information:

In the **Link information to users** window, you can link the displayed identification information to any user by selecting the necessary link attribute (IP address, e-mail address, UIN, etc.) and the corresponding user in the right part of the window, and by clicking the **Link user** button.

To remove a link between the user and identification attributes, select the necessary link attribute or the corresponding user and click **Unlink** user.

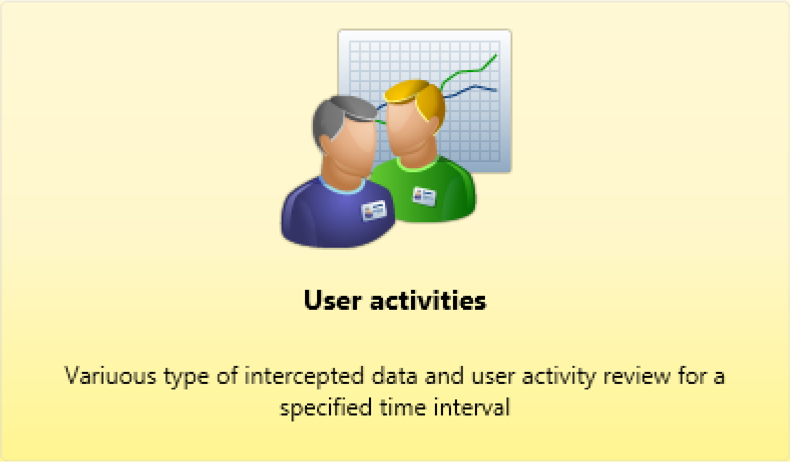
6 Monitoring user network activity

In addition to exact *identification of data senders and recipients*, the program features monitoring various type of intercepted data and network activities of specified network users. The program applies a user card system with binding of each local network user to **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.).

Besides, user cards provide group membership information. As well as user cards, **the user groups** are created with the help of the Administrator Console and each of them is assigned with certain user rights. Groups may 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”).

You can monitor **network activity** of each network user as a report for the period of time you want starting from the period of last 30 days to an hourly specification of user activities. The information presented in the report includes the number of visited web-addresses, e-mail messages, instant messenger conversations, received or sent files and requests. You may view the details of each data type by clicking it.

To monitor user network activity, click in the **User activities** area on the program start page or click **User activity** on the program toolbar.

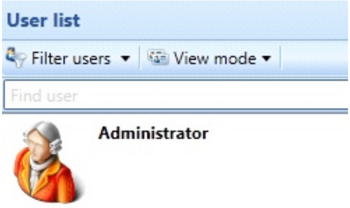


User activities

Variuous type of intercepted data and user activity review for a specified time interval

6.1 User list

In the left pane of the user network activity window, you will see the list of network users generated on the basis of user cards that were created in the Administrator Console.



Filtering user list

By default, the list contains all users irrespective of their employment period. You can select a corresponding command on the **All users** menu to show/hide currently working or redundant users, as well as users with active sessions on the computers controlled by agent.

Besides, you can find the necessary user card in the list by entering the corresponding name or e-mail address in the Find user text field. Filtering user list will start with the first symbol entered; with each additional symbol entered, all the irrelevant results will be excluded from the user list. To clear the search results and return to the full user list, delete text from the Find user field.

Note: Search by e-mail address is performed not by exact match, but by the presence of the specified symbol combination in the e-mail address.(Example: if you enter “ted” in the Text to filter by field, the search results will show not only users with the email address teddy@gmail.com, but also the one with wanted@hotmal.com.)

User list view mode

You can select a desired mode for viewing network users.

To view all users as a simple list, click **View mode** on the toolbar and then click **List view**.

To have users displayed as user cards with photos, click **View mode** and then click **Card view**.

To have users displayed by administrative user groups, click **View mode** and then click **Group by company/department view**.

In this mode the information about network users will be represented in hierarchy tree form that may repeat the structure of your company with its departments.

You can collapse/expand certain groups by clicking the button with “-“/”+” icons located in front of the corresponding group.

Filtering user list

By default, the list contains all users irrespective of their employment period. You can select a corresponding command on the **All users** menu to show/hide currently working or redundant users, as well as users with active sessions on the computers controlled by agent.

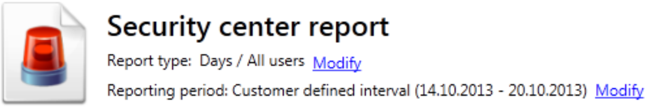
Besides, you can find the necessary user card in the list by entering the corresponding name or e-mail address in the Find user text field. Filtering user list will start with the first symbol entered; with each additional symbol entered, all the irrelevant results will be excluded from the user list. To clear the search results and return to the full user list, delete text from the Find user field.

Note: Search by e-mail address is performed not by exact match, but by the presence of the specified symbol combination in the e-mail address.(Example: if you enter “ted” in the Text to filter by field, the search results will show not only users with the email address teddy@gmail.com, but also the one with wanted@hotmal.com.)

The **Active Directory structure view** mode provides user list displaying in compliance with Active Directory structure. All AD user accounts will be displaying and available for choice regardless existence of the user card for selected AD account.

The **Groups view** mode provides user displaying in compliance with groups organized by the **SecureTower** User authentication server.

You can collapse/expand certain groups by clicking the **Unfold** button located in front of the corresponding group.



Security center report

Report type: Days / All users Modify

Reporting period: Customer defined interval (14.10.2013 - 20.10.2013) Modify

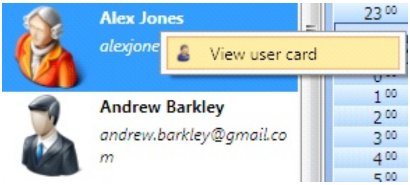
Refreshing user list

To refresh a user list, click **Refresh** on the toolbar of the user list window. This may be helpful for obtaining updated information on user cards that can be modified by other users of **SecureTower** Client or Administrator applications.

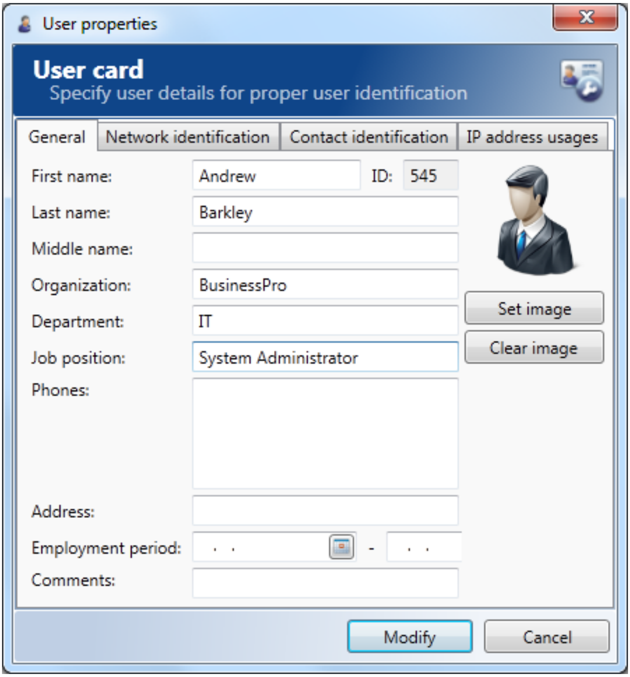
6.2 User cards

Viewing and modifying information in user cards

To be able to view and modify user cards, select the necessary user in the user list window, right-click their name and click the **View user card** command in the context menu.



The **Modify user card** window contains the following tabs: **General, Network identification, Contact identification** and **IP address usages**. By switching between these tabs you can view and enter the corresponding information. Upon finishing modifying the user card, click **Modify** to apply the changes made.



First name: Andrew ID: 545
Last name: Barkley
Middle name:
Organization: BusinessPro
Department: IT
Job position: System Administrator
Phones:
Address:
Employment period: . . - . .
Comments:

General In this tab you 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 and address, in the corresponding text fields. Apart from that, you can specify additional information in the **Comments text** field.

To provide a user with a certain image, click **Set image** in the right part of the tab. In the open file dialogue box, specify the folder in which the necessary file is located, select it and click **Open**. The file added will be displayed in the top right corner of the **General** tab.

Network identification

In this tab you can view the information about the Windows Active Directory account of the selected user. To change the current Active Directory account of the user, click **Browse** and select the user’s AD account.

Besides, this tab contains information about the internal user account in the **SecureTower** system, including the name and password (this section should be filled when using the internal authentication mode). After the default password is specified, you may oblige the user to change it at next logon for security purposes (for more information, see *Getting started. Connecting to the server*). To do this, check the corresponding option.

The next section of the tab contains IP address usage history for the current user. IP address usage history reflects what IP addresses were used by this user and within which time interval.

Contact identification

This tab contains the user’s network contacts (e-mail addresses, ICQ numbers, Skype and Viber accounts). Though the system enables automatic linking of contact information to user cards (refer to **Automatic assignment of contact information** of the Administrator Guide), you can add contact data to the user card manually.

IP address usages

This tab contains the IP-address usage history for selected user. IP address usage history reflects what IP addresses were used by this user and within which time interval.

You can enter a record on a certain IP address usage yourself by clicking **Add IP address usage**. In the dialogue box opened, specify the necessary IP address and time interval within which it was used by the current user, and click **Add**.

To delete a record on a certain IP address usage, select the corresponding record and click **Delete IP address usage**.

6.3 Viewing user network activity report

The user network activity window has two main components: **the user activity report board** in the right pane, **the users list** in the left pane. In order to open a network activity report for a certain user, select the corresponding user in the user list and just double click them or click **Build report** on the report board toolbar.

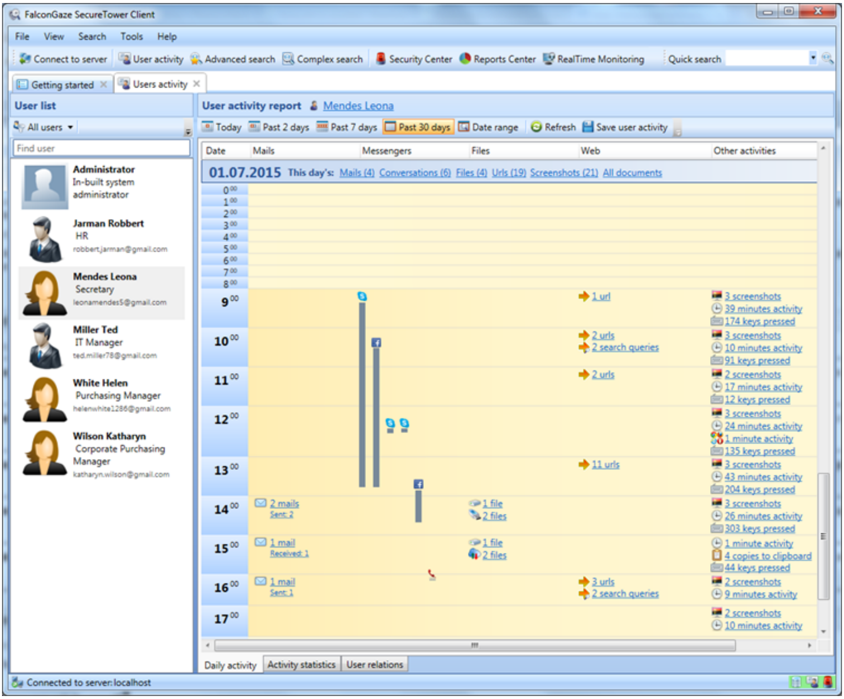
The report can be saved to the HTML file. After saving the report data in the HTML format can be opened with a web browser.

6.3.1 Viewing daily network activity of a certain user

You will be able to see the number of messages, e-mails, requests, or files that the current user sent or received every hour within the specified period of time. If there was no network activity within a certain period of time, only a date will be displayed (without an hourly activity specification) and statement "**No intercepted data found**".

The total quantity of all data types is indicated on the information panel next to the corresponding date in the form of active links.

Clicking on each link, you can open a report with all data of corresponding type (Mails, Conversations, Files, etc.) captured within the selected day. "All documents" link opens a report containing all information collected for the selected user during the whole day.



Administrator
In-built system administrator

Jarman Robbert
HR
robbert.jarman@gmail.com

Mendes Leona
Secretary
leonamendes5@gmail.com

Miller Ted
IT Manager
ted.miller78@gmail.com

White Helen
Purchasing Manager
helenwhite1286@gmail.com

Wilson Katharyn
Corporate Purchasing Manager
katharyn.wilson@gmail.com

01.07.2015 This day's: Mails (4) Conversations (6) Files (4) Urls (19) Screenshots (21) All documents

Date	Mails	Messengers	Files	Web	Other activities
0:00					
1:00					
2:00					
3:00					
4:00					
5:00					
6:00					
7:00					
8:00					
9:00				1 url	3 screenshots 39 minutes activity 174 keys pressed
10:00				2 urls 2 search queries	3 screenshots 10 minutes activity 91 keys pressed
11:00				2 urls	2 screenshots 17 minutes activity 12 keys pressed
12:00					3 screenshots 24 minutes activity 1 minute activity 135 keys pressed
13:00				11 urls	3 screenshots 43 minutes activity 204 keys pressed
14:00	2 mails Sent: 2		1 file 2 files		3 screenshots 26 minutes activity 303 keys pressed
15:00	1 mail Received: 1		1 file 2 files		1 minute activity 4 copies to clipboard 44 keys pressed
16:00	1 mail Sent: 1			3 urls 2 search queries	2 screenshots 9 minutes activity
17:00					2 screenshots 10 minutes activity

Specifying the report period

The user activity can be displayed for different time periods. The following options are available on the period selection toolbar:

Today	To view network activity of a user for the current day, click **Today** on the toolbar of the report window. You will see how many messages, e-mails and other data types were sent or received by the user every hour of the current day.
Past 2 days	To view network activity of a user for the previous and present day, click **Past 2 days** on the toolbar of the report window. You will see how many messages, e-mails and other data types were sent or received by the user every hour of the previous and present days.
Past 7 days	To view network activity of a user for the past 7 day, click **Past 7 days** on the toolbar of the report window. You will see how many messages, e-mails and other data types were sent or received by the user every hour of the specified period of time.
Past 30 days	To view network activity of a user for the past 30 day, click **Past 30 days** on the toolbar of the report window. You will see how many messages, e-mails and other data types were sent or received by the user every hour of the specified period of time.
Date range	To view network activity of a user for a certain period of time, click **Date range** on the toolbar of the report window and either enter the necessary dates range manually or use the drop-down menu by clicking the calendar icon in the right corner of entry boxes. Click **Build report**.

Report refresh

The system database of intercepted data is updated in the real-time mode.

To build report on user activity based on real-time intercepted data click **Refresh** on the toolbar.

Saving a user activity report

There is a possibility to save a currently displaying user activity report to the HTML file. After saving the report data in the HTML format can be opened with a web browser.

To save a report as HTML-file follow the steps below:

1. Click **Save user activity** on the toolbar.

2. There are the list of dates, which were specifying upon report creation, in the newly opened window. The number of documents containing information about the user's activity is indicated next to the date in parentheses. To select the type of the document, which detailed information will be included in a HTML-report, click the drop-down arrows. The checked type documents will be accessible for inspecting from a web browser window.

3. If any type of documents or all the documents of the certain date should not be included in the HTML-report, uncheck them. These data will be displayed in the report but will not be accessible for inspection.

4. Click **Save** to continue.

5. To view HTML-report open it with a web browser.

6. To inspect a document of user activity report click the corresponding interactive link.

6.3.2 Viewing different types of intercepted data

Types of data accessible for review

Different data types of data are presented in the report in the corresponding columns. The information provided in the report is grouped by four main categories: mail messages, instant messenger conversations, transferred files and visited web-resources (see below).

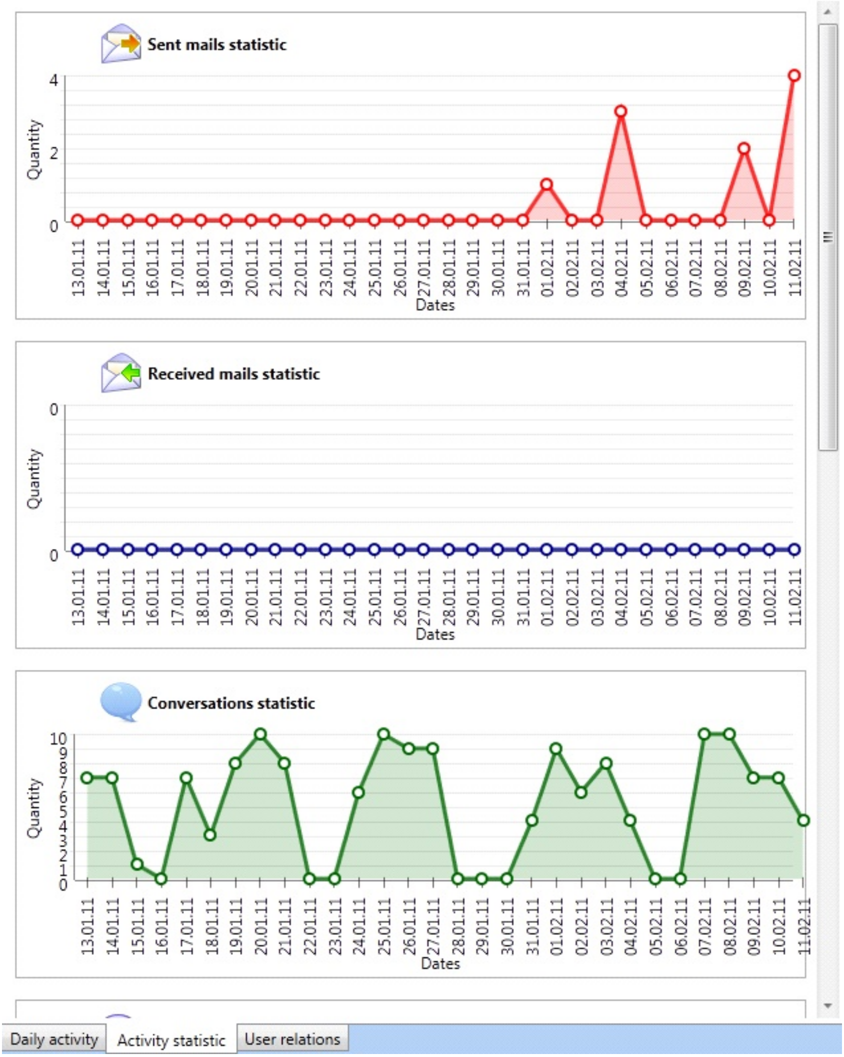
Mails	In this category, the report provides the total number of mail messages hourly for a certain period of time with the number of sent and received mail messages specified. You can both view all the mail messages found and choose to view only sent or received messages. For this, either click the link with the total number of messages, or click the link Sent or Received correspondingly.
Messages	In this category, the report provides the total number of conversations hourly for a certain period of time with the number of messages sent by the current user. You can open and view the found conversations in a new tab.
Files	In this category, the report provides the total number of files sent or received by the current user hourly for a certain period of time. You can open and view the found files in a new tab.
Web	In this category, the report provides the total number of visited web-

	resources or sent requests of the current user hourly for a certain period of time. To view the visited URLs or sent requests, click the link with the corresponding result.
Other	In this category, the report provides the total number of screenshots, computer activity statistic and keylogger data taken at the user’s workstation hourly for a certain period of time. The browser activity? clipboard data as well as devices audit data. To view the type of data you need, click the corresponding link. *Note: the system does not take screenshots if the user’s computer is switched off, locked or a screensaver is active*.

6.3.3 Viewing user’s activity statistics

To view a user’s activity statistics go to the corresponding tab in the lower part of the user activity report window.

The information on the selected user’s network activity in the **Activity statistic** tab is displayed in the form of diagrams.



The following diagrams are displayed in the **Activity statistic** tab:

- **Sent mails statistic** (the diagram displays the number of outgoing e-mails sent by user on every date in the selected time period)
- **Received mails statistic** (the diagram displays the number of incoming e-mails received by user on every date in the selected time period)
- **Conversations statistic** (the diagram displays the number of IM communication sessions the user participated in on every date in the selected time period)

- **Conversation messages statistic** (the diagram displays the number of instant messages sent and received by user on every date in the selected time period)
- **Files statistic** (the diagram displays the number of files sent and received by user as attachments to e-mails or via IMs on every date in the selected time period)
- **URLs statistic** (the diagram displays the number of URLs visited by user on every date in the selected time period)
- **Posts statistic** (the diagram displays the number records posted by user in blogs, forums or social networks or otherwise entered into text fields on web-pages, including search queries, on every date in the selected time period)
- **Printers usage statistic** (the diagram displays the number of printed documents);

- **User activity statistic** (time of user computer activity is shown. The tops of the chart link to detailed information about user activity on the selected day);

- **Web browsers statistic** (the duration of user web activity with help of browsers);

- **Clipboard statistic** (the number of clipboard copy per day);

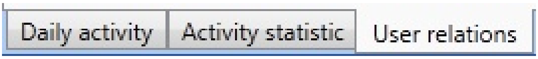
- **Keylogger statistic** (the number of keystrokes per day).

To view detailed information on sent or received e-mails, files, IM conversations, visited web-pages or posted web-queries of the selected user click the diagram point above the corresponding date. A search results window will open with an active filter by the following parameters: **Mail, Messengers, Web** or **Files** (for more information, see *Search results list window toolbar*).

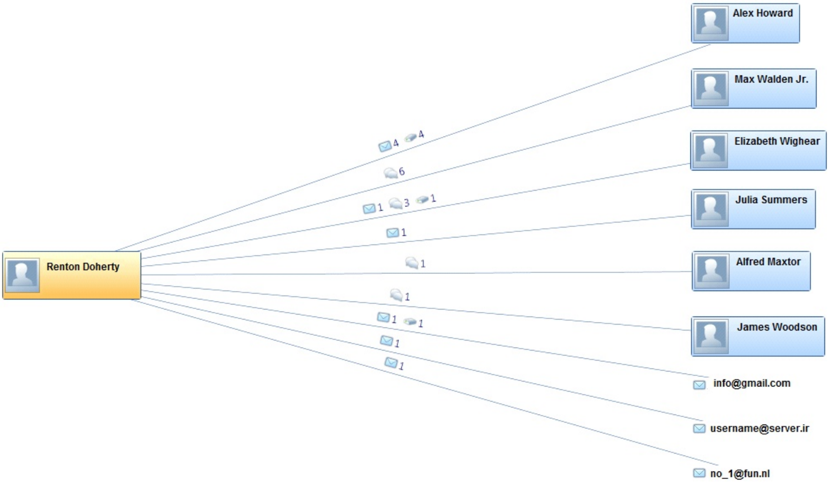
6.3.4 Viewing user relations with Graph-analyzer

To view a user relations Graph-analyzer

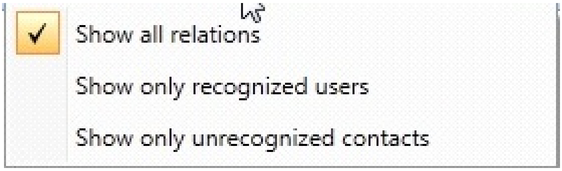
1. Go to the **User relations** tab in the lower part of the user's network activity report window.



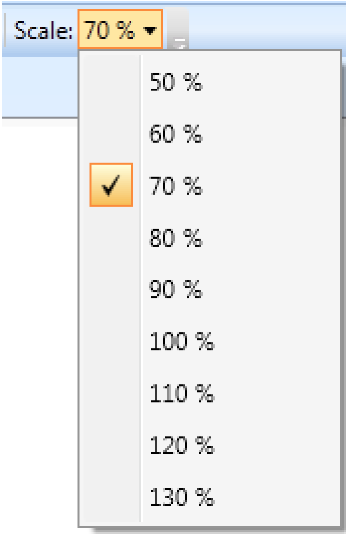
2. All the contact of the selected user will be graphically displayed in the graph form in the window, i.e. all other users person has exchanged e-mails, instant messages and files with.



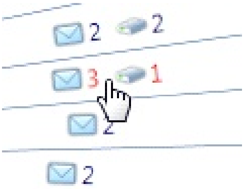
3. All users with relations are displayed as top and branch of the Graph-analyzer – with both recognized and unrecognized contacts by default. To display only the relations with recognized contacts (i.e. with users having user cards and already known to the system), or only with unrecognized contacts, select the corresponding option in the **Show all relations** filter, located in the **User relations** tab toolbar.



4. To change a scale of the Graph-analyzer on the **User relations** tab toolbar, click **Scale** and select a necessary scale value.

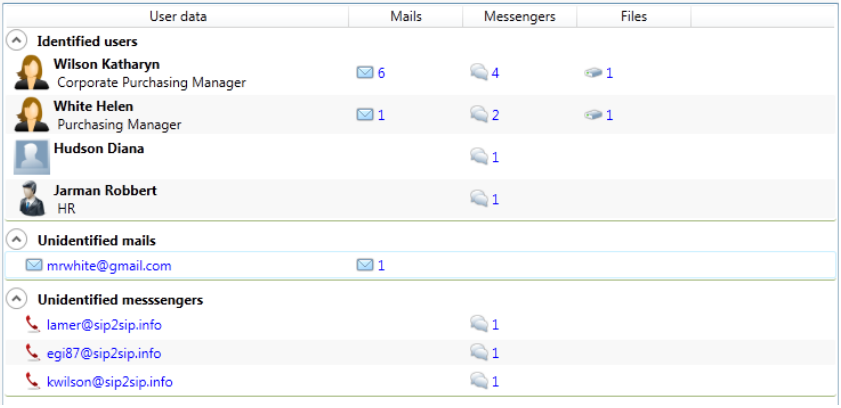


5. Above each relation line in the Graph-analyzer you can see the numbers of e-mails, instant messages and files exchanged by the users within the selected time period. The details of these e-mails, messages and files can be viewed by clicking the figures.



6. To select a mode of relations display select one of the filters from the **Relations view** filter:

- Select the **Table** mode to view a user relations in the table form. Herewith user contacts will be divided on the following groups: recognized contacts from the system user data base; unrecognized messengers contacts; unrecognized mail accounts.



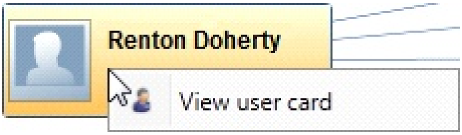
User data	Mails	Messengers	Files
Identified users			
Wilson Katharyn Corporate Purchasing Manager	6	4	1
White Helen Purchasing Manager	1	2	1
Hudson Diana		1	
Jarman Robbert HR		1	
Unidentified mails			
mrwhite@gmail.com	1		
Unidentified messsengers			
lamer@sip2sip.info		1	
egi87@sip2sip.info		1	
kwilson@sip2sip.info		1	

- Select the **Graph** mode to view a user relations in the graph form with recognized and unrecognized contacts in the tops.

The way of contact presentation in the graph form can be set as well - grouped and ungrouped modes are available. To set the presentation way, on the toolbar click the **Group mode** and select the necessary mode. Relationships are displayed in the graph form with the grouped contacts in the tops.

Viewing a local user card

A right-click the central user (the user for whom an analysis of relations was carried out) opens a context menu including the **View user card** option. Click the option to open the user card (for more information, see *User cards*).

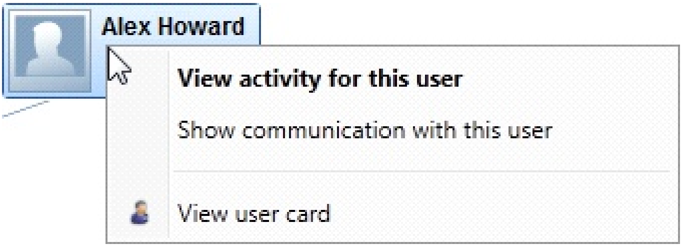


Recognized contact information

A right click on an icon of a recognized contact the selected user has exchanged data with, opens a context menu containing the following options:

- **View activity for this user** – if this option is selected, the program construct a similar graphic analyzer for this user. The same can be done by double clicking such user’s name.
- **Show communications with this user** – clicking on this option opens a **Search results** tab displaying all communications between this user and the central user for whom the Graph-analyzer has been constructed.
- **View user card** – clicking on this option opens the user card of this user (for more

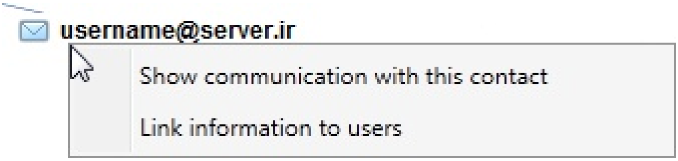
information, see *User cards*).


Alex Howard
View activity for this user
Show communication with this user
View user card

Unrecognized contact information

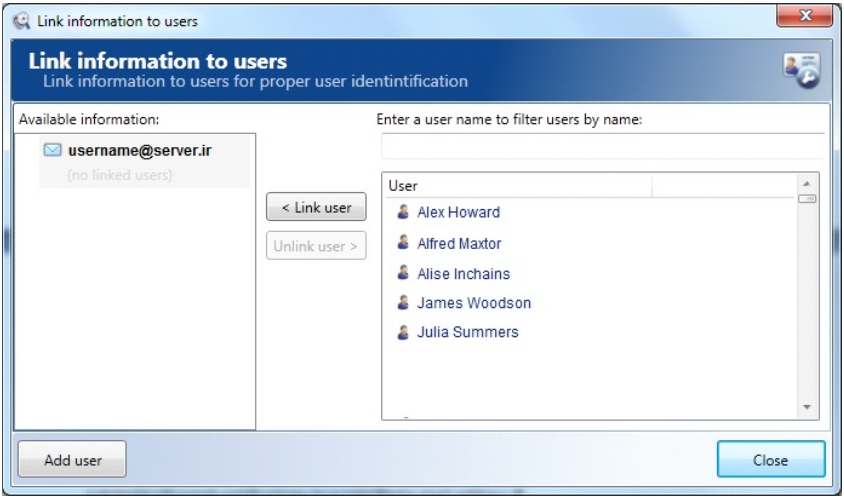
A right click on an icon of an unrecognized contact the selected user has exchanged data with, opens a context menu containing the following options:

- **Show communications with this contact** – clicking on this option opens a **Search results** tab displaying all communications between this contact and the central user.
- **Link information to users** – clicking on this option opens a window in which you can link this contact to one of the existing users or create a new user to link the contact to.

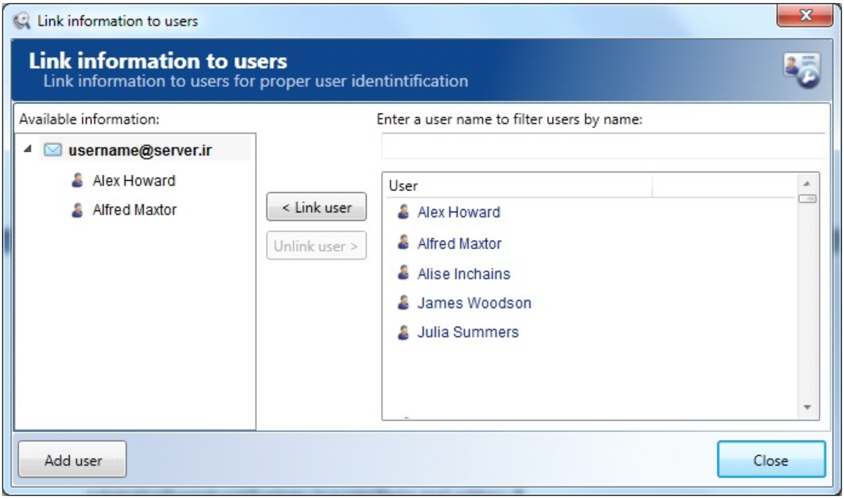

username@server.ir
Show communication with this contact
Link information to users

Linking information to users

1. In the left area of the **Link information to users** window an unrecognized contact is displayed. It can be linked to one of the existing users from the list in the right area of the window.



2. In case you know that the selected unrecognized contact belongs to one of the existing users of your network, highlight that user’s name in the list and click **Link user**. If the contact is used by more than one user, you can link it to several users. The names of all users the contact has been linked to will be displayed in the left part of the window.



3. To unlink the contact from the linked users, click the name of the user in the left part of the window and click **Unlink user**. This will delete existed link and remove the user’s name from the left list.

Search among the existing users

1. To perform a search among the existing users, enter the letters which a searched user name contains into the search box above the right list of users.

Enter a user name to filter users by name:

2. To create a new user click **Add user**. After the user card is filled out (refer to *User cards*) the name of the new user will appear in the list in the right part of the window. The order of linking the new user is the same as described *above*.
3. To close the contact linking window, click **Close**.

Saving relationship report

Save procedure is available only for the reports in the graph form.

To save report in the graph form to the PNG file set the graph mode as was described above and click **Save user activity** on the toolbar. Specify a save location in the dialog window and click **Save** to finish.

7 Security Center Management

Security Center inspects every packet flowing across a network and sending an alert when prohibited by security policy data is found . The intercepted data are analyzed in an automatic mode based on an assigned list of security rules. If any documents or information satisfying the requirements listed in security rules are detected, the Center automatically sends alert notifications to a specified e-mail address.

SecureTower automatically extracts and analyzes text data from files transmitted in the network. Please refer to *Annex* for a complete list of file formats available for full-text search in **SecureTower**.

Client console is used for configuring the Security Center and for assigning security policy rules.

The structure of the security policy can be hierarchical and can involve classifying the rules by various groups depending on a security aspect that these rules are to cover. For example, a separate group of rules can be created for a security officer who is responsible for legal issues, or for the one responsible for financial data control, etc. You can drag&drop security rules between groups. One can specify e-mail addresses of the relevant security officer for each group, and, thus, each security officer will be receiving notifications on breaches associated with the specific security aspect they are responsible for.

The system also enables configuring the set of complex search conditions subject to which traffic analysis is to be conducted. For example, automatic data analysis rules can be provided for sending notifications about actions of a certain user or about an outgoing message to a certain e-mail address.

Security Center

Different types of security rules configuration, security breach alerts setting and review

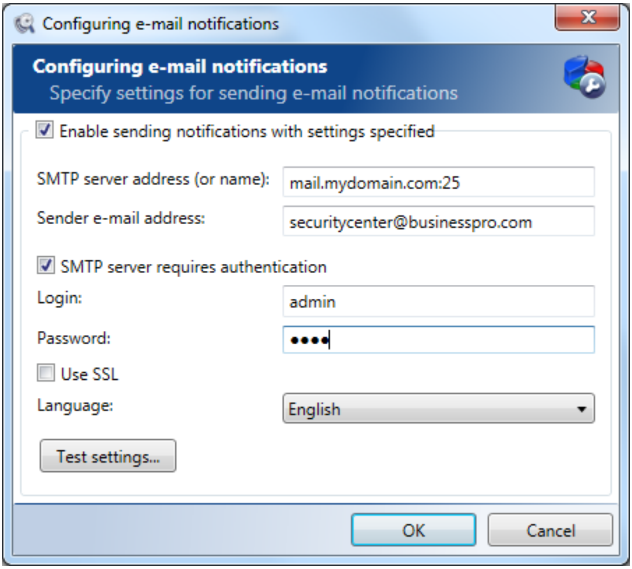
To start work with security rules and alerts click in the **Security Center** area on the program start page or click **Security Center** on the program toolbar.

7.1 Configuring security notifications delivery

SMTP server parameters

1. To configure notification delivery parameters, click **Settings** on the Security Center toolbar.

2. In the **SMTP server address** text box of **Setting up e-mail notifications** window, enter the IP address or name of the server that will be used for sending e-mail security 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*. The name of the server may be specified in the *server:port* format.



Configuring e-mail notifications

Configuring e-mail notifications

Specify settings for sending e-mail notifications

☑ Enable sending notifications with settings specified

SMTP server address (or name): mail.mydomain.com:25

Sender e-mail address: securitycenter@businesspro.com

☑ SMTP server requires authentication

Login: admin

Password: ●●●●

☐ Use SSL

Language: English

3. In the **Sender e-mail address** text box, enter the e-mail address that will be used for sending security notifications.

4. If SMTP server connection authorization is necessary to use, select the **SMTP server requires authentication** check box and specify the user name (login) and password of the e-mail box that will be used for sending security notifications .

Note: *User name and password should be specified only if the SMTP server requires authorization. Otherwise, these fields may 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. To apply this specify the user name that the system notification service will be running under and assign the required mail server access rights in the Windows Services section.*

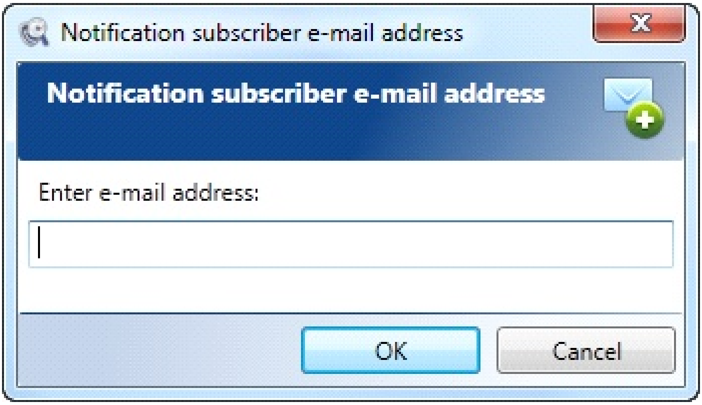
5. If encrypted connection is necessary to use, select the **Use SSL** check box.

6. Select the language of notification in the corresponding list box.
7. To check out if the notification settings are configured properly, click **Test settings**. In case of a successful test completion, a test message will be sent to the specified e-mail address.
8. To save the settings entered, click **OK**. To discard the changes, click **Cancel**.

Add a new subscriber

To add a new subscriber for security notifications delivery:

1. Click **Add subscriber** in the **Add security rule** window,


Notification subscriber e-mail address
Notification subscriber e-mail address
Enter e-mail address:
OK
Cancel

2. Enter the e-mail address in the dialog box and click **OK**.
3. To activate the brief report form select the **Send a brief report** check box.

Displaying the notifications in mail client interface

The reports with notifications that is sent by the Security Center in accordance to preset schedule contains data about security rules went off.

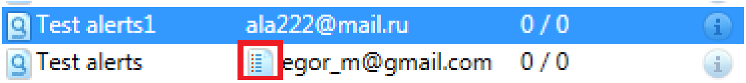
The alerts in the report are grouped by rules names and sorted by protocols. All records in the report are interactive links to the corresponding notifications in the Client console if it was installed on the local computer.

Note: *In some cases the links to security incidents become inactive. The possible reason is the mail applications with built-in active content blocking is used for mail receiving (f.e. gmail web interface).*

The possibility of choice between full and brief report versions is provided. A full report contains the full list of links to incidents, otherwise a brief one contains the number of incidents for each rule without links (it's can be useful when the big number of incidents is expected).

To activate the brief report form check the **Send a brief report** check box upon the rule or group of rules properties configuring (for more information, see *Creating a group of security rules* and *General security rule*).

Rules or groups for which the brief report was assigned will be marked in the list of Security Center rules with the corresponding symbol.



Test alerts1	ala222@mail.ru	0 / 0	ℹ
Test alerts	egor_m@gmail.com	0 / 0	ℹ

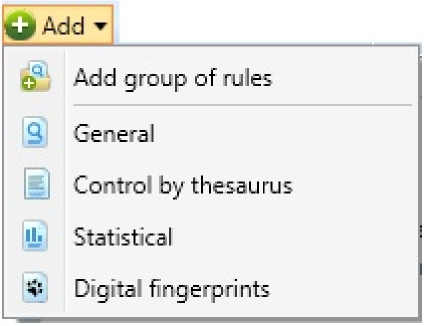
7.2 Assigning a security policy

In the **Manage Security Center** window, the list of security rules groups is displayed. By default, the FalconGaze **SecureTower** Security Center **Group of rules** is assigned as core group. Within this group, one can create other groups of rules or just create rules only if there is no need in managing groups of rules. The default group cannot be deleted. Also, if some e-mail address is specified in the settings of this group, notifications will be sent to the specified address for all the security rules and security rule groups that this group includes.

Information displayed in a table for each group of rules and rules includes the group **Name**, the list of **Subscribers** (e-mail addresses to which notifications are sent), **Incidents**, **Status** of search process and item **Description**.

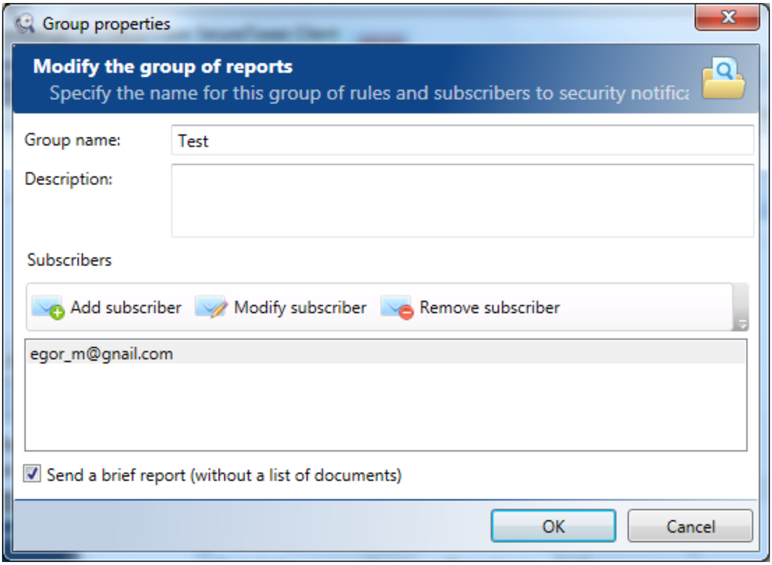
7.2.1 Creating a group of security rules

1. To create a new group of rules, in the **Add** drop-down menu of the **Manage Security Center** window ribbon toolbar click the **Add group of rules** option.



The corresponding option from an existed group/rule context menu may be used as well.

2. 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.



Group properties

Modify the group of reports

Specify the name for this group of rules and subscribers to security notific

Group name: Test

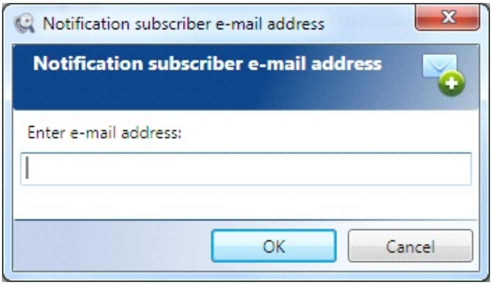
Description:

Subscribers

egor_m@gnail.com

☑ Send a brief report (without a list of documents)

3. To specify the e-mail address (or addresses) to which security breach notifications will be sent, click **Add subscriber** and enter the corresponding e-mail address in a new dialogue window. Click **OK**. To discard adding the subscriber, click **Cancel**.



Notification subscriber e-mail address

Notification subscriber e-mail address

Enter e-mail address:

4. To modify some e-mail address to which security breach notifications are to be sent, click **Modify subscriber** and make the necessary changes to the e-mail address in the opened dialogue window. Click **OK**. To discard the changes, click **Cancel**.

5. To exclude some e-mail address from the list of notification subscribers, click **Remove subscriber** and click **Yes** in the action confirmation dialogue window. To cancel the action, click **No**.

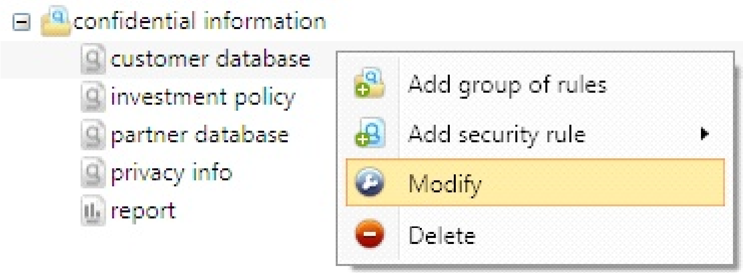
6. To activate the brief report form select the **Send a brief report** check box. The setting will be applied for all nested items.

7. 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 security rules in the **Manage Security Center** window.

7.2.2 Modifying a group of security rules

1. To modify a certain group of security rules, select the necessary group and click Modify in the **Manage Security Center** toolbar or click this command on the context menu opened by right-clicking the necessary group. The group settings window can also be opened by double-clicking the necessary group.



2. In the opened dialogue window, make the necessary changes as described in *Creating a group of Security rules* and click **OK**.

7.2.3 Deleting a group of security rules

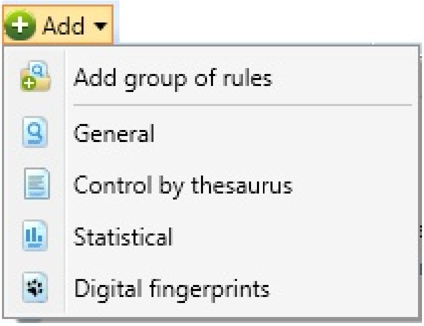
1. To delete a group of rules, select the necessary group and click Delete in the **Manage Security Center** toolbar or select this command in the context menu opened by right-clicking the necessary group.

2. In the action confirmation dialogue window, click **Yes**. To cancel the action, click b.

7.2.4 Assigning a security rule

1. To create a security rule, select the group this rule will be related to.

2. Click the **Add** ribbon toolbar menu of the **Manage Security Center** window. In the drop-down menu, select the type of a security rule – **General**, **Control by thesaurus, Statistical** or **Digital fingerprints**.



3. Security rule will operate as alerts with specified parameters.

A general security rule notifies about activities of a certain user, IP address, or involving specific text, etc.

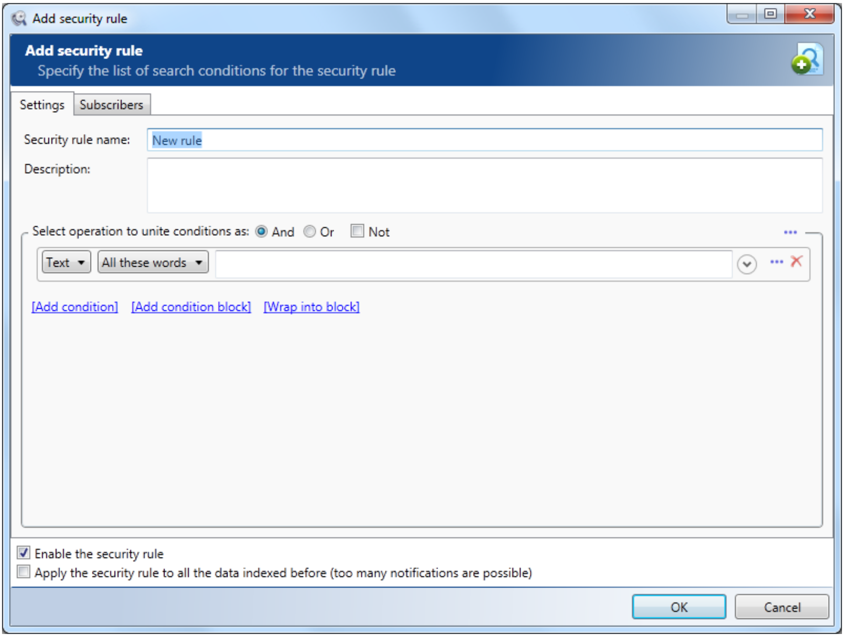
Security policies based on control by thesaurus are used for automatic detection of words and expressions included in specific subject thesaurus.

A statistical rule is used to notify of certain network activities the number of which is above or below the specified number over a term per user or per network. For example, the security department can receive notifications of chat conversations if there have been more than 10 IM-conversations per user within a business day, or of e-mail messages if there have been less than 5 messages per user within 4 hours (for a company that actively employs direct mail marketing).

A digital fingerprints security rule enables configuring notifications in case any matches are detected between a classified document for which a digital fingerprint has been created, and any data transmitted by users.

7.2.4.1 General security rule

1. If you have selected a general security rule, a dialog window will open in which you are to specify the name of the new security rule in the **Security rule name** text box and fill out the **Description** text box (optionally).



Security rule name: New rule

Description:

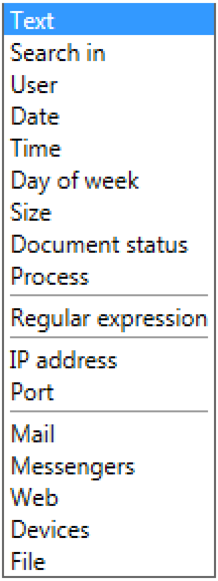
Select operation to unite conditions as: ● And ○ Or □ Not

☑ Enable the security rule

□ Apply the security rule to all the data indexed before (too many notifications are possible)

2. In the section under the **Description** text box specify the conditions for the search that will be conducted by the **Security Server** in an automatic mode.

Data can be searched by a certain text or a regular expression in the intercepted data, IP address (as well as local or remote), by the specified port (as well as local or remote), by a user name, by the size of data, by the type of data and by the interception date. Condition types are available in the drop-down list opened by clicking **Text** .



For various search conditions different relevant operations can be specified (for more information, see *Search request creation*).

3. To apply the newly created rule, select the **Enable the security rule** check box under the search condition entry window. To disable the rule temporarily without canceling the settings, clear this option.

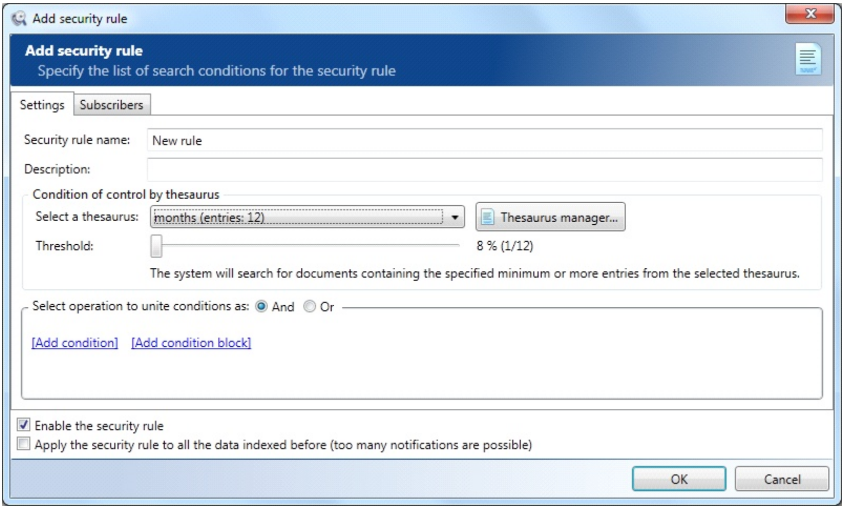
4. If it is important to receive notifications on the created rule based on the analysis of all the data in the index, check the **Apply rule to all the data indexed before** option. With this option enabled, the **Security Center** will search through all the data contained in the index and will provide notifications for past periods. If this rule can be applied only for newly intercepted (and indexed) data, clear the corresponding check box. *The option is available only upon creating a new security rule.*

5. To save the settings entered, click **OK**.

6. Go to the **Subscribers** tab to specify the e-mail addresses a notification will be sent to in case of breach of the security rule (see below).

7.2.4.2 Control by thesaurus

Security policies based on control by thesaurus are used for automatic detection of words and expressions included in specific subject thesaurus. When you select option **Control by thesaurus** from the **Add** menu, a new window will open where you have to specify security rule conditions.



Add security rule

Add security rule
Specify the list of search conditions for the security rule

Settings | Subscribers

Security rule name: New rule
Description:

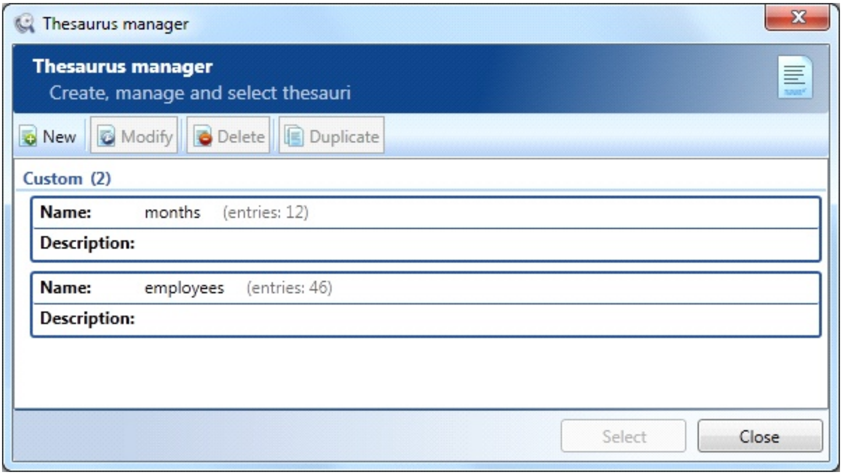
Condition of control by thesaurus
Select a thesaurus: months (entries: 12)

Threshold: 8 % (1/12)
The system will search for documents containing the specified minimum or more entries from the selected thesaurus.

Select operation to unite conditions as: ● And ○ Or

☑ Enable the security rule
□ Apply the security rule to all the data indexed before (too many notifications are possible)

1. Select one of the subject thesauri in the drop-down list. There are several default thesauri created in the system. If you wish to view/edit existing thesauri or add new ones, click **Thesaurus manager**.



Thesaurus manager

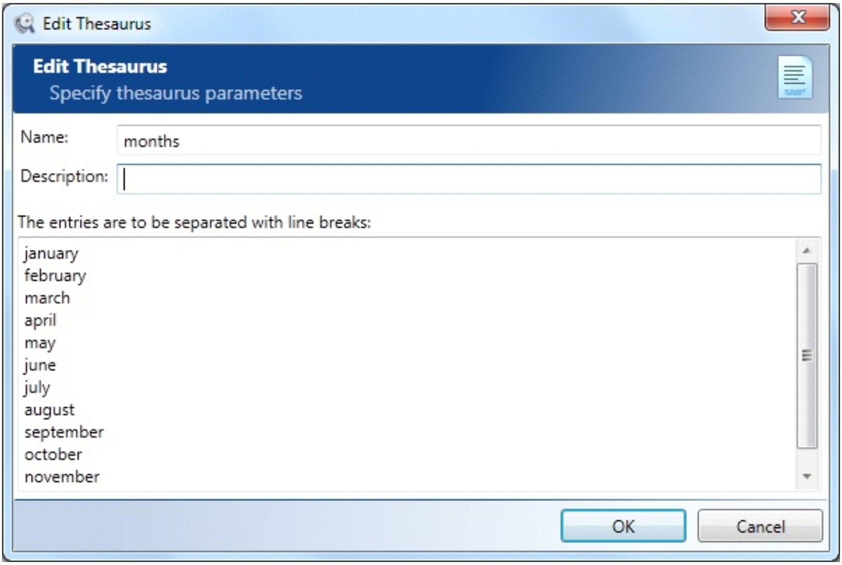
Thesaurus manager
Create, manage and select thesauri

Custom (2)

Name: months (entries: 12)
Description:

Name: employees (entries: 46)
Description:

- To view/edit an existing thesaurus, highlight its name and click **Modify**.



Edit Thesaurus

Specify thesaurus parameters

Name: months

Description:

The entries are to be separated with line breaks:

january
february
march
april
may
june
july
august
september
october
november

A window will open containing a list of all entries in the selected thesaurus. You can add words or expressions into the thesaurus. All entries have to be separated by line breaks. Once you have finished editing the list of words and expressions, click **OK** to save or **Cancel** to discard your changes.

To create a new thesaurus, click **Add new** in the thesaurus manager window. To delete one of the existing thesauri, highlight its name and click **Delete**. If you wish to create a new thesaurus based on an existing one, highlight the name of the existing thesaurus and click **Duplicate**. A thesaurus creation window will open containing all entries from the duplicated thesaurus. Edit the entries as needed, specify a name for the new thesaurus and click **OK**.

2. Set the threshold for the security rule. Moving the slide bar, select a number of entries to be detected by the system. **SecureTower** will trigger an alert only when it detects the specified number of entries from the selected thesaurus within one intercepted document. *For example, if you select thesaurus "Months" and set threshold slide bar to the leftmost position, the system will trigger an alert every time it detects any name of the months in the traffic flow. Set the slide bar to the rightmost position to trigger alerts only when all 12 names of months are detected within one document*.

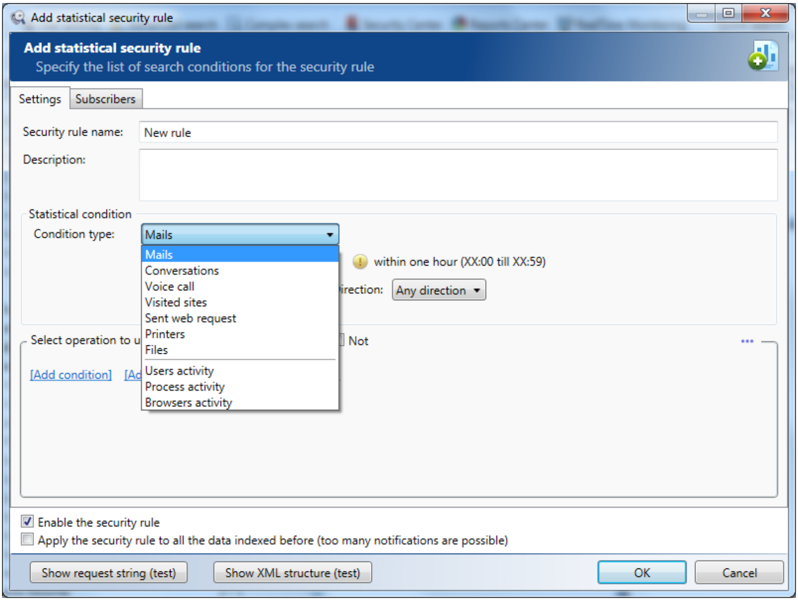
3. Further limiting conditions for this security rule similar to the ones used in **General security rules** may be added as well (refer to *General security rule*.).

7.2.4.3 Statistical security rule

Statistical security rules can be used to automatically monitoring activity of the local users in different communication channels.

To create a rule, you have to specify the statistical conditions in the section under the **Description** text box:

1. On the **Condition type** menu, select the type of a network event based on which you need to receive security notifications. The system enables automatic counting of emails, IM conversations and number of messages within a conversation, IM voice calls, number of visited web sites, sent web request, number of printed documents and pages, number of files. Beside this, it's possible to calculate the users and processes activity time.



Add statistical security rule

Add statistical security rule

Specify the list of search conditions for the security rule

Security rule name: New rule

Description:

Statistical condition

Condition type: Mails

within one hour (XX:00 till XX:59)

irection: Any direction

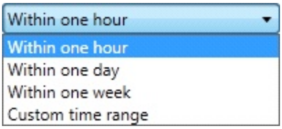
Select operation to u

Not

☑ Enable the security rule

□ Apply the security rule to all the data indexed before (too many notifications are possible)

2. Having selected the event type, select the term the specified type of users activity should be counted within on the term menu below.

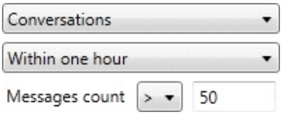


- within one hour (events of selected type will be counted within full hour, for example, 9:00 till 10:00, 10:00 till 11:00, etc.);
- within one day (events of selected type will be counted within full calendar days, i.e. from 0:00 am till 11:59 pm every day);
- within one week (events of selected type will be counted within full calendar

weeks, i.e. from 0:00 am Monday till 11:59 pm Sunday);

- Custom (user defined) time range (events of selected type will be counted within specified period, i.e. 9 am till 6 pm every day. The data of the last hour will be ignored).

3. Specify the subtype of network events (if necessary) and their number (i.e. the number of e-mails, messages, visited sites, exchanged files, etc.) to trigger the security rule, and one of the logical parameters (>, <, =). In the example shown below the security rule will trigger an alert if any user exchanges more than 50 messages in any IM within one hour.



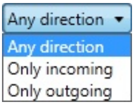
Conversations

Within one hour

Messages count > 50

4. In accordance to the selected activity type the different precise conditions can be set:

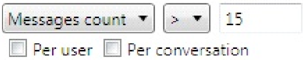
- For certain types of activity (mail, messages, calls and files) a direction can be set, i.e. the system can count only incoming, only outgoing or any data regardless of the direction.



Any direction

- Select the **Per user** check box if it's necessary to apply the specified conditions on a per-user basis. Clear it, if conditions should be applied to the entire network.

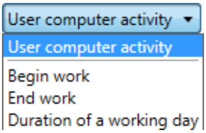
- If the **Conversations** type of condition for statistic notifications was selected, the search parameters you entered may be applied for each conversation. For this, select the **Per conversation** option.



Messages count > 15

□ Per user □ Per conversation

- If the **Users activity** condition is selected the following precise conditions are available:



User computer activity

- User computer activity (the active work or idle PC time);

- Begin work (the notification will be triggered if the first user activity was detected earlier or later than a specified value);

- End work (the notification will be triggered if the last user activity was detected earlier or later than a specified value);

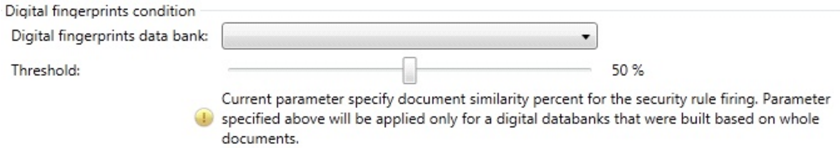
- Duration of a working day (the notification will be triggered if the total user activity time is bigger or smaller than a specified value).

- If the **Process activity** condition is selected specify the time interval to keep statistic, a process state and a triggered parameters in absolute or relative units.

5. All other conditions sections of the window are filled out as described in *General security rule*.

7.2.4.4 Search rule by digital fingerprints

If a search rule by digital fingerprints was selected , one have to fill out the Digital fingerprints condition section located below the **Description** text box.



Digital fingerprints condition

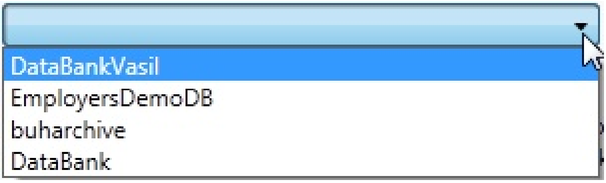
Digital fingerprints data bank:

Threshold: 50 %

Current parameter specify document similarity percent for the security rule firing. Parameter specified above will be applied only for a digital databanks that were built based on whole documents.

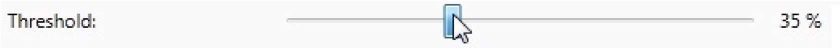
1. Click the **Digital fingerprints data bank** arrow and select the data bank with the fingerprints of the classified documents you wish to control.

Note: *For instructions on creating a data bank of digital fingerprints, please refer to the **SecureTower** Administrator Guide (**Creating Data Banks**)*



DataBankVasil
EmployersDemoDB
buharchive
DataBank

2. Move the **Threshold** slider bar with your mouse to set the percentage of matches between classified documents and documents transmitted by users, which will trigger the security policy breach alert.

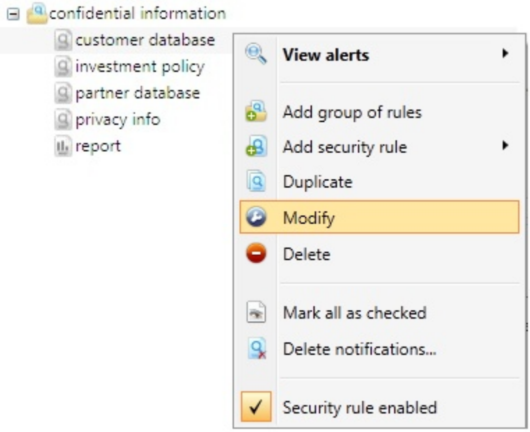


Threshold: 35 %

3. All other sections of the window are filled out as described in *General security rule*.

7.2.5 Modifying a security rule

1. To modify a certain security rule, select the necessary rule and click **Modify** in the **Manage Security Center** ribbon toolbar or select this command in the context menu opened by right-clicking the necessary rule.



The security rule settings window can also be opened by double-clicking the necessary rule.

2. In the opened dialogue window, make the necessary changes in accordance with the instructions provided in *Assigning a security rule* and click **OK**.

7.2.6 Deleting a security rule

1. To delete a security rule, select the necessary rule and click **Delete** in the **Manage Security Center** ribbon toolbar or select this command in the context menu opened by right-clicking the necessary rule.
2. In the action confirmation dialogue window, click **Yes**. To cancel the action, click **No**.

7.3 Security notifications review

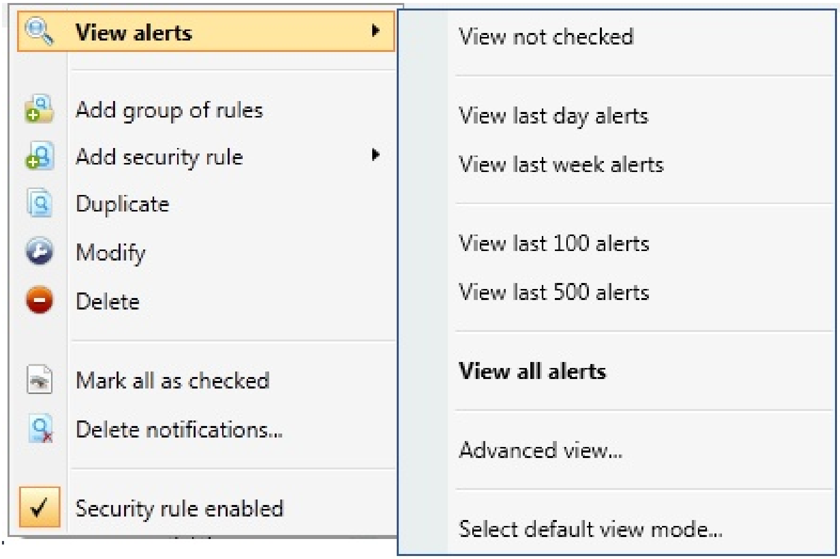
There are two ways to view the **Security Center** notifications: in the Manage Security Center window of the Client console and with an email client software.

7.3.1 Viewing notifications in Security Center

In the right pane of the **Manage Security Center** window, you can see all the notifications on the existing security rules. To view notifications, double-click the security rule.

Note: *By default, only the notifications generated on the current day will be displayed. In case no notifications were generated during the current calendar day, nothing will be displayed upon a double click. Please note, that in this case the date of notification is taken into consideration, and not the date when the notification-triggering data was intercepted. Thus, if you, for example, create a new security rule and activate the option to apply it to all previously intercepted data* (for more information, see *General security rule for details), all notification generated by this security rule will be accompanied by the date rule creation.*

To view other notifications, right-click the security rule and point to **View alerts** option in the context menu. The context menu includes the following options: **view last day alerts** (default options), **view last week alerts**, **view last 100 and 500 alerts**, **view all alerts** and **advanced view.** The **Select default view mode** options is also available.



To mark all notification of selected rule as inspected already select the **Mark all as checked** option**.**

Specifying personal options for alert viewing

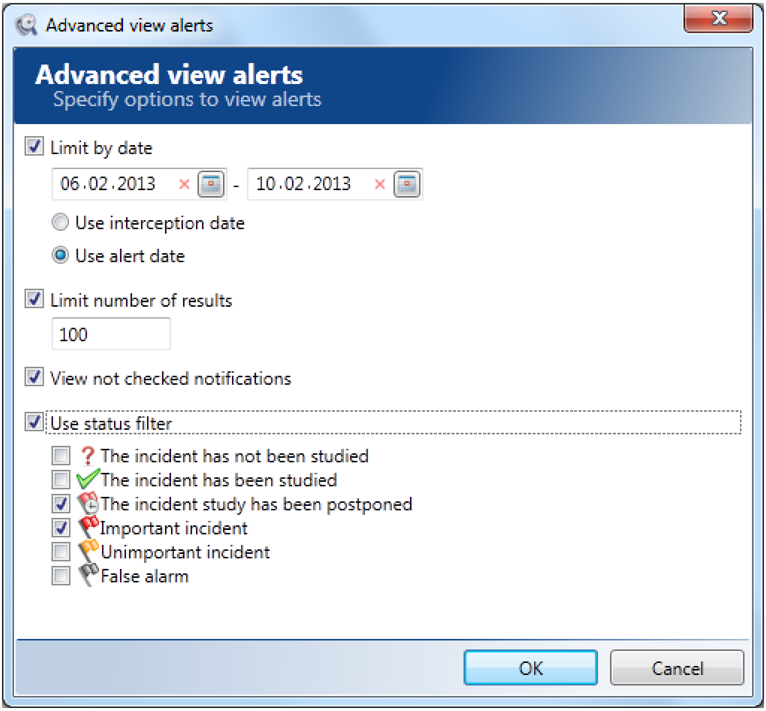
To specify personal options for alert viewing select the **Advanced view** option:

In the **Alert date** field you can specify the range of dates to display alerts for.

You can also limit the number of notifications to display by typing a number in the corresponding field.

To view new not studied notification only check corresponding option.

To apply a status filter to notification list check corresponding option and choose status of incidents you need to be displayed .


Advanced view alerts

Advanced view alerts
Specify options to view alerts

☑ Limit by date

06.02.2013 - 10.02.2013

○ Use interception date

● Use alert date

☑ Limit number of results

100

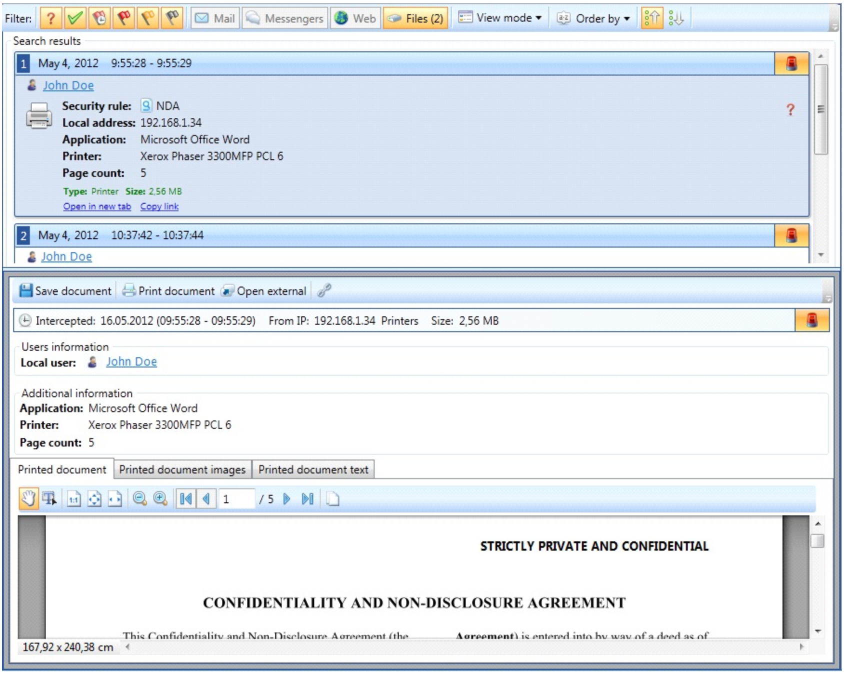
☑ View not checked notifications

☑ Use status filter

□ The incident has not been studied
□ The incident has been studied
☑ The incident study has been postponed
☑ Important incident
□ Unimportant incident
□ False alarm

The example from figure above displays alerts for the corresponding security rule for the period from February 6 to 10, 2013, but limit their number to 100 items. Thus, if there were more than 100 alerts for this security rule in this period, the system will only display the last 100 of them. Also displayed notifications will have checked status.

When viewing notifications in the Security Center, all cases of selected rule triggering will be displayed in a list in the upper right part of the window. When you select a notification in the list, the data that triggered the security rule will be displayed in the lower right part of the window.



1 May 4, 2012 9:55:28 - 9:55:29
John Doe
Security rule: NDA
Local address: 192.168.1.34
Application: Microsoft Office Word
Printer: Xerox Phaser 3300MFP PCL 6
Page count: 5
Type: Printer **Size:** 2,56 MB
Open in new tab Copy link

2 May 4, 2012 10:37:42 - 10:37:44
John Doe

Intercepted: 16.05.2012 (09:55:28 - 09:55:29) From IP: 192.168.1.34 Printers Size: 2,56 MB

Users information
Local user: John Doe

Additional information
Application: Microsoft Office Word
Printer: Xerox Phaser 3300MFP PCL 6
Page count: 5

STRICTLY PRIVATE AND CONFIDENTIAL

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

This Confidentiality and Non-Disclosure Agreement (the Agreement) is entered into by way of a deed as of

167,92 x 240,38 cm

The upper toolbar of the notifications window provides several options for notification filtering and display.

Filtering status of the incident

? - incident has not been investigated

✓ - incident has been investigated

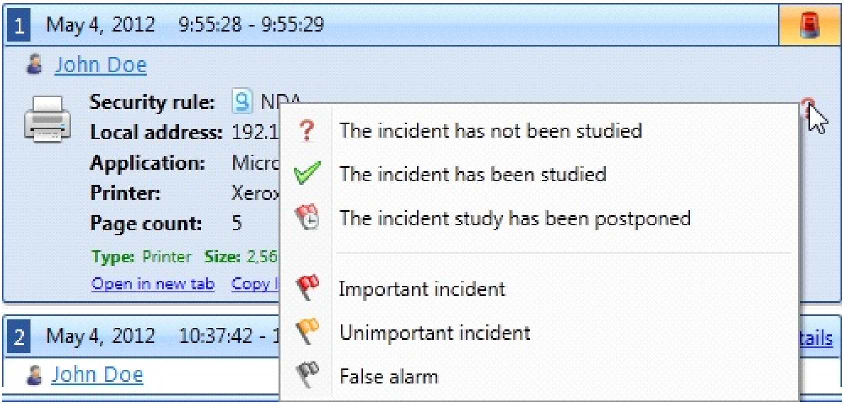
⏲ - incident investigation has been postponed

⚑ - important incident

⚑ - unimportant incident

⚑ - false positive

***Note:** Incident status is set manually by the user by assigning an appropriate flag in the notification card (using a context menu).*



1 May 4, 2012 9:55:28 - 9:55:29

John Doe

Security rule: NDA

Local address: 192.1

Application: Micro

Printer: Xerox

Page count: 5

Type: Printer Size: 2,56

2 May 4, 2012 10:37:42 - 1

John Doe

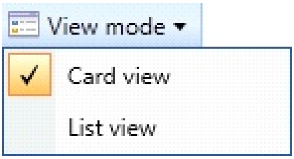
Open in new tab
Copy l
The incident has not been studied
The incident has been studied
The incident study has been postponed
Important incident
Unimportant incident
False alarm
tails

Data type (Email, Messengers, Web traffic, Files) filtering

By default, all notifications will be displayed that are available for the security rule. To filter the list, click specific data types to deactivate them.

Selecting a view mode

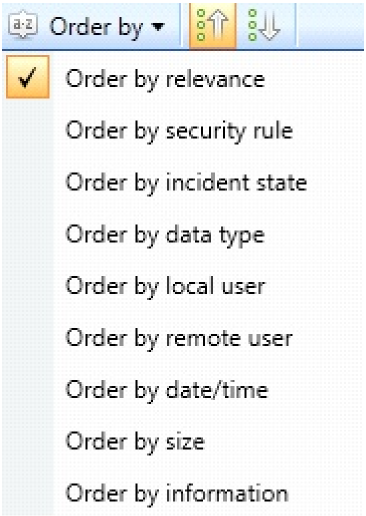
You can select one of the two view modes in the notification area ribbon toolbar:



- **Card view** (displaying all notification as cards containing detailed information on the notification: date and time of notification, local user, name of the security rule, as well as additional information subject to the type of intercepted data)
- **List view** (displaying all notifications as a list containing basic information: name of the security rule, names of the local and remote users, date, time and some other information)

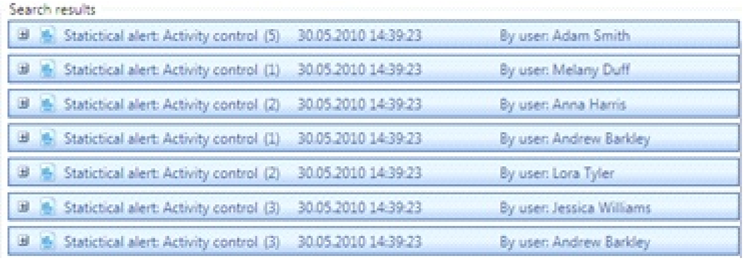
Sorting notifications

In the notification area ribbon toolbar you can also select a notification sorting parameter and direction (descending or ascending).



Statistic security rules notifications

When viewing notifications of statistic security rules, you can expand/collapse the list of results for each notification by clicking a corresponding icon **“+” / ”-“**.



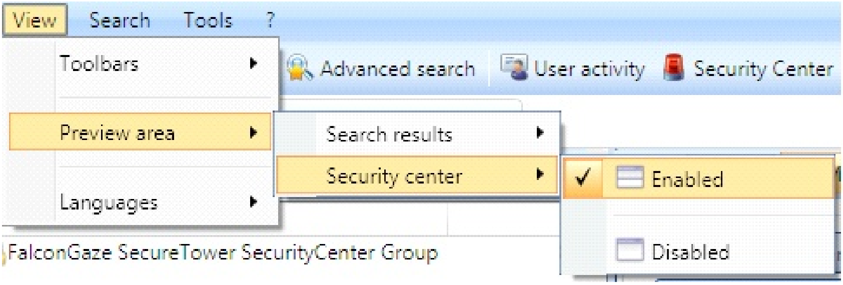
Search results

Statictical alert: Activity control (5)	30.05.2010 14:39:23	By user: Adam Smith
Statictical alert: Activity control (1)	30.05.2010 14:39:23	By user: Melany Duff
Statictical alert: Activity control (2)	30.05.2010 14:39:23	By user: Anna Harris
Statictical alert: Activity control (1)	30.05.2010 14:39:23	By user: Andrew Barkley
Statictical alert: Activity control (2)	30.05.2010 14:39:23	By user: Lora Tyler
Statictical alert: Activity control (3)	30.05.2010 14:39:23	By user: Jessica Williams
Statictical alert: Activity control (3)	30.05.2010 14:39:23	By user: Andrew Barkley

Preview

Preview for the results is also available. To adjust their settings, on the program toolbar click the **View** menu.

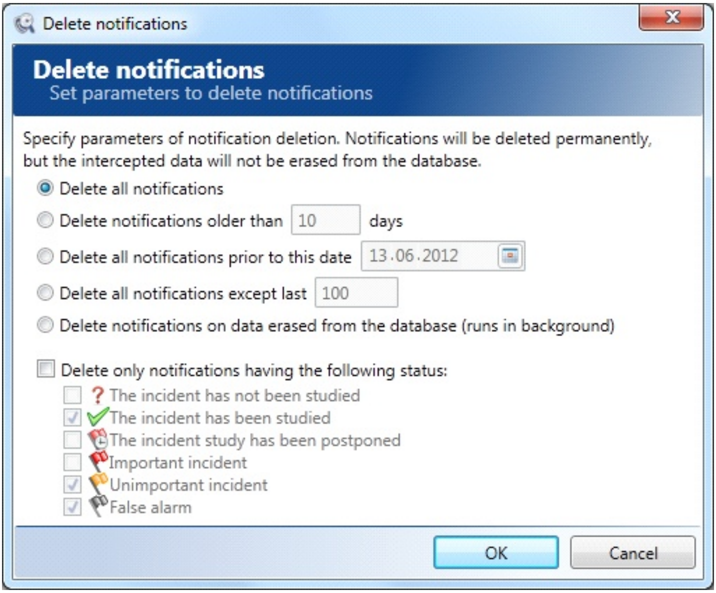
On the **View** menu, point to **Preview area**, then point to **Security Center** and finally click the necessary preview mode.



See also *Search results list* to find more information about available options for the Security Center results.

7.3.2 Deleting notifications

1. To delete notifications generated by certain security rules, right-click the rule and select **Delete notifications** option in the context menu or select corresponding tool from the **Tools** drop-down menu (**The Manage Security Center ribbon toolbar**).



Delete notifications

Delete notifications
Set parameters to delete notifications

Specify parameters of notification deletion. Notifications will be deleted permanently, but the intercepted data will not be erased from the database.

● Delete all notifications

○ Delete notifications older than 10 days

○ Delete all notifications prior to this date 13.06.2012

○ Delete all notifications except last 100

○ Delete notifications on data erased from the database (runs in background)

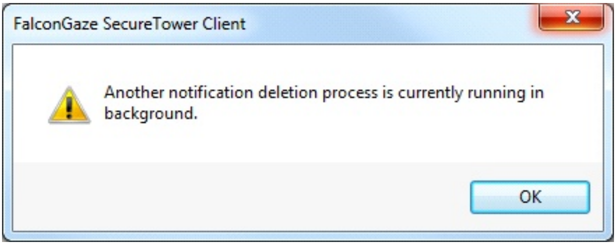
□ Delete only notifications having the following status:

- □ The incident has not been studied
- ☑ The incident has been studied
- □ The incident study has been postponed
- □ Important incident
- ☑ Unimportant incident
- ☑ False alarm

In the new window you can select one of the following options:

- **Delete all notifications**
- **Delete notifications older than** … days (only the notifications generated during the specified number of previous days will remain)
- **Delete all notifications prior to this date** (only the notifications generated on the specified day or later will remain)

- **Delete all notifications except last …** (only the specified number of most recent notifications will remain)
- **Delete notifications on data erased from the database** (this option deletes notifications generated by intercepted data that have already been purged from the database – for example, as a result of a regular planned database cleanup). This operation runs in background, and until it is completed, other notification deletion operations cannot be started. If a user attempts to start another similar operation before completion of the one running in background, the following warning will be displayed:



FalconGaze SecureTower Client

Another notification deletion process is currently running in background.

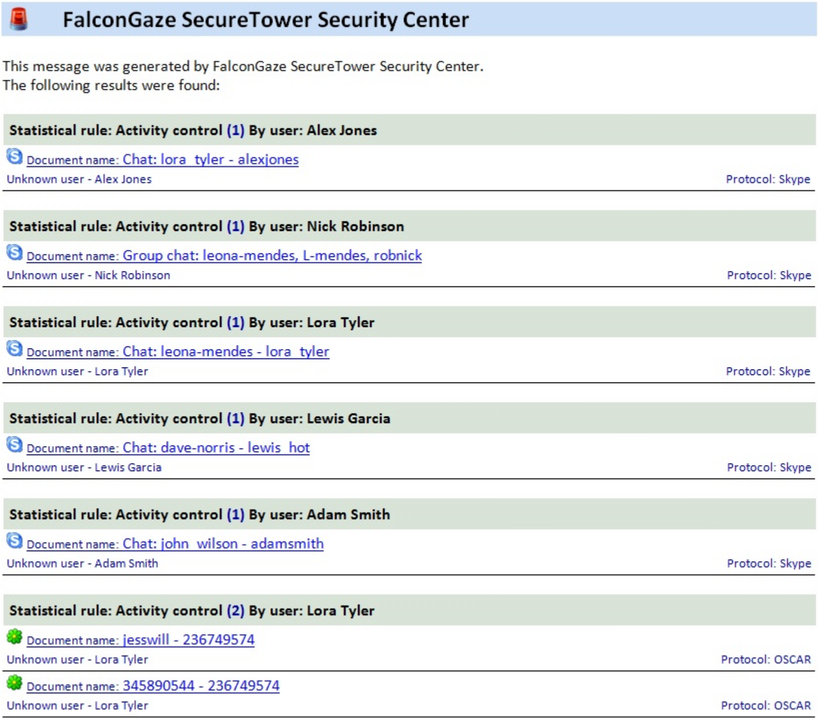
2. To start a new notification deletion operation, you have to wait for the completion of the background process.

   For all of the above deletion options (except for deletion of notifications on data erased from the DB) you can set one or several additional parameters to delete only the notifications having specific statuses:

- **Incident has not been studied**
- **Incident has been studied**
- **Incident study has been postponed**
- **Important incident**
- **Unimportant incident**
- **False alarm**

3. After you have selected the deletion options, click **OK** to start the process.

7.3.3 Viewing notifications with an email client software



FalconGaze SecureTower Security Center

This message was generated by FalconGaze SecureTower Security Center.
The following results were found:

Statistical rule: Activity control (1) By user: Alex Jones

Document name: Chat: lora_tyler - alexjones
Unknown user - Alex Jones — Protocol: Skype

Statistical rule: Activity control (1) By user: Nick Robinson

Document name: Group chat: leona-mendes, L-mendes, robnick
Unknown user - Nick Robinson — Protocol: Skype

Statistical rule: Activity control (1) By user: Lora Tyler

Document name: Chat: leona-mendes - lora_tyler
Unknown user - Lora Tyler — Protocol: Skype

Statistical rule: Activity control (1) By user: Lewis Garcia

Document name: Chat: dave-norris - lewis_hot
Unknown user - Lewis Garcia — Protocol: Skype

Statistical rule: Activity control (1) By user: Adam Smith

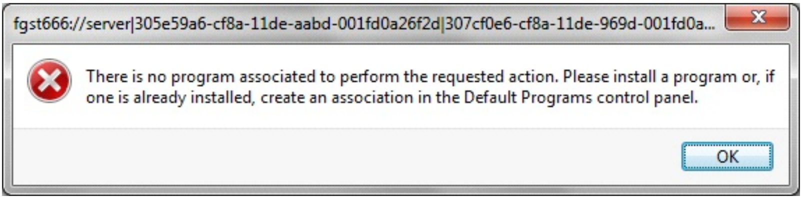
Document name: Chat: john_wilson - adamsmith
Unknown user - Adam Smith — Protocol: Skype

Statistical rule: Activity control (2) By user: Lora Tyler

Document name: jesswill - 236749574
Unknown user - Lora Tyler — Protocol: OSCAR

Document name: 345890544 - 236749574
Unknown user - Lora Tyler — Protocol: OSCAR

Once delivery of security notifications to a certain e-mail address has been set up, one will be able to view them with the help of an email client software. The results will be grouped by security rules names and will be sorted by protocols. You can select to view the details of any notification as well as of the intercepted data by clicking the corresponding link. The details will open in the security officer console if it is installed on the computer from which e-mail security notifications are viewed. Otherwise, the following window will appear:



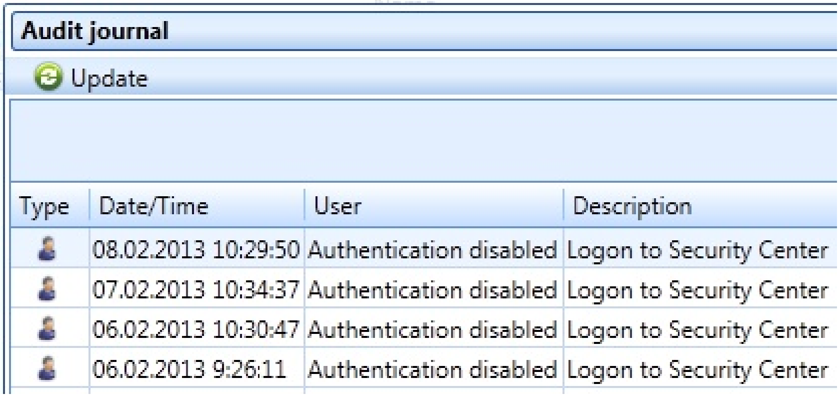
fgst666://server|305e59a6-cf8a-11de-aabd-001fd0a26f2d|307cf0e6-cf8a-11de-969d-001fd0a...

There is no program associated to perform the requested action. Please install a program or, if one is already installed, create an association in the Default Programs control panel.

Note: *In some cases the link to security alert becomes inactive. This happens due to a mail client security settings when a web-interface is used for mail accessing (for example, gmail).*

7.4 Inspection of Security Center users activity

SecureTower system saves information on actions of all users, authenticated in Security center. To inspect an activity log, on the **Tools** menu click **Audit journal** (The **Manage Security Center** ribbon toolbar). The section will be displayed in a new window.



Type	Date/Time	User	Description
👤	08.02.2013 10:29:50	Authentication disabled	Logon to Security Center
👤	07.02.2013 10:34:37	Authentication disabled	Logon to Security Center
👤	06.02.2013 10:30:47	Authentication disabled	Logon to Security Center
👤	06.02.2013 9:26:11	Authentication disabled	Logon to Security Center

To manage the journal use the corresponding buttons on the **Audit journal** toolbar:

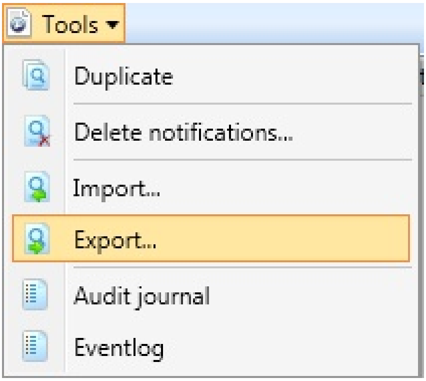
- To update the data of the log, click **Update**.
- To display all the entries, click **Show all messages**.

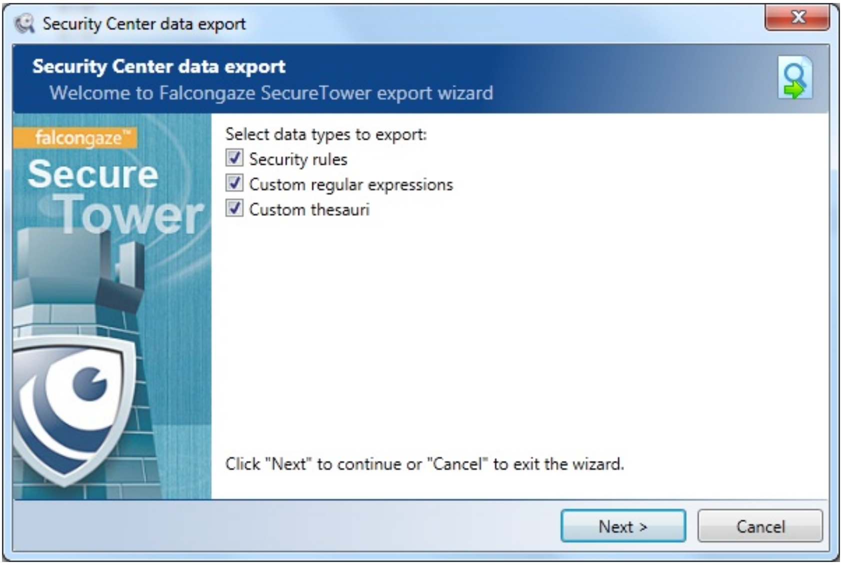
7.5 Data export/import in Security Center

SecureTower supports export of set of custom security groups, rules, thesauri and regular expressions to output file for effective configuration of the same settings in another LAN or workstation. The import feature is actual as well.

7.5.1 Data export

1. To export security policy click **Export** on the **Tools** menu (The **Manage Security Center** ribbon toolbar).





Security Center data export

Welcome to Falcongaze SecureTower export wizard

Select data types to export:

☑ Security rules

☑ Custom regular expressions

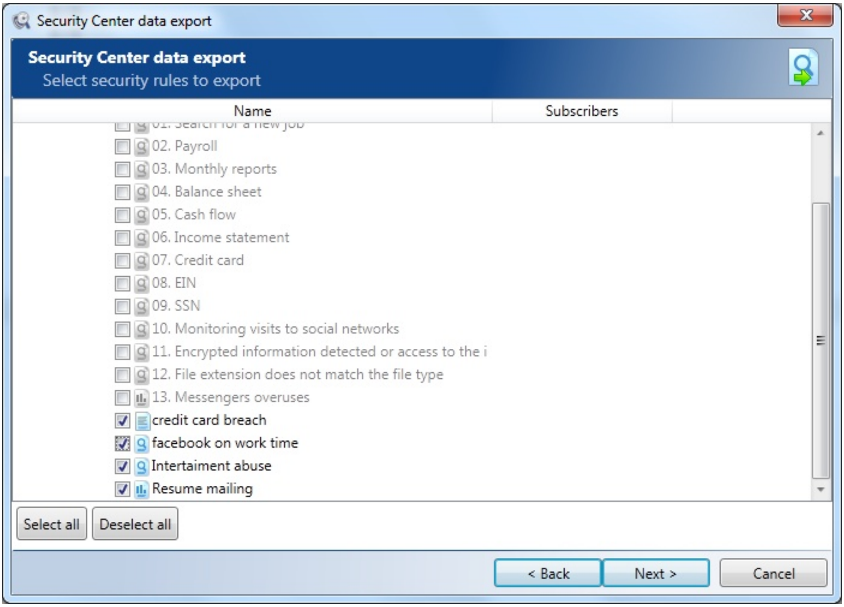
☑ Custom thesauri

Click "Next" to continue or "Cancel" to exit the wizard.

2. Select data types to export in opened window:

- Security rules
- Custom regular expression
- Custom thesauri

Click **Next** to continue.



Security Center data export

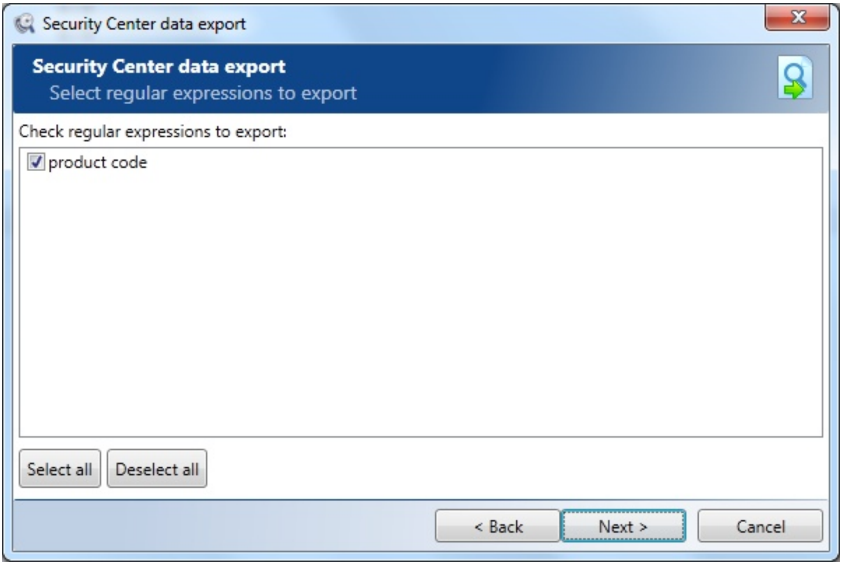
Security Center data export

Select security rules to export

Name	Subscribers
□ 01. Search for a new job	
□ 02. Payroll	
□ 03. Monthly reports	
□ 04. Balance sheet	
□ 05. Cash flow	
□ 06. Income statement	
□ 07. Credit card	
□ 08. EIN	
□ 09. SSN	
□ 10. Monitoring visits to social networks	
□ 11. Encrypted information detected or access to the i	
□ 12. File extension does not match the file type	
□ 13. Messengers overuses	
☑ credit card breach	
☑ facebook on work time	
☑ Intertaiment abuse	
☑ Resume mailing	

3. Select necessary rules from the list to export. To mark all rules as selected click **Select all**. Click **Deselect all** to cancel selection for all rules in the list. Click **Next** to continue.

4. Select regular expression to export and click **Next** to continue.



Security Center data export

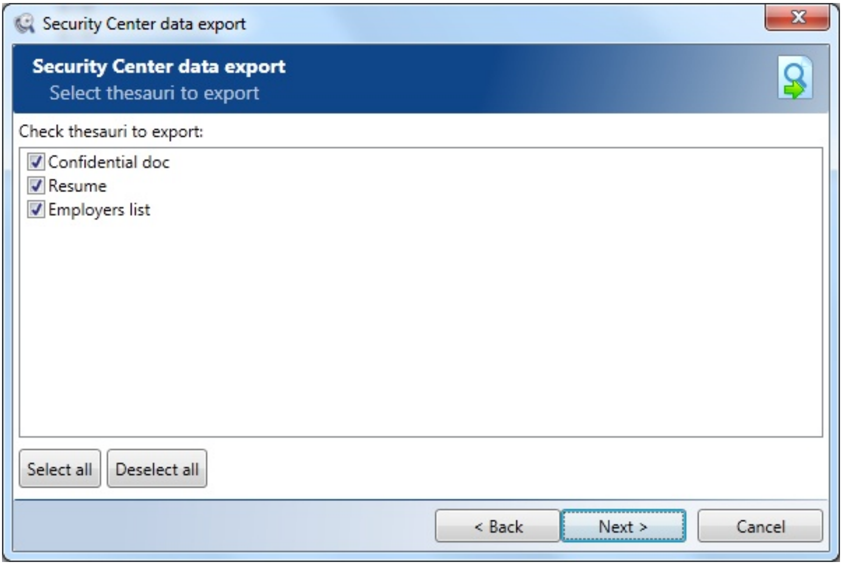
Security Center data export

Select regular expressions to export

Check regular expressions to export:

☑ product code

4. Select necessary thesauri from the list to export and click **Next**.



Security Center data export

Select thesauri to export

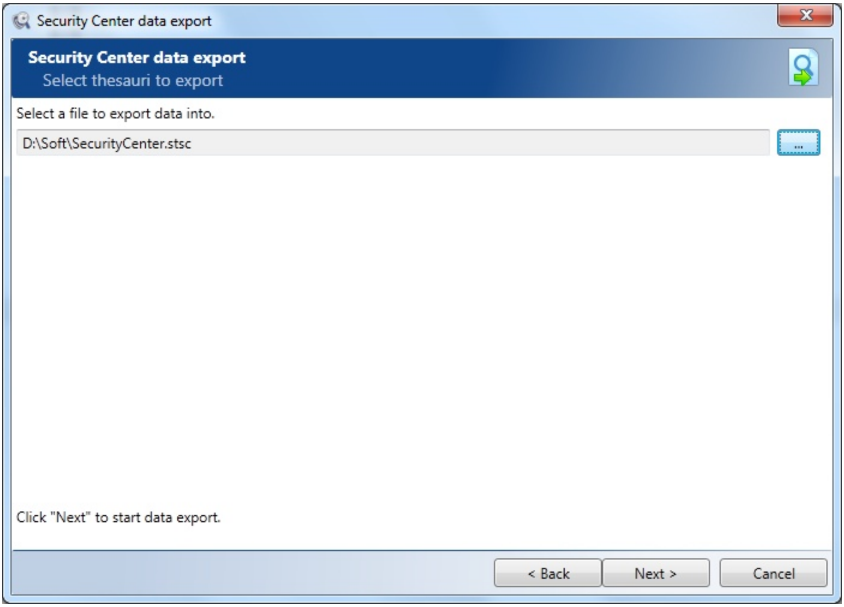
Check thesauri to export:

☑ Confidential doc

☑ Resume

☑ Employers list

5. To select the export file location click the **Tools** button ... and when the location dialog box appears find the folder where you would like **SecureTower** to store saved file by navigating through the folders on your computer. The export file will be displayed in location field with full path and `.stsc` extension. Click **Next** to continue.



Security Center data export

Select thesauri to export

Select a file to export data into.

D:\Soft\SecurityCenter.stsc

Click "Next" to start data export.

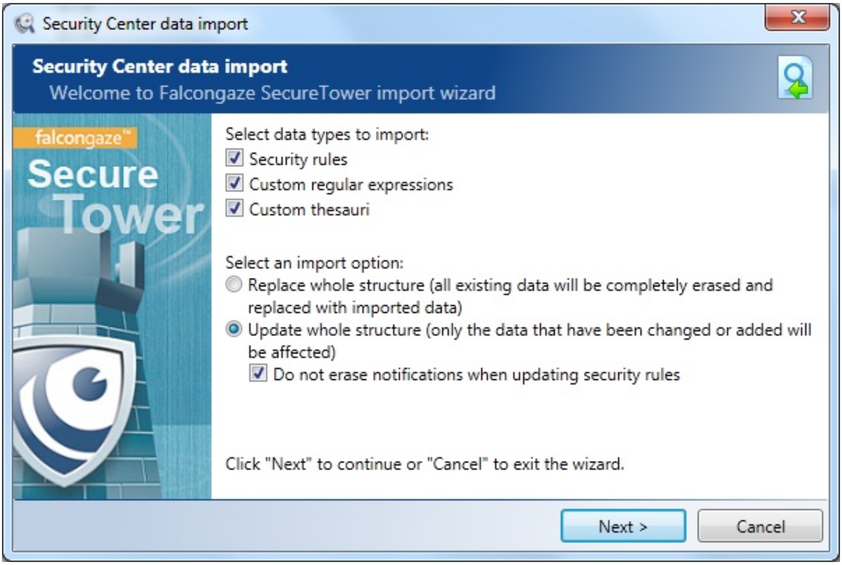
6. The dialog box with successful export confirmation will appear. Click **OK** to finish.

7.5.2 Data import

Import of data is useful for fast recovery of security rules, thesauri and regular expression from an external file.

1. To import corresponding data to Security Center on the **Tools** menu click **Import** (The **Manage Security Center** ribbon toolbar) *(Export tool)*.

2. Select the file with ***.stsc** extension you want to import by navigating through the folders on your computer in the Location dialog box. The export file will be displayed in location field with full path and `.stsc` extension. Click **Open** to continue.



Security Center data import

Security Center data import
Welcome to Falcongaze SecureTower import wizard

Select data types to import:
☑ Security rules
☑ Custom regular expressions
☑ Custom thesauri

Select an import option:
○ Replace whole structure (all existing data will be completely erased and replaced with imported data)
● Update whole structure (only the data that have been changed or added will be affected)
☑ Do not erase notifications when updating security rules

Click "Next" to continue or "Cancel" to exit the wizard.

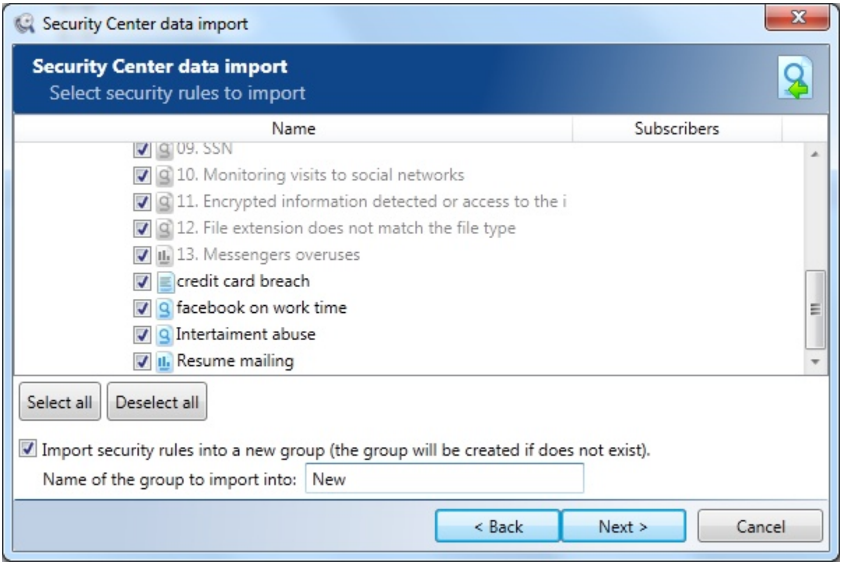
3. In the **Security center data import** window select data types you want to import and mode of import:

   - Select the **Replace whole structure** radio button if full data updating is required. While replacing all existing data will be deleted and replaced by imported data.

   - Select the **Update whole structure** radio button if existing data will not be deleted. While updating new data from the imported file will be added. If names of existing security rules, thesauri or regular expressions matches with imported, it will be replaced by new data. In this case already existing notifications related to replaced rules could be saved by checking corresponding option.

   Click **Next** to continue.

4. Select necessary rules from the list to import. To mark all rules as selected click **Select all**. Click **Deselect all** to cancel selection for all rules in the list. If new group for imported data should be created, check corresponding option and type a group name in the text field. Click **Next** to continue.



Security Center data import

Select security rules to import

☑ 09. SSN

☑ 10. Monitoring visits to social networks

☑ 11. Encrypted information detected or access to the i

☑ 12. File extension does not match the file type

☑ 13. Messengers overuses

☑ credit card breach

☑ facebook on work time

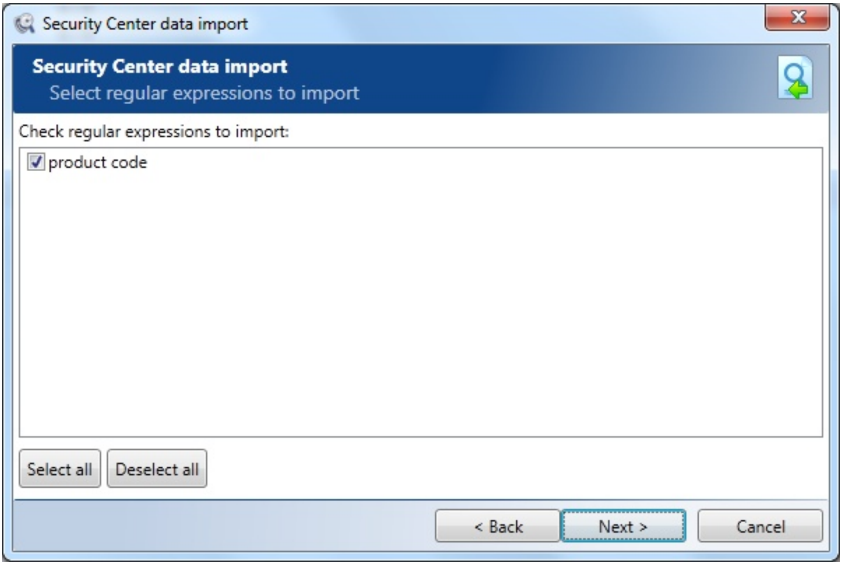
☑ Intertaiment abuse

☑ Resume mailing

☑ Import security rules into a new group (the group will be created if does not exist).

Name of the group to import into: New

5. Select regular expression to import and click **Next** to continue.



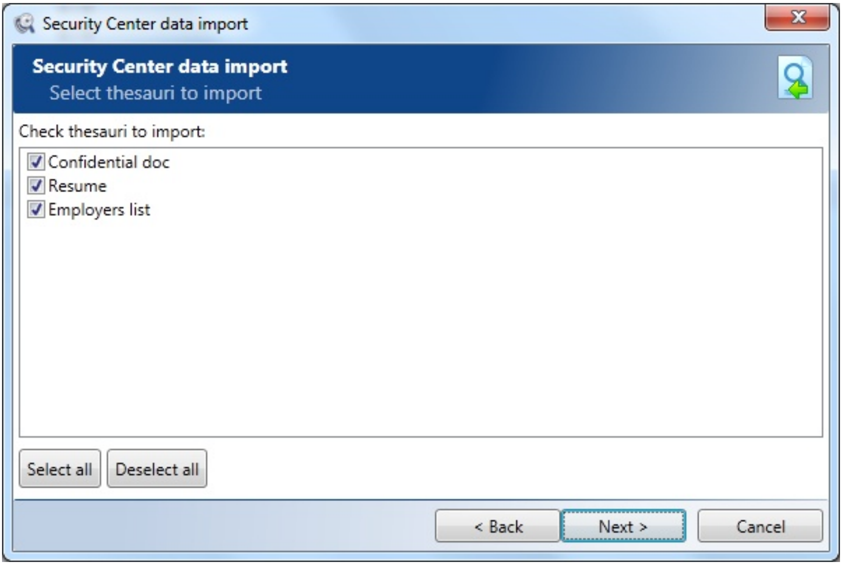
Security Center data import

Select regular expressions to import

Check regular expressions to import:

☑ product code

6. Select necessary thesauri from the list to import and click **Next**.


Security Center data import
Security Center data import
Select thesauri to import

Check thesauri to import:

☑ Confidential doc
☑ Resume
☑ Employers list

Select all
Deselect all
< Back
Next >
Cancel

7. The dialog box with successful import confirmation will appear. Click **OK** to finish.

8 Reports Center Management

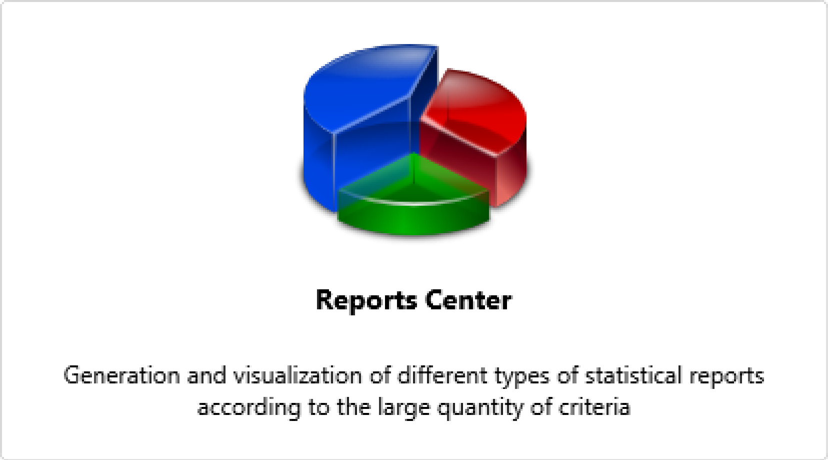
Reports Center is a tool featured generation of network usage and user activity statistics. Statistics is displayed in the form of graphic reports in various foreshortening.

Besides, each report may be adjusted by various criteria: reporting period, the number of users, type of result sorting.

Client console is used for configuring the Reports Center structure, for reports generation, creation and results review.

The intercepted data are analyzed by the program and in case of detection of data satisfied to the given criteria, Reports Center adds the relevant information to the created report.

The reports structure may be hierarchical and provides distribution of reports on different groups depending on a report type regulated by its parameters. For example, it is possible to create a report group with statistics of users web activity (visit of web resources by means of HTTP protocols), group for reports on activity of messengers users, etc.



Reports Center

Generation and visualization of different types of statistical reports according to the large quantity of criteria

To start work with reports click in the **Reports Center** section on the program start page or click **Report Center** on the program toolbar.

Note: *If the functionality of Reports Center isn't active – a loss of connection with* ***Report and Security server*** *might be a possible reason. Check the indicator of connection with the server in the lower right corner of the program window and reconnect to the server if it is necessary.*

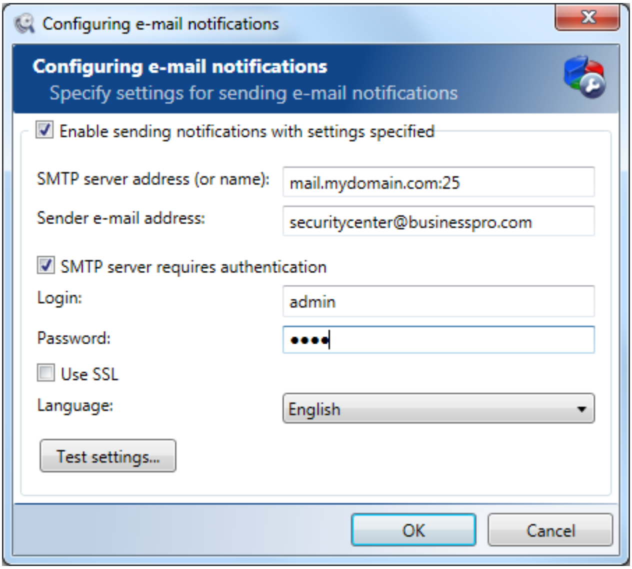
If it's you first time using Reports Center (for example if the **SecureTower** version was updated) and in case of a considerable volume of data intercepted earlier, some time for data processing will pass before Center functionality becomes available. A management of Reports Center could be started after information updating.

8.1 Configuring reports notifications delivery

Reports center notifications with list of links to reports in the SecureTower Client Console and attached PDF-copies of reports can be sent to any specified subscriber email. A scheduler for every type of reports can be set as well.

SMTP server parameters

1. To configure notification delivery parameters, click **Settings** on the Reports Center toolbar.
2. In the **SMTP server address** text box of **Setting up e-mail notifications** window, enter the IP address or name of the server that will be used for sending e-mail security 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*. The name of the server may be specified in the *server:port* format.



Configuring e-mail notifications

Configuring e-mail notifications

Specify settings for sending e-mail notifications

☑ Enable sending notifications with settings specified

SMTP server address (or name): mail.mydomain.com:25

Sender e-mail address: securitycenter@businesspro.com

☑ SMTP server requires authentication

Login: admin

Password: ••••

□ Use SSL

Language: English

3. In the **Sender e-mail address** text box, enter the e-mail address that will be used for sending security notifications.
4. If SMTP server connection authorization is necessary to use, select the **SMTP server requires authentication** option and specify the user name (login) and password of the e-mail box that will be used for sending security notifications .

***Note**: User name and password should be specified only if the SMTP server requires authorization. Otherwise, these fields may 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. To apply this specify the user name that the system notification service will be running under and assign the required mail server access rights in the Windows Services section.*

5. If encrypted connection is necessary to use, check the **Use SSL** option.

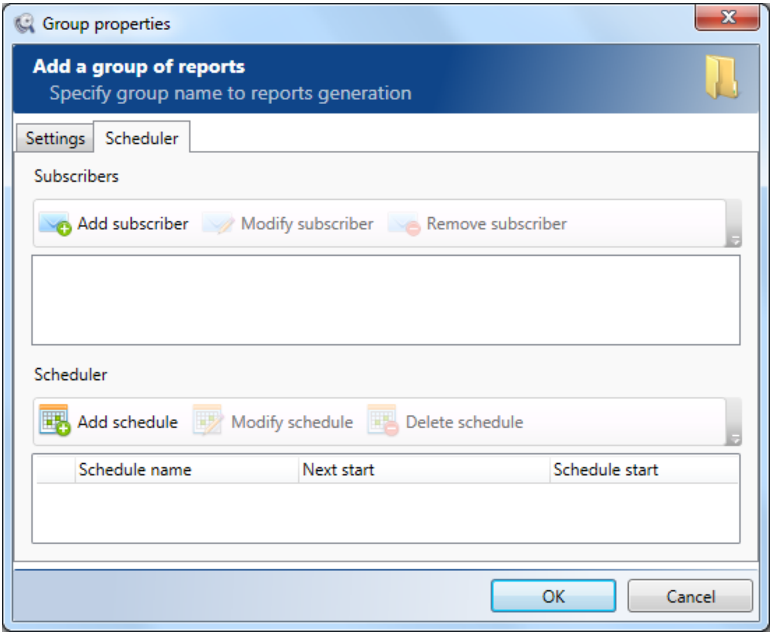
6. Select the language of notification in the corresponding list box.

7. To check if the notification settings function properly, click **Test settings**. In case of a successful test completion, a test message will be sent to the specified e-mail address.

8. To save the settings entered, click **OK**. To discard the changes, click **Cancel**.

Notification delivery scheduler

1. To set up a schedule of sending the emails with reports data and the list of subscribers, go to the **Scheduler** tab of the object's properties window.



2. To add a new subscriber mail address click **Add subscriber** and specify the email in the newly opened window text box. Click OK to continue - the new email will appear in the subscribers list.

3. To specify a new scheduler click **Add scheduler**.

4. Type a name of the scheduler and select the corresponding check box to enable it

activity.

5. In the **Schedule startup parameters** section you are to specify the date and time the schedule will be started, and the frequency of mails with reports sending:

   - **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.

   - **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.

   - **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.

   - **Monthly**. In case you select this option, specify the month(s) and day(s) to repeat the job. Select at least one month in the Month 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).

     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).:

6. 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.

7. 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.

Notifications appearance in mail client interface

The mail with notifications that is sent by the Report Center in accordance to preset schedule contain the list of links to reports data in the SecureTower Client console. The PDF-version copies of reports are attached to the email.

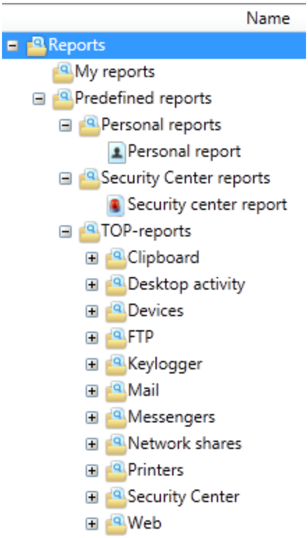
Note: *In some cases the links to reports become inactive. The possible reason is the mail applications with built-in active content blocking is used for mail receiving (f.e. gmail web interface).*

8.2 Management of Reports Center structure

Four different types of report can be created with Report Center tools:

- **TOP-report** - the report with statistical data on TOP - users activity. Employees with extremal values of report results are considered as TOP - users .
- **Personal report** - the report with statistical data on activity of the particular employee.
- **Security center report** - the report with statistical data on Security center incidents.
- **Consolidated report** - the report contains consolidated statistic on selected users activity parameters within specified period.

In the **Reports Center** window the hierarchical list of groups and reports is displayed. The root **Reports** group is created by default and unavailable for deleting. Two child groups are created within this root group. The **Predefined reports** group includes several groups of reports sorted by types of information on which users activity statistics are carried out. The preset reports are created for the fact-finding purposes. Within the **My reports** group creating of other groups or single report is possible. Groups and reports can be created at any hierarchy level as well.



Name

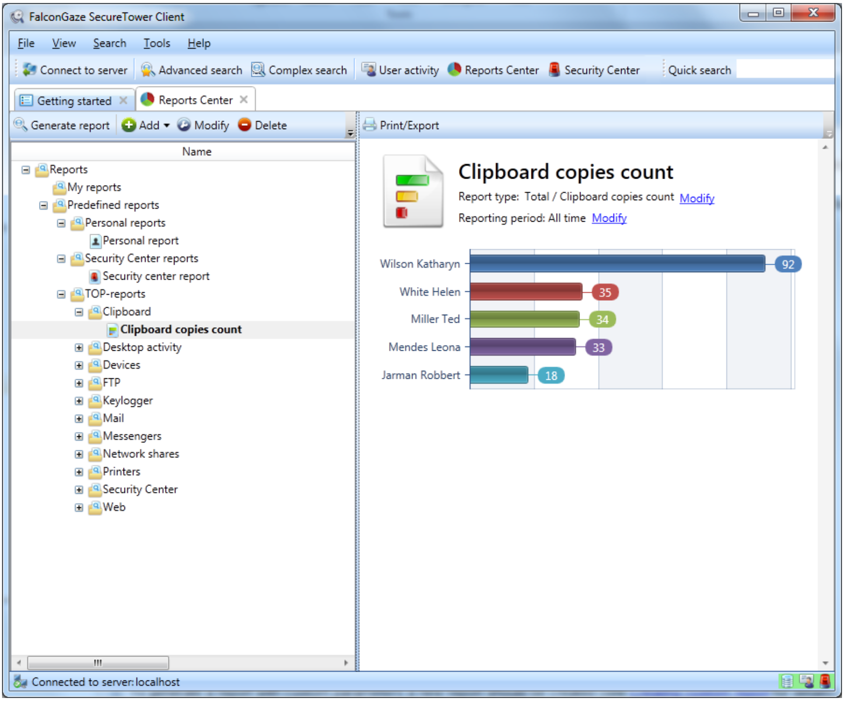
- ⊟ Reports
  - My reports
  - ⊟ Predefined reports
    - ⊟ Personal reports
      - Personal report
    - ⊟ Security Center reports
      - Security center report
    - ⊟ TOP-reports
      - ⊞ Clipboard
      - ⊞ Desktop activity
      - ⊞ Devices
      - ⊞ FTP
      - ⊞ Keylogger
      - ⊞ Mail
      - ⊞ Messengers
      - ⊞ Network shares
      - ⊞ Printers
      - ⊞ Security Center
      - ⊞ Web

The information for each group (report) containing the name and the description of the group (report) is displayed in the window. Contents of the group can be expanded or collapsed by clicking the corresponding button ⊞ / ⊟ on the left of the group name. Besides, the corresponding option from a group shortcut menu can be used as alternative tool. The group shortcut menu is available by right-clicking the group name.

***Note**: The reports are updated automatically once a day (for more information, see Updating report results).*

8.2.1 Generating report

1. To generate a necessary report, select its name from the list in the **Reports Center** window.
2. Click **Generate Report** in the window toolbar or click the [Enter] key on the keyboard. Report generation is also available by double clicking on the selected report name and from the report context menu available by right-clicking on its name.
3. Statistic on an appropriate type of information will be displayed in the right part of the **Reports Center** window (Report results area) in a graphic form.



Clipboard copies count

Report type: Total / Clipboard copies count Modify

Reporting period: All time Modify

To generate a report with custom parameters a new report should be created (*for more information, see [Creating custom report]*) or any predefined report should be modified or duplicated (for more information, see chapters from *[Report parameters modification]* to *[Deleting and duplicating reports]*).

8.2.2 Saving batch of reports

Batch saving procedure is available only for personal reports and is useful when a number of reports must be saved with the template parameters. Herewith it is no necessity to configure and build every single report from the batch.

To save a batch of personal reports:

1. Right-click any personal report entry in the list to open the report context menu.

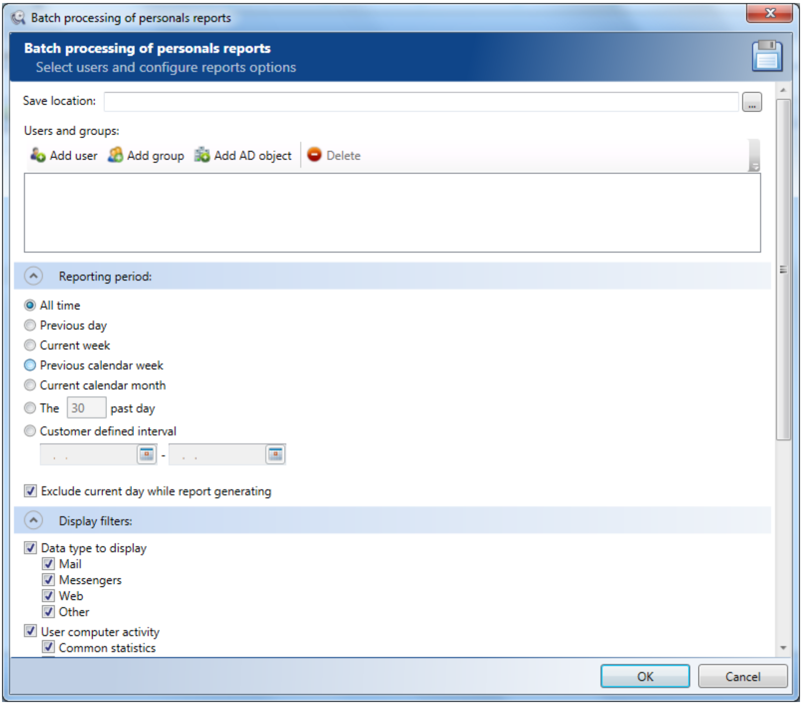
2. On the context menu click **Save batch**.

3. Type the save location in the corresponding field or click the button next to the field ... and select the location.

4. Select the users whose personal reports should be saved and configure reports template as described in *Personal report parameters configuration*.

5. When finish the template configuring click **OK** to save the settings.

Users selection



Batch processing of personals reports
Select users and configure reports options

Save location:

Users and groups:

Reporting period:

● All time
○ Previous day
○ Current week
○ Previous calendar week
○ Current calendar month
○ The 30 past day
○ Customer defined interval

☑ Exclude current day while report generating

Display filters:

☑ Data type to display
- ☑ Mail
- ☑ Messengers
- ☑ Web
- ☑ Other

☑ User computer activity
- ☑ Common statistics

To build report based on the particular users group activity, select the **Specified users** radio button on the **Users** section and make a choice.

To include a particular user accounts to the list click **Add user**. Select the necessary user accounts from the list in the newly opened window. To select user accounts follow the steps below:

- To add a user immediately, click the line with necessary account in the list and click **Add user to list**. To add more then one user simultaneously hold down Ctrl while clicking or Shift for consistent choice). Click **Select** when finish.

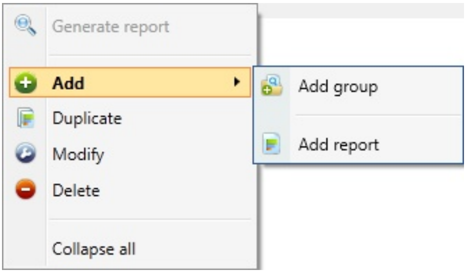
- To add a user and finish process select the necessary one in the list and click **Select**.

To add a group of system users, click **Add group** and select the necessary one from the list of SecureTower users groups.

To add the AD objects, click **Add AD object** and select the necessary domain name and objects from the AD structure. Use filtration if necessary.

8.2.3 Creating group of reports

To create a new group of reports, in the **Add** drop-down menu of the **Reports Center** window ribbon toolbar click the **Add group** option or use group context menu alternatively.

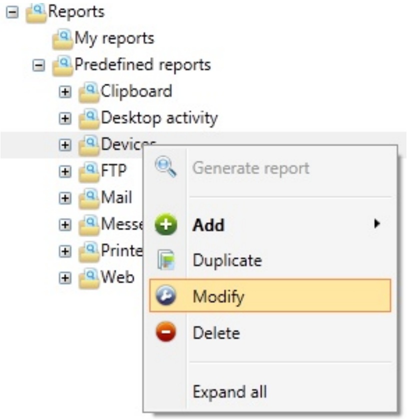


1. In the **Group name** text box of the opened dialogue window, enter the name of the created group and enter the group description in the **Description** text box (optional).
2. Go to the **Scheduler** tab and configure a scheduler settings and add a subscriber if necessary.
3. Click **OK** when finish with group settings entering. The newly added group will be displayed in the list in the **Reports Center** window .

***Note**: Scheduler settings are described in the Configuring reports notifications delivery.*

8.2.4 Modifying group of reports

1. To modify a group of reports, select the necessary group and click Modify on the **Reports Center** ribbon toolbar or select this command in the context menu opened by right-clicking the necessary group. The group settings window can also be opened by double-clicking the necessary group.



2. In the opened dialogue window, make the necessary changes as described in *Creating a group of reports* and click **OK**.

8.2.5 Deleting and duplicating group of reports

Deleting

1. To delete a group, select the necessary group and click **Delete** on the **Reports Center** ribbon toolbar or select this command in the context menu opened by right-clicking the necessary group.
2. In the action confirmation dialogue window, click **Yes**. To cancel the action, click **No**.

Duplicating

1. To duplicate a group, select the necessary group and select **Duplicate** command in the context menu opened by right-clicking the necessary group.
2. In the action confirmation dialogue window, click **Yes**. To cancel the action, click **No**.
3. Follow instructions from *Creating group of reports*.

8.2.6 Creating custom report

To create a new report with custom parameters, on the **Add** menu of the **Reports Center** window ribbon toolbar click an appropriate option: **TOP-report**, **Consolidated report**, **Security center report** or **Personal report** or use context menu alternatively.

1. In the **Report name** text box of the opened dialogue window, enter the name of the new report and enter report description in the **Description** text box (optional). The entered report name will be displayed in the header of report result after its generating as well.

3. Configure all report parameters (for more information, see *TOP Report parameters configuration*, *Personal report parameters configuration*, *Consolidated report parameters configuration* and *Security Center reports configuration*).

4. Click **OK** to confirm or **Cancel** to cancel all action. Created report will be displayed in the **Report Center** window.

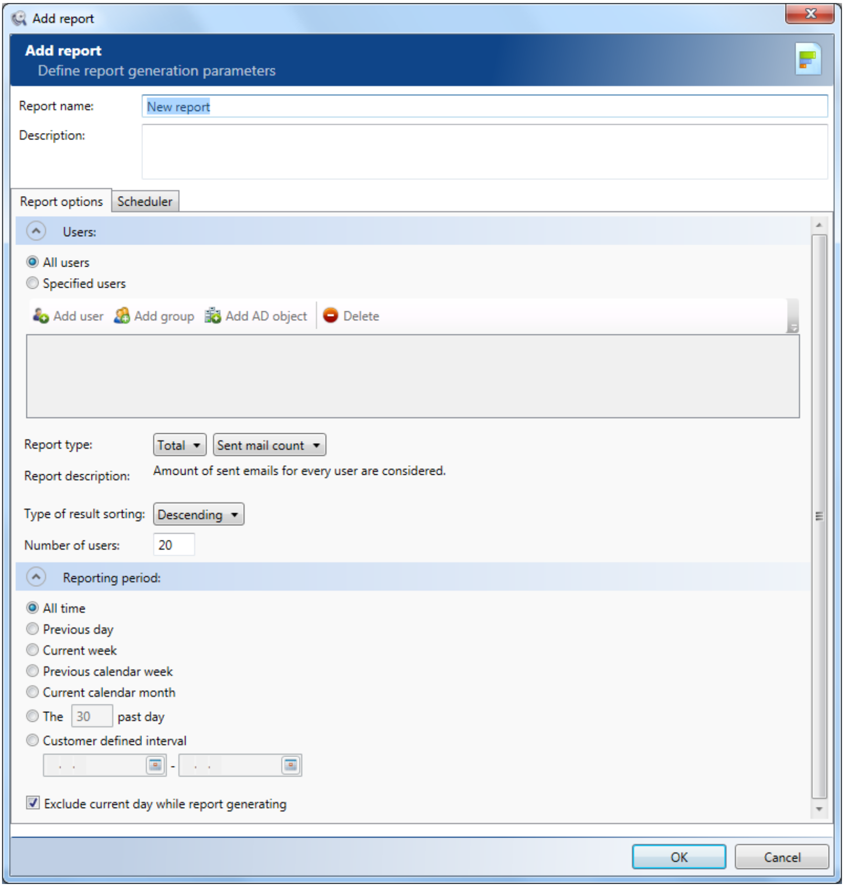
Note: *Data of the current day will not be taken into account while report generating by default in order to prevent inaccuracy of the average daily results. These data will be considered after beginning of a new day. The Report Center data are updated in every 10 minutes and the report results are update automatically as well.*

8.2.6.1 TOP report parameters configuration

The following parameters of report are accessible for TOP report configuration:

- **Users** (reports can be based on the all users statistics or on the statics of the specified group of users).
- **Report type** (depends on type of intercepted data and statistical function type).
- **Number of users** (the number of top-users the TOP report result will be displayed for on the chart).
- **Type of result sorting**(order of TOP report result distribution on the chart).
- **Reporting period**(only data intercepted over this term will be considered in the report)

Note*: Scheduler settings are described in the *Configuring reports notifications delivery*.*



Add report
Define report generation parameters

Report name: New report

Description:

Users:

● All users

○ Specified users

Report type: Total ▾ Sent mail count ▾

Report description: Amount of sent emails for every user are considered.

Type of result sorting: Descending ▾

Number of users: 20

Reporting period:

● All time

○ Previous day

○ Current week

○ Previous calendar week

○ Current calendar month

○ The 30 past day

○ Customer defined interval

☑ Exclude current day while report generating

Users selection

To build report based on the particular users group activity, select the **Specified users** radio button on the **Users** section and make a choice.

To include a particular user accounts to the list click **Add user**. Select the necessary user accounts from the list in the newly opened window. To select user accounts follow the steps below:

- To add a user and proceed with selection, click the line with necessary account in the list and click **Add user to list**. To add more then one user simultaneously hold down Ctrl while clicking or Shift for consistent choice). Click **Select** when finish.
- To add a user and finish process select the necessary one in the list and click **Select**.

To add a group of system users, click **Add group** and select the necessary one from the list of SecureTower users groups.

To add the AD objects, click **Add AD object** and select the necessary domain name and objects from the AD structure. Use filtration if necessary.

Report type

More than 30 types of statistical information are available for review in **Security Center** reports. A summary statistics on investigated data types as well as an average daily statistics are available (except statistics on the start time and the end time of user activity). To select the necessary TOP - report type :

1. Select a type of statistical function from the corresponding drop-down list by left-clicking the field with the predefined **Total** value:

    - To create a report with summary statistics on the investigated data type choose the **Total** value. The sum of quantitative values of data types intercepted over reporting period will be calculating for each user upon report creating .
    - To create a report with average daily statistic on the investigated data type choose the **Average daily** value. The average daily mean of quantitative features of data types intercepted over reporting period will be calculating for each user upon report creating .

2. To select a data type for a report creation left-click the **Sent mail count** (or other predefined value) arrow. Use scroll to view all of types and click one from the list.

According to the selection a detailed description of data type that will be analyzed for the report generation will be displayed in the **Description** text field.

The number of top-users

To specify the number of top-users enter the necessary number in the corresponding text field. The report result will be visualized for this top-users only. The **Top - users** value is a quantity of users with the highest or the lowest quantitative value of selected report type result.

Type of result sorting

To select type of sequence for results displaying on the chart in the report result area, click the button with predefined type opposite the corresponding field and select the necessary type from the drop-down list:

- Select **Ascending** to distribute results on the chart in ascending order. The results with the biggest characteristic will be on top.
- Select **Descending** to distribute results on the chart in descending order. The results with the least characteristic will be on top.

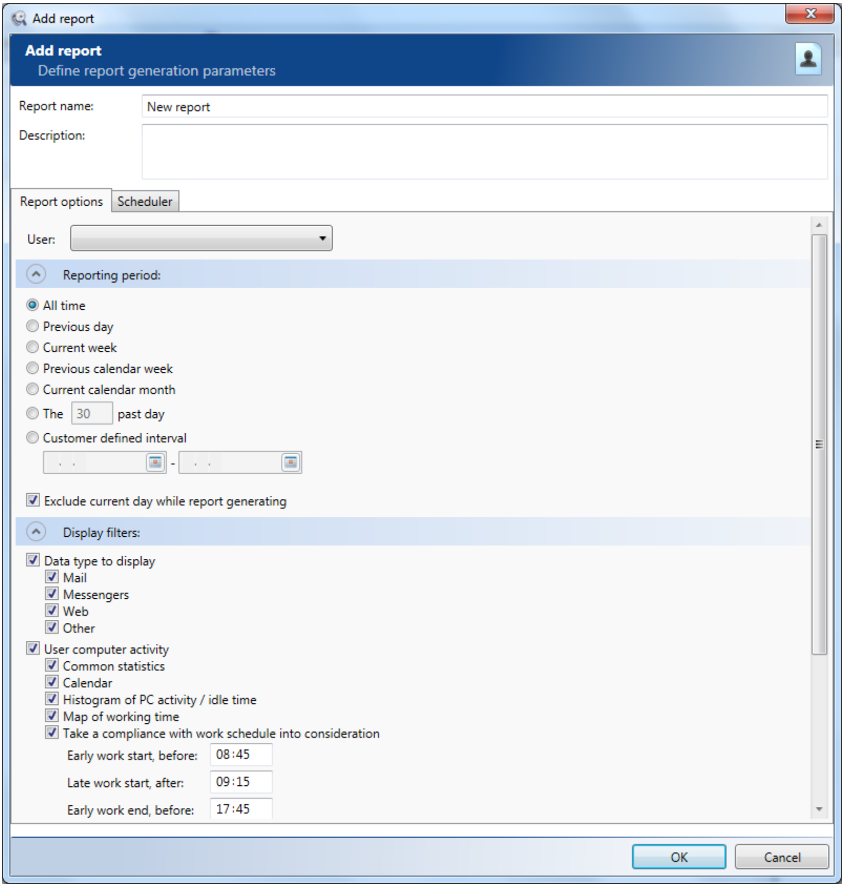
Reporting period

Reports Center analyzes information which was intercepted within specified time interval to generate a report. To specify this interval select one statement from the list or choose your own with built-in calendar tool in the **Customer defined interval** field.

Make sure that the **Exclude current day while report generating** option is checked in order to prevent inaccuracy in the average daily report results. Otherwise clear this option check box to include data, which was intercepted during passed part of the current day.

8.2.6.2 Personal report parameters configuration

The following options of personal report and display filters of report results are accessible for configuring:



Add report

Add report
Define report generation parameters

Report name: New report
Description:

Report options | Scheduler

User:

Reporting period:

● All time
○ Previous day
○ Current week
○ Previous calendar week
○ Current calendar month
○ The 30 past day
○ Customer defined interval
. . - . .

☑ Exclude current day while report generating

Display filters:

☑ Data type to display
- ☑ Mail
- ☑ Messengers
- ☑ Web
- ☑ Other

☑ User computer activity
- ☑ Common statistics
- ☑ Calendar
- ☑ Histogram of PC activity / idle time
- ☑ Map of working time
- ☑ Take a compliance with work schedule into consideration

Early work start, before: 08:45
Late work start, after: 09:15
Early work end, before: 17:45

Note: *Scheduler settings are described in the [Configuring reports notifications delivery](#).*

Report options

1. Select user name from the drop-down list opposite **User** field to generate report for.

2. Reports Center analyzes information which was intercepted within specified time interval to generate a report. To specify this interval select one statement from the **Reporting period** list or choose your own with built-in calendar tool in the **Customer defined interval** field.:

3. Make sure that the **Exclude current day while report generating** option check box is selected in order to prevent inaccuracy in average daily report results. Otherwise clear this option check box to include data, which was intercepted during passed part of the current day.

Display filters

***Note**: All type of statistics on the user activity will be displayed by default.*

The personal report can contain different type of data about user network activity, user computer activity and statistic on applications activity which was used by particular user.

To configure the way of report result displaying it is necessary to choose corresponding display filters.

To clear all preset filters check box click **Deselect all** and proceed with configuring filters you need.

1. Select the **Data type to display** check box and choose the data type which you want to see in the report result. Statistics on correspondence in mail exchange programs (**Mail** option), conversations in IM- programs(**Messengers** option), web traffic data (**Web** option) as well as statistics on files transferred over **FTP** protocol, copied to **external devices** or **network shares**, printed on local/network printers, user **desktop screenshots**, **desktop activity** and **clipboard content** statistics (**Other** option).

2. Select the **User computer activity** check box and proceed with filters configuration:

   - Select the **Common statistic** check box to include data on miscellaneous time parameters of user activity in report results.

   - Select the **Calendar** check box if information about computer on/off time, activity and idle time per calendar day should be included in report results.

   - Select the **Histogram of PC activity/idle time** check box to include an activity-idle ratio in graphic form with time specification.

   - Select the **Map of working time** check box to include user working/idle diagram in chronological sequence.

   - Select the **Take a compliance with work schedule into consideration** check box and specify time frame corresponding to the employee work schedule. The fact of the start or the end of user activity at the computer before/after the specified time frames will be included in report results (for more information, see *Personal report*).

3. Select the **Application activity** check box, to include list of application and its activity statistics in the report results:

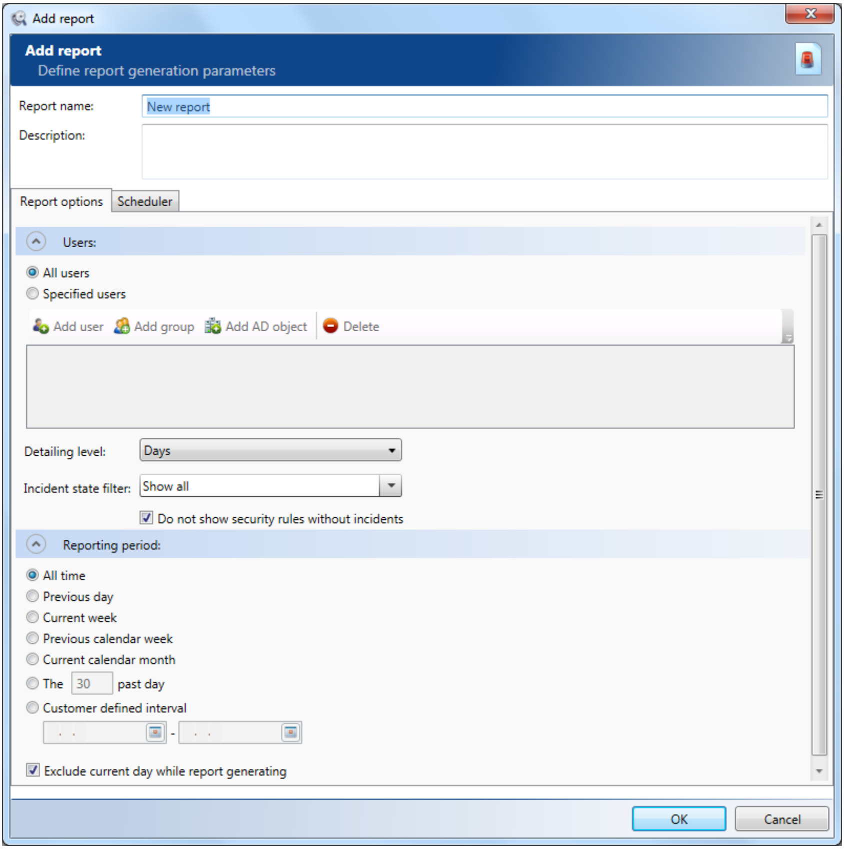
   - Select the **Pie chart** check box to display statistics on application activity on the pie chart.
   - Select the **Active application list** check box to display the list of active application on the computer with activity time and description for each one.

4. Select the **Security center statistic** check box, to include statistical data on Security center incidents in the report results:

To select all of the filters click **Select all**.

8.2.6.3 Security center report configuration

To create a reports on Security center incidents configure the report generation parameters as described below.



Add report

Add report

Define report generation parameters

Report name: New report

Description:

Report options | Scheduler

Users:

● All users

○ Specified users

Detailing level: Days

Incident state filter: Show all

☑ Do not show security rules without incidents

Reporting period:

● All time

○ Previous day

○ Current week

○ Previous calendar week

○ Current calendar month

○ The 30 past day

○ Customer defined interval

☑ Exclude current day while report generating

Users selection

To build report based on the particular users group activity, select the **Specified users** radio button in the **Users** section and make a choice .

To include a particular user accounts to the list click **Add user**. Select the necessary user accounts from the list in the newly opened window. To select user accounts follow the steps below:

- To add a user immediately, click the line with necessary account in the list and click **Add user to list**. To add more then one user simultaneously hold down Ctrl while clicking or Shift for consistent choice). Click **Select** when finish.
- To add a user and finish process select the necessary one in the list and click **Select**.

To add a group of system users, click **Add group** and select the necessary one from the list of SecureTower users groups.

To add the AD objects, click **Add AD object** and select the necessary domain name and objects from the AD structure. Use filtration if necessary..

Report parameters

Select the necessary level of report time interval detailing from the **Detailing level** list to display the incident number per every day, week, month or to display the number of incidents registered for all report period.

3. Select the necessary state of incident which data should be included in the report results (for more information, see *Viewing notifications in Security Center*) from the corresponding list. Select the **Do not show security rules without incidents** check box to include only the information on rules with registered security incident in report results.

4. **Reports Center** analyzes information which was intercepted within specified time interval to generate a report. To specify this interval check one from the list or choose your own with built-in calendar tool in the **Customer defined interval** field.

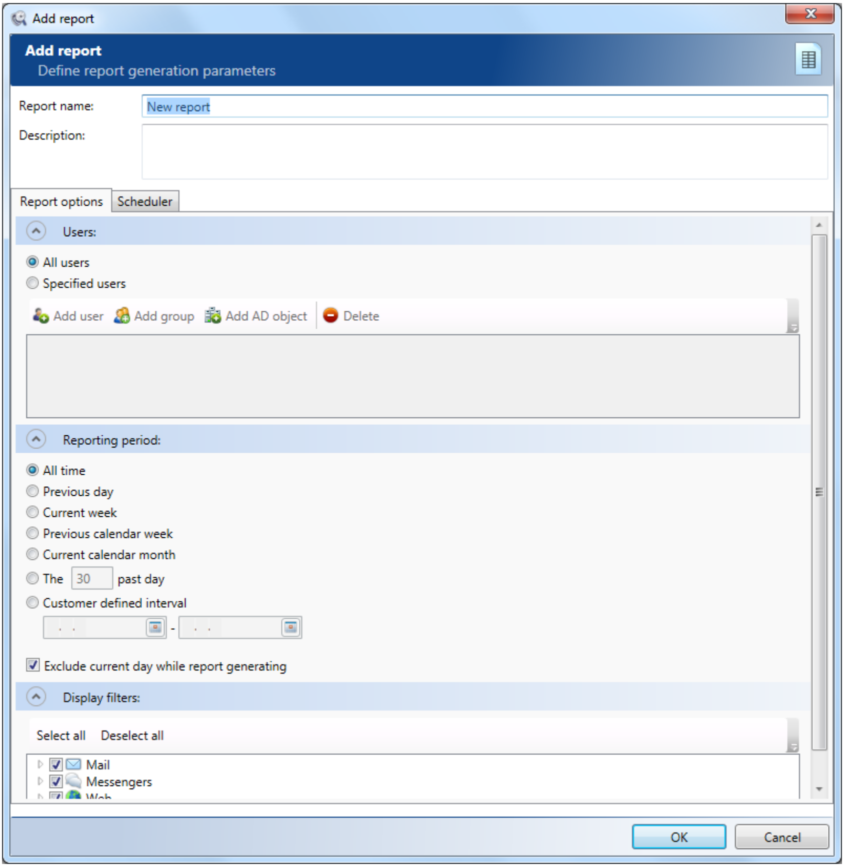
Make sure that the **Exclude current day while report generating** option is checked in order to prevent inaccuracy in average daily report results. Otherwise clear this option check box to include data, which was intercepted during passed part of the current day.

***Note**: Scheduler settings are described in the Configuring reports notifications delivery*.

8.2.6.4 Consolidated report configuration

The report parameters and the scheduler of report notifications sending are available for Consolidated report configuring.

Note*: Scheduler settings are described in the [Configuring reports notifications delivery](#).*



Add report

Add report

Define report generation parameters

Report name: New report

Description:

Report options | Scheduler

Users:

● All users

○ Specified users

Add user · Add group · Add AD object · Delete

Reporting period:

● All time

○ Previous day

○ Current week

○ Previous calendar week

○ Current calendar month

○ The 30 past day

○ Customer defined interval

. . - . .

☑ Exclude current day while report generating

Display filters:

Select all Deselect all

☑ Mail

☑ Messengers

☑ Web

OK Cancel

Users selection

To build report based on the particular users group activity, select the **Specified users** radio button in the **Users** section and make a choice .

To include a particular user accounts to the list click **Add user**. Select the necessary user accounts from the list in the newly opened window. To select user accounts follow the steps below:

- To add a user immediately, click the line with necessary account in the list and click **Add user to list**. To add more then one user simultaneously hold down Ctrl while clicking or Shift for consistent choice). Click **Select** when finish.

- To add a user and finish process select the necessary one in the list and click **Select**.

To add a group of system users, click **Add group** and select the necessary one from the list of SecureTower users groups.

To add the AD objects, click **Add AD object** and select the necessary domain name and objects from the AD structure. Use filtration if necessary.

Reporting period

Reports Center analyzes information which was intercepted within specified time interval to generate a report. To specify this interval select one statement from the list or choose your own with built-in calendar tool in the **Customer defined interval** field.

Make sure that the **Exclude current day while report generating** option is checked in order to prevent inaccuracy of the average daily report results. Otherwise clear this option to include data, which was intercepted during passed part of the current day.

Display filters

There are a wide range of user activity statical data available for including into consolidated report. A summary statistics on investigated data types as well as an average daily statistic are available to choose. The average statistics is considered on the basis of actual working days during the specified time.

To configure the display filters change the current display mode.

Note*: All statistical data is included into the report.*

To discard all preset filtering settings click **Deselect all**.

To display the necessary type of statistical parameters select the corresponding check box. To select a particular parameter click the corresponding parameter type arrow to expand the list of parameters and select the necessary one from the available for this type of data.

To select all parameters check boxes and use preset settings click **Select all**.

8.2.7 Report parameters modification

1. To modify a report, select the necessary group and click **Modify** in the Reports Center ribbon toolbar or select this command in the context menu opened by right-clicking the necessary report. The report parameters can be accessible by double-clicking the necessary report .
2. In the opened dialogue window, make the changes as described in *Creating custom report* and click **OK**.

8.2.8 Deleting and duplicating reports

Deleting

1. To delete a report, select the necessary report and click **Delete** on the **Reports Center** ribbon toolbar or select this command in the context menu opened with right click the necessary report.
2. In the action confirmation dialogue window, click **Yes**. To cancel the action, click **No**.

Duplicating

1. To duplicate a report, select the necessary report and click **Duplicate** in the context menu opened by right-clicking the necessary report.
2. In the action confirmation dialogue window, click **Yes**. To cancel the action, click **No**.
3. To create a report with custom settings follow instructions from the *Creating custom report*.

8.2.9 Updating report results

Statistics updating is performed in automatic mode at night time. After updating all the reports are built by the system without considering the followed changes of interception statistics and changes in the system. Therefore the manual statistics data updating should be performed to include the latest changes into reports results.

To update reports click **Update reports** on the report window toolbar and proceed with reports generating.

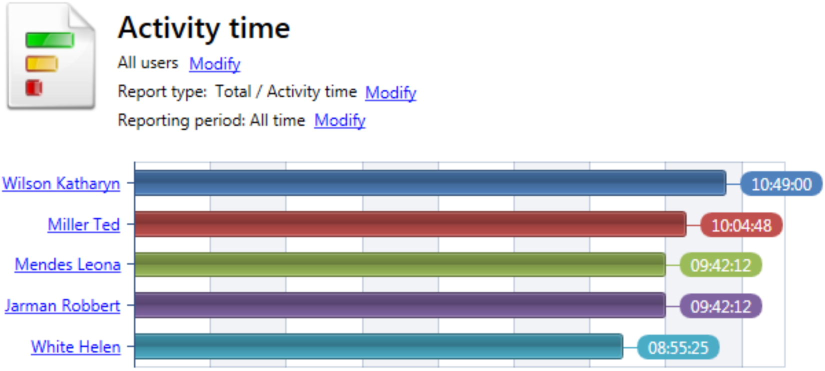
8.2.10 Viewing a report

Results of report generation are displayed in the right part of the **Reports Center** window in compliance with given parameters.

To view report results select the appropriate report name in the list and click **Generate report** on the **Reports Center** window ribbon toolbar.

Statistics on an appropriate type of information will be displayed in the right part of the **Reports Center** window (report results area).

8.2.10.1 TOP report



Activity time

All users Modify

Report type: Total / Activity time Modify

Reporting period: All time Modify

The report name, reporting period as well as results chart are displayed in the report results area.

Names of users, which intercepted data satisfied to the specified report parameters are represented in the chart.

Users name are interactive and link to the detailed data on subject of the currently report for selected user name.

During a report viewing, it is possible to change the **Report on user** and the **Reporting period** fields value. To make changes click **Modify** (opposite corresponding field) and select the necessary value from the drop-down list (*Personal report parameters configuration*).

Note*: Upon such modification one should keep in mind that all changes influence on the display of the current report only and will not be applied to the report settings.*

The number of users in the chart corresponds to the value, specified in the **Add report** window. Quantitative value of investigated data types for every user are represented in the chart opposite user name.

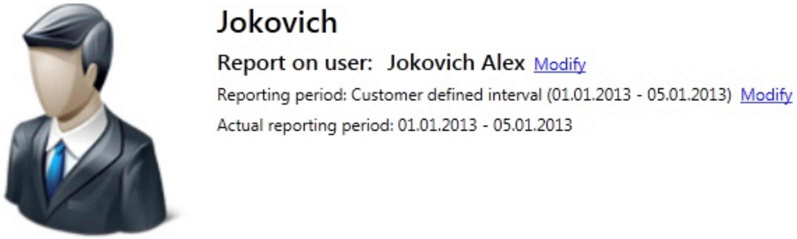
To export/print/send by e-mail image of report result click **Print/Export** in the report results area toolbar.

8.2.10.2 Personal report

The header of personal report, statistics on user network activity, user computer activity and statistics on applications activity are displayed in the report result area.

To export/print/send by e-mail image of report results click **Print/export** in the report results area toolbar.

Header of Personal report



Jokovich

Report on user: Jokovich Alex Modify

Reporting period: Customer defined interval (01.01.2013 - 05.01.2013) Modify

Actual reporting period: 01.01.2013 - 05.01.2013

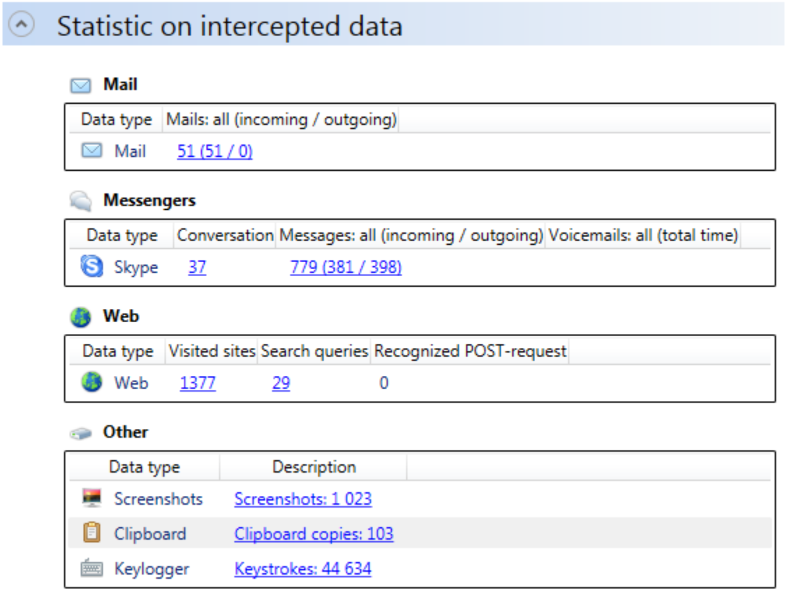
The name of the report, specified while report parameters configuring is displayed in the top of the report results area.

The name of the user, reporting period and actual period which data for report has been collected within are presented in the header.

While report viewing, it is possible to change the **Report on user** and the **Reporting period** fields values. To make changes click **Modify** (opposite corresponding field) and select the necessary one from the drop-down list (*Personal report parameters configuration*).

Note*: Upon such modification one should keep in mind that all changes influence on the display of the current report only and will not be applied to the report settings.*

Statistics on intercepted data



Statistic on intercepted data

Mail

Data type	Mails: all (incoming / outgoing)
Mail	51 (51 / 0)

Messengers

Data type	Conversation	Messages: all (incoming / outgoing)	Voicemails: all (total time)
Skype	37	779 (381 / 398)	

Web

Data type	Visited sites	Search queries	Recognized POST-request
Web	1377	29	0

Other

Data type	Description
Screenshots	Screenshots: 1 023
Clipboard	Clipboard copies: 103
Keylogger	Keystrokes: 44 634

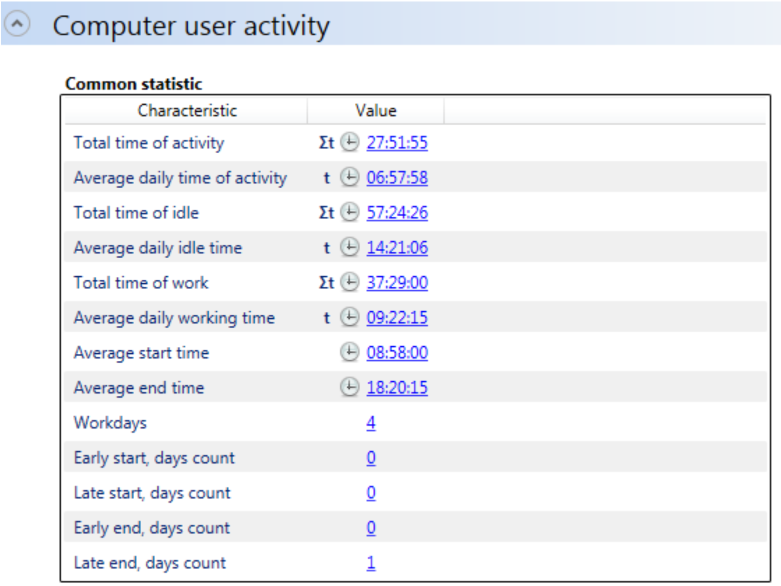
Fields of this zone represent statistic on data type, specified while report parameters configuring.

The **Mail** field contains the statistic on e-mails transferred via **POP3, SMTP, IMAP, MAPI**.

The **Messengers** field contains the statistic on correspondence via **ICQ (OSCAR protocol), Skype,SIP, XMPP (Jabber), Mail.Ru Agent, Yahoo IM, Microsoft Lync, Viber**.

The **Web** field contains the statistic on visited sites, search queries, recognized POST-requests.

The **Other** field contains the statistic on such activity as: files transferred over **FTP** protocol, copied to **external devices** or **network shares**, printed on local/network printers, user **desktop screenshots**, as well as **desktop activity** statistics and **clipboard content**.



Computer user activity

Common statistic

Characteristic	Value
Total time of activity	Σt 27:51:55
Average daily time of activity	t 06:57:58
Total time of idle	Σt 57:24:26
Average daily idle time	t 14:21:06
Total time of work	Σt 37:29:00
Average daily working time	t 09:22:15
Average start time	08:58:00
Average end time	18:20:15
Workdays	4
Early start, days count	0
Late start, days count	0
Early end, days count	0
Late end, days count	1

Characteristics

Statistical data on computer user activity bases on analysis of user activity pattern during the calendar day.

Start time is computed by the system as the computer first start time or the time of the first user interaction with PC, detected for a calendar day.

End time is computed as the computer latest shut down time or the time of the latest user interaction with PC, detected (in case of computer wasn't switched off) for a calendar day.

Working time is computed as the difference between **end time** and **start time**. It should be mentioned that the user activity pattern isn't considered while computing(for example, the idle time of the computer is considered as working time as well). The actual hours of user interaction with computer can be assessed with **activity time** parameters.

All calendar days with computer user activity(for example, clipboard or mouse activity) are considered as **working days**. *The day will not be considered as working, if a user presents at his work place but doesn't activate his computer as well as if the computer is left activated from the previous day, but the user is absent at his work place or doesn't interact with his computer.*

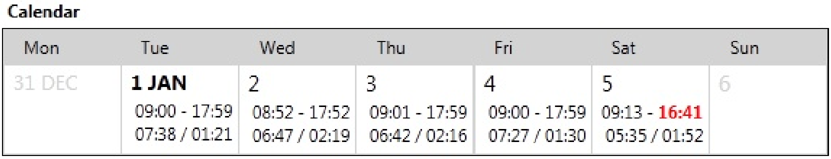
Value of the **Early start** field complies with start time events, detected earlier than the previously specified time while display filters configuring (*Personal report parameters configuration*) .

Value of the **Late start** field complies with end time events, detected later than the previously specified time in corresponding field while display filters configuring.

Value of the **Early end** field complies with end time events, detected earlier than the previously specified time in corresponding field.

Value of the **Late end** field complies with end time events, detected later than the previously specified time while display filters configuring.

Calendar



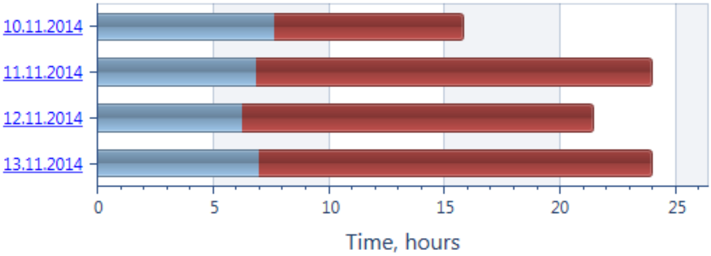
Calendar

Mon	Tue	Wed	Thu	Fri	Sat	Sun
31 DEC	**1 JAN** 09:00 - 17:59 07:38 / 01:21	2 08:52 - 17:52 06:47 / 02:19	3 09:01 - 17:59 06:42 / 02:16	4 09:00 - 17:59 07:27 / 01:30	5 09:13 - 16:41 05:35 / 01:52	6

Each calendar cell contains information about corresponding day: working day start and end time, activity time and idle time.

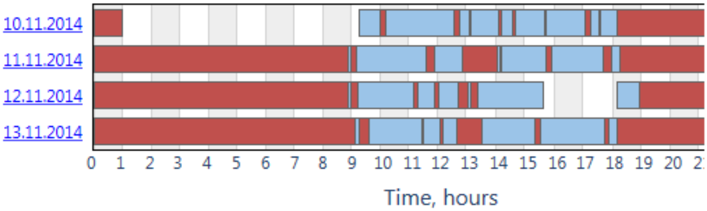
Examine the **Calendar legend** field to find more detailed key information.

Histogram of PC activity/idle time



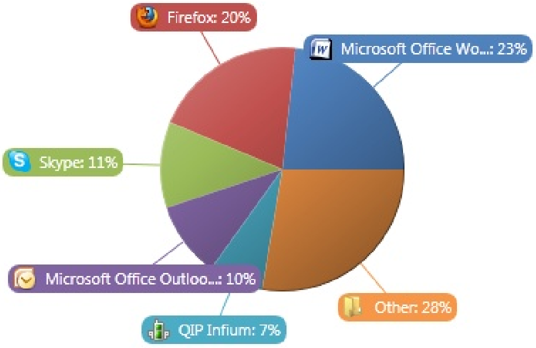
The activity-idle ratio in graphic form with time specification is represented in the **Histogram** section.

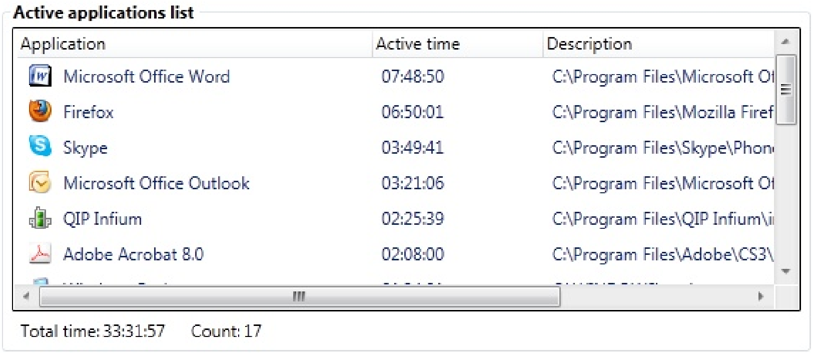
Map of working time



There are interval of active(blue) and idle(red) working time in chronological sequence for each report day on the map. The information about time interval size is available when mouse cursor is over.

Application activity





Active applications list

Application	Active time	Description
Microsoft Office Word	07:48:50	C:\Program Files\Microsoft Of
Firefox	06:50:01	C:\Program Files\Mozilla Firef
Skype	03:49:41	C:\Program Files\Skype\Phon
Microsoft Office Outlook	03:21:06	C:\Program Files\Microsoft Of
QIP Infium	02:25:39	C:\Program Files\QIP Infium\i
Adobe Acrobat 8.0	02:08:00	C:\Program Files\Adobe\CS3\

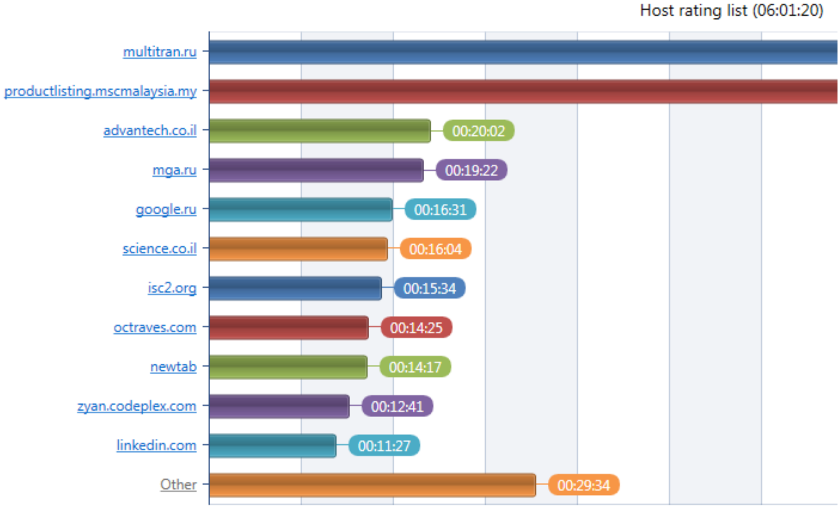
Total time: 33:31:57 Count: 17

The **Pie chart** with list of application, which activity has been detected on user computer, are displayed in the **Application activity** section.

Six most active applications are usually presented on the chart as well as at the top of list. The data of applications activity in percentage (pie chart) and in hours (list) are displayed. The applications names and description for all active applications can be found in list as well.

Total time of applications activity and total amount of active application are displayed in corresponding field below the list.

Browsers activity



The rating of web sites with the biggest session durations is displayed on the chart. The duration of visits are figured next to the each site column.

The name of the web sites are performed in the link form. To view the full report on the particular site visits click the necessary site name and inspect the results in the search results window.

The list of the web sites that were visited by user during specified report period is displayed in the table below the chart. Use the scrollbar to view all the records. To expand the list click the expand arrow.

The summary on browser activity time and the number of sites are displayed in the field below the table.

Security Center statistic

The list of security rules and the number of corresponding incident, which was initiated by user during the report period in the field are displayed.

The number of incident is an interactive link to corresponding alerts in Security Center.

8.2.10.3 Security center report

Report header

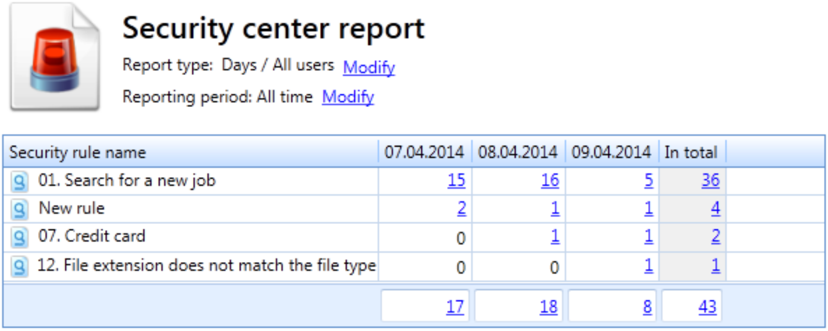
The header with report type and reporting period is displayed in the top of report result area.

While report viewing, it is possible to change the **Report type** and the **Reporting period** fields values.

To change the currently displayed report type click **Modify** (opposite corresponding field) and select the necessary type from the drop-down list (*Security center report configuration*).

Note*: Upon such modification one should keep in mind that all changes influence on the appearance of the currently considered report only and will not be applied to the report settings.*

Results



Security center report

Report type: Days / All users Modify

Reporting period: All time Modify

Security rule name	07.04.2014	08.04.2014	09.04.2014	In total
01. Search for a new job	15	16	5	36
New rule	2	1	1	4
07. Credit card	0	1	1	2
12. File extension does not match the file type	0	0	1	1
	17	18	8	43

Report results are displayed in the table form. Each line corresponds to the particular security rule and contains the rule name, amount of incidents on this rule per specified time interval in corresponding cells and total number of incidents for this rule in the last column as well.

The number of all security incidents which were registered by the system during each therm and the number of all ever registered incidents are presented in the last row.

The number of incident is an interactive link to corresponding alerts in Security Center.

To export/print/send by e-mail image of report results click **Print/Export** in the report results area toolbar.

8.2.10.4 Consolidated report

Report header

The header with report type and reporting period is displayed in the top of report result area.

While report viewing, it is possible to change the **Report type** and the **Reporting period** fields values.

To change the currently considered report type click **Modify** (opposite corresponding field) and select the necessary type from the drop-down list (*Security center report configuration*).

***Note**: Upon such modification one should keep in mind that all changes influence on the appearance of the currently considered report only and will not be applied to the report settings.*

Consolidated table of results

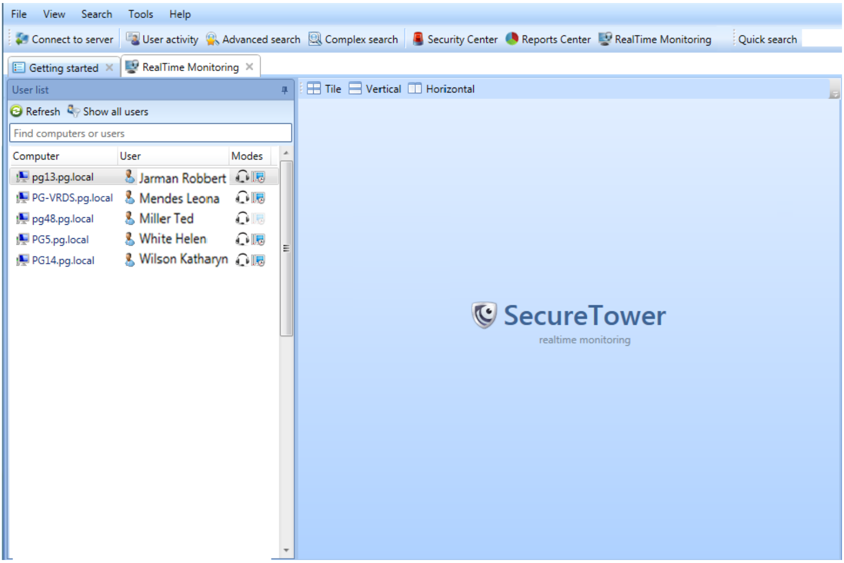
The results of report generating are displayed in the table form.

The quantitative values of parameters is a link to results of interception the corresponding type of activity. To inspect the interception results click the necessary link. The detailed information will be displayed in the search results window.

9 RealTime Monitoring

SecureTower provides users with access to an audio stream from PC audio recording device(connected microphone) and a video stream with a desktop video in real-time mode according to the system access permission. If the appropriate access permission is set, one can listen to audio stream and watch a user desktop video separately or simultaneously. Herewith recording of the both type of streams in real-time mode and their playback are available.

To start click in the **RealTime Monitoring** section on the program start page or click the corresponding button in the program toolbar. The window will be opened in the new tab.



Computer	User	Modes
pg13.pg.local	Jarman Robbert	
PG-VRDS.pg.local	Mendes Leona	
pg48.pg.local	Miller Ted	
PG5.pg.local	White Helen	
PG14.pg.local	Wilson Katharyn	

***Note**: If it is impossible to establish connection with any EndPoint Agent Server, the RealTime Monitoring service will be unavailable and will appear dimmed on the console main page.*

9.1 Starting monitoring

The **Users list** bar of the window contains the list of workstation with associated users. The list contains users which monitoring can be carried out according to the access rights. In the **Modes** column the audiomonitoring 🎧 and videomonitoring 🖥 states are displayed in accordance to the agent settings profile (for more information, see *RealTime monitoring chapter of the Administrator Guide*).

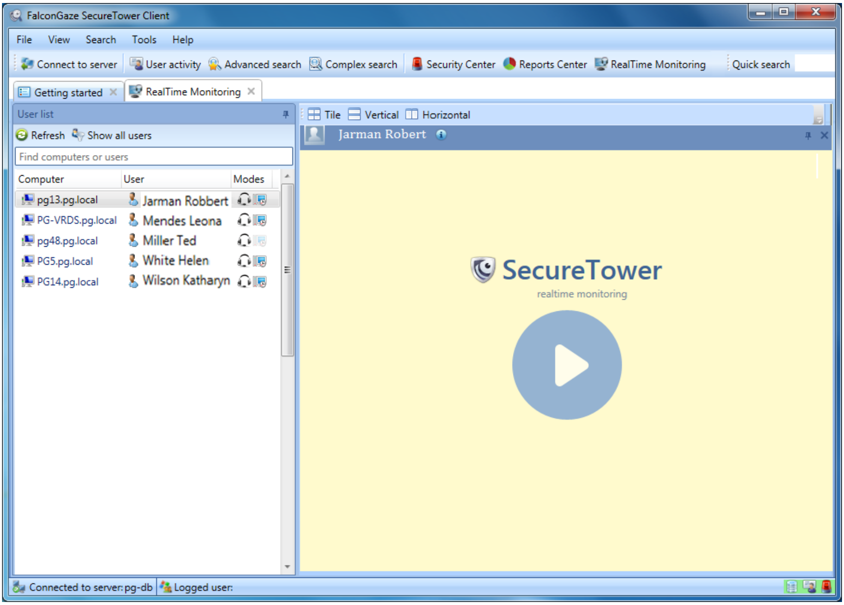
***Note**: Listening audio and watching video are possible in real-time mode only. The stream data is not saved to database automatically, but can be saved by user from the RealTime Monitioring window manually.*

To see all the controlled users click **Show all users** on the toolbar. Only monitored users are presented in the list by default.

To refresh the list of users click the corresponding button on the toolbar.

To establish connection with the particular user workstation:

1. Double-click on the corresponding row in the users list. The connection with the necessary workstation will be established. The built-in media player window will appear next to the users list panel.



Computer	User	Modes
pg13.pg.local	Jarman Robbert	
PG-VRDS.pg.local	Mendes Leona	
pg48.pg.local	Miller Ted	
PG5.pg.local	White Helen	
PG14.pg.local	Wilson Katharyn	

***Note**: If the target computer is off or microphone or other audio recording device is not connected to the PC, the corresponding error messages will be displayed in the media player window.*

A dynamic playback controls panel is displayed at the top of the player window upon monitoring startup and fade out by itself a few seconds later. To show the panel hover over the area where the panel was shown last time.

The following buttons are available on the playback controls panel:

▶	**Play**	Starts translation of the audio and/or video streams from the selected workstation.
■ ■	**Stop**	Stops translation and recording of the audio and/or video streams from the selected workstation.
●	**Record**	Playback of the audio and/or video streams from the selected workstation and records the data to the media file on the local disc. The default save path can be changed to a custom from the **Options** menu of the Client console (for more information, see *Quick tips for results viewing*).

▶	**Play**	Starts translation of the audio and/or video streams from the selected workstation.
■ 🟥	**Stop**	Stops translation and recording of the audio and/or video streams from the selected workstation.
🎧	**Listening to audio**	Audio activation/deactivation.
🖥	**Watching video**	Video activation/deactivation.
1:1	**Original size**	Scales the image to the original size in the media player zone.
Records list (3)		Access to the records list. Records quantity is displayed in the parentheses
⛶	**Full screen**	Allows user to use the entire computer screen for browsing the video.
✥	**Fit to screen**	Scales the image to fit the player window borders.
📌/▣	**Auto hide**	Activate/deactivate auto hide mode.
▮──		Volume adjustment.

2. To start translation of the video and audio streams click **Playback** ▶ in the media player window or **Play** ▶ on the playback control panel.

***Note**: If the level of the audio signal decreases lower than minimal one that the system can intercept or a microphone or any other audio recording device was disconnected while monitoring, the error messages will appear instead of the equalizer.*

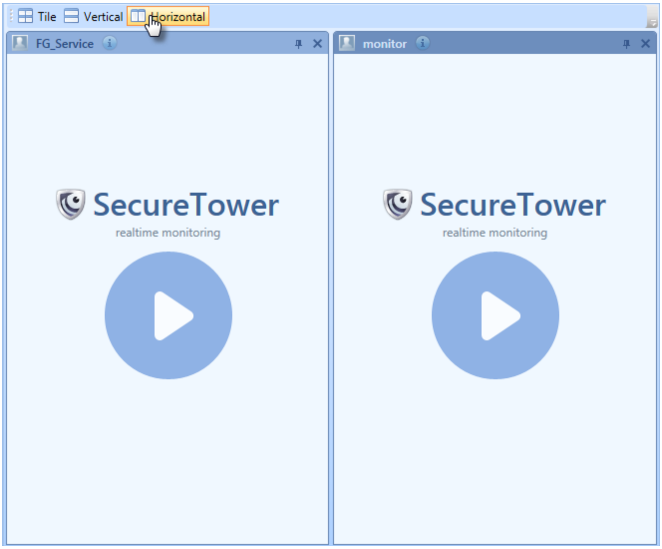
3. To stop translation click **Stop** ■ on the playback controls panel or press Spacebar. To restart click **Playback** ▶ or **Play** ▶ or left-click anywhere in the player window area.

4. To disconnect from the current monitored workstation close the corresponding media player window.

Monitoring of several users simultaneously

Monitoring of several users can be implemented in the parallel mode.The new player window tab will be opened for every new user.

If you have more than one media player window open, use the arrangement button on the viewing area toolbar to specify the way the windows appear in the viewing area.



Advanced procedures

There are several procedures available while monitoring:

- Changing monitoring sources. Audio and video stream can be monitored separately:

- To stop video translation and listen only the audio stream click **Watching video** on the media player toolbar to disable it.
- To stop audio translation and play only the video stream click **Listening to audio** on the media player toolbar to disable it.

- Volume adjustment. Move the slider on the playback control panel to adjust the volume of audio stream.

- Viewing in the full-screen mode:

- Click **Fullscreen** on the playback controls panel or press Alt+Enter or double-click anywhere in the player window area to switch to full-screen mode.
- To exit from the full-screen mode press Esc or Alt+Enter or double-click anywhere in the player window area.
- To scale the image press and hold the Ctrl key while rolling the mouse wheel.

- Viewing in the original size. To scale image to the original size click **Original size** 1:1 on the playback controls panel. To fit the image to the screen click **Fit to screen** .

- Viewing a user details. Click **Show user details** on the user panel to expand it and display user information.

- Hiding the audio oscilloscope panel. To close audio oscilloscope panel click the **Close** button on the panel or click to clear the **Display the audio oscilloscope** check box available from the context menu (right-click anywhere in the media player area). To display the panel right-click anywhere in the media player area and click **Display the audio oscilloscope** on the context menu.

See also: *Options*

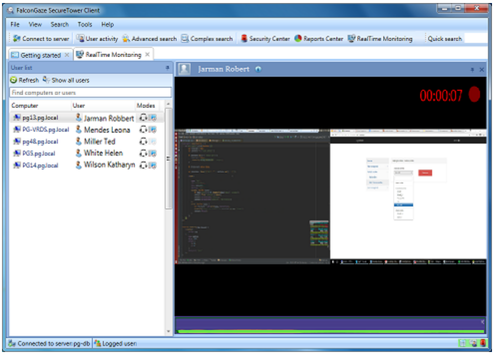
9.2 Recording monitoring data

Real-time recording is available for audio and video streams monitoring results. The media file with data can be saved manually by Client console user to the default location if the custom save location was not specified instead. To familiarize with default settings and change default file save path, see *Quick tips for results viewing*.

To start recording:

1. Establish connection with the particular user workstation as described in *Monitoring startup*.

2. Click **Record** ● on the playback controls panel. The record function is also accessible while translation.



Computer	User	Modes
pg13.pg.local	Jarman Robbert	
PG-VRDS.pg.local	Mendes Leona	
pg48.pg.local	Miller Ted	
PG5.pg.local	White Helen	
PG14.pg.local	Wilson Katharyn	

3. To discontinue recording click **Stop** recording ■ or **Stop** playback ■ if interrupting of translation is necessary as well. Recorded data will be saved.

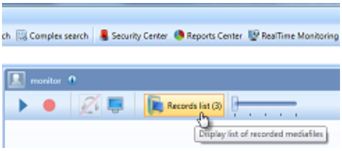
Records playback

Records of monitoring data can be opened with most of media player (in some cases the additional media codec must be installed).

1. To playback an existed record in the Client console:

2. Connect to the workstation of user whose records it's necessary to play.

3. Click **Records list** on the playback controls toolbar.



4. Click the necessary file link in the list of records. The file will be opened with the default media player.

To show record in the folder click **Open folder** next to the file link.

To delete record click **Delete** .

Click **Close** when finish with records list.

9.3 Options

To organize the window space the undocking, docking, pinning to the margin and auto hide options are available for panels in the monitoring window.

A panel title is used during work with the procedures.

Panels auto hide

The user list and media player window panels can be hidden automatically when the mouse pointer leaves its area:

- To enable the automatic hiding functionality click **Auto hide** / displayed within the panel's caption or click **Auto hide** on the panel context menu. The panel will then be hidden and will only be displayed when you mouseover the panel title in the corresponding margin.
- To activate the panels click their captions. The active panel even if it has its auto hide feature enabled is not automatically hidden when the mouse pointer leaves its area.
- To disable the automatic hiding functionality mouseover the panel title and then click the auto hide button again. The panel will be docked to the corresponding margin.

The automatic hiding functionality is activated for playback controls panel by default:

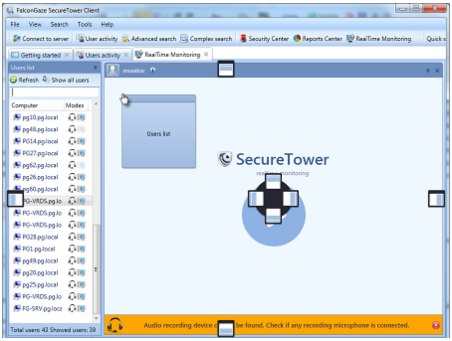
- To disable the auto hide function mouseover the top margin of the player window until the panel appears and then click **Pin** on the panel. The panel will be pinned to the top margin.
- To hide the panel click **Pin** again.

Docking to a margin

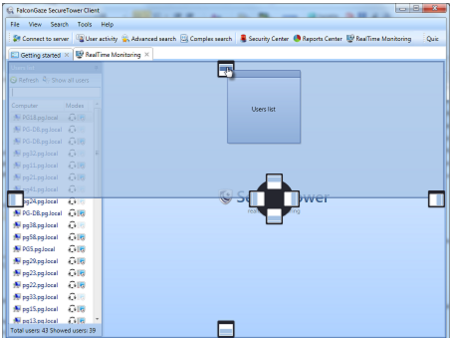
Panels can be docked to the top, left, bottom or right margin of the monitoring window or to another panel.

To dock panel:

- Click in the panel title bar and drag the panel out to display it in a separate window.



- Drag it onto one of the light blue location icons. When you are dragging a panel light blue "location icons" will appear on each side of the monitoring window. Drag the mouse cursor onto one of these icons to dock the pane on that side of the window.



Making the media player panel floating

To display a media player panel as a separate window double-click on it's title bar or drag it out of the program window or click **Float** on the panel context menu.

10 Annex

List of controlled file extensions:

Adobe Acrobat (*.pdf)

Ami Pro (*.sam)

Ansi Text (*.txt)

ASCII Text

ASF media files (metadata only) (*.asf)

CSV (Comma-separated values) (*.csv)

DjVu

DBF (*.dbf)

EBCDIC

EML files (emails saved by Outlook Express) (*.eml)

Enhanced Metafile Format (*.emf)

Eudora MBX message files (*.mbx)

Flash (*.swf)

GZIP (*.gz)

HTML (*.htm, *.html)

JPEG (*.jpg)

Lotus 1-2-3 (*.wk?, *.123)

MBOX email archives (including Thunderbird) (*.mbx)

MHT archives (HTML archives saved by Internet Explorer) (*.mht)

MIME messages

MSG files (emails saved by Outlook) (*.msg)

Microsoft Access (*.mdb)

Microsoft Access 2007 (*.accdb)

Microsoft Document Imaging (*.mdi)

Microsoft Excel (*.xls)

Microsoft Excel 2003 XML (*.xml)

Microsoft Excel 2007 (*.xlsx)

Microsoft Outlook Express 5 and 6 (*.dbx) message stores

Microsoft PowerPoint (*.ppt)

Microsoft Rich Text Format (*.rtf)

Microsoft Searchable Tiff (*.tiff)

Microsoft Word for DOS (*.doc)

Microsoft Word for Windows (*.doc)

Microsoft Word 2003 XML (*.xml)

Microsoft Word 2007 (*.docx)

Microsoft Works (*.wks)

MP3 (metadata only) (*.mp3)

Multimate Advantage II (*.dox)

Multimate version 4 (*.doc)

OpenOffice version 1, 2, and 3 documents, spreadsheets, and presentations (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (includes OASIS Open Document Format for Office Applications)

Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw)

TAR (*.tar)

TIFF (*.tif)

TNEF (winmail.dat)

Treepad HJT files (*.hjt)

Unicode (UCS16, Mac or Windows byte order, or UTF-8)

Windows Metafile Format (*.wmf)

WMA media files (metadata only) (*.wma)

WMV video files (metadata only) (*.wmv)

WordPerfect 4.2 (*.wpd, *.wpf)

WordPerfect (5.0 and later) (*.wpd, *.wpf)

WordStar version 1, 2, 3, 4, 5, 6 (*.ws)

WordStar 2000

Write (*.wri)

XBase (including FoxPro, dBase, and other XBase-compatible formats) (*.dbf)

XML (*.xml)

XML Paper Specification (*.xps)

XSL

XyWrite

ZIP (*.zip)