Going Global with Security
falcongaze™

SecureTower™

Installation Guide

Contents

1. Product Overview

SecureTower is a complex software product for ensuring internal information security through network traffic interception and analysis. This solution enables enterprises to control the leak and undesired disclosure of confidential information over the internet by intercepting such information as incoming and outgoing e-mail, chat in instant messengers, transmitted documents, files, viewed web pages, etc.

2. Product Components

The product consists of several components, each of them responsible for a certain task, which presents a possibility of an interception system scaling and ensures its reliable functioning even in the environment of a heavily loaded network.

The product has client-server architecture. The server-based part of the product consists of interception and database servers, data processing server (which includes search and indexing service, Security Center, and user identification service), mail processing server and endpoint agents control server. The client-based part of the product includes administrator and security officer consoles that serve as the program's GUI.

2.1. Server-based Components:

2.1.1. Interception Server

The main system component is a traffic interception server. This server is responsible for capturing traffic from the network interface card of a dedicated server (the so-called interception point) and analyzing it.
The information retrieved as a result of traffic analysis is saved to the database.

2.1.2. Database server

The data retrieved by the interception server (e-mail and chat messages, files, etc.) are saved to the Microsoft SQL Server, Oracle, PostgreSQL or SQLite DBMS. These data are used by the search service for building and updating search indexes and are accessed when specific documents need to be viewed.

2.1.3. Data processing server

Data processing server includes several services: search and indexing service, security center, user identification service and license server.

2.1.3.1. Search and Indexing Service

The program's search service enables conducting quick full-text search within the intercepted data, as well as text retrieval subject to the context of the intercepted data (by mail, by data of instant messenger clients, etc.).

The service is responsible for indexing and search functions.
After being saved to the database, all the intercepted information is indexed. Index service is responsible for information retrieval out of complicated data formats and for processing text documents in order to convert them into a searchable content. To accelerate full-text search, the index service creates indexes of the intercepted data including a list of all the words that the data contain together with their location within the indexed document. A data index contains not only the list of keywords of the intercepted data, but also such their attributes as message subject and size, e-mail address, UIN, IP-address, etc. The accuracy of the search results displayed depends on the customizable indexing frequency.

Searching and viewing search results is available in the client-based part of the product.
The search service accepts requests from the security officer console, performs search operations within index files, and submits results to the console. The search service efficiency relies on the interaction with the search index owing to which searching is carried out within the structured document images, and not the original intercepted data.

2.1.3.2. Security Center

Security Center enables receiving security breach notifications. The intercepted data are analyzed in the automatic mode based on the list of assigned security rules. The analysis means conducting a search within the intercepted data by requests developed in accordance with security rules. Upon detecting files or data satisfying the stipulations of the security department rules, the center sends notifications to a specified e-mail address.

2.1.3.3. License Server

The license server is responsible for controlling the use by an end-user of the product in compliance with the terms and conditions of the license agreement and the license dongle provided. The server receives and processes the license information written in the dongle and, based on this information, blocks or permits access to the application components.

The license information includes the following types of restrictions: number of workstations that are a workplace of specialists whose network activities are monitored and controlled by the software (which can technically be IP addresses, working sessions if there is a computer terminal in the local area network, etc.), number of modules (the number of server components copies working simultaneously), data types under control (e-mails, instant

messengers, web traffic, endpoint activity), the maximum number of days of the product's permitted use (term of use) or the product expiration date, after which the application shall no longer be accessible for use. In most cases time restrictions are not applicable for licensed copies of the product as they are designed to restrict the period of use of trial or test versions of the application.

Without a license dongle, the following license information is used by the system: the number of workstations – 25, the number of modules – 1 copy of each server component, the term of use – 30 days from the moment of first product startup. Upon expiration of the above term, the application's functions shall be inaccessible.

When the hardware license dongle received by an end-user in accordance with the license agreement or supply contract connects to the license server, the latter reads new security data from the dongle that are used within the entire period of use of the application. The license dongle must at all times be connected to the computer with the license server installed, since the server checks for a dongle on a regular basis and, if there is no dongle, it uses the license information described above.

The following components are licensed: interception server, data processing server? Mail processing server and endpoint agent control server. After installation of these components, their connection to the license server should be configured (in the administrator console). Since the Licensing server is part of the Data processing server, there is no need to manually configure their connection. For all other components, you need to setup connection to the same machine where the Data processing server is installed. Without connection to the license server, the components are inaccessible for use.

2.1.4. Endpoint agent control server

This server is used for centralized installation and management of agents for Skype and SSL traffic interception. It includes an endpoint agent control server and agent modules. The server checks the presence of workstations in the network and, depending on the selected installation strategy, implements remote installation of agents to network computers invisibly for their users. Endpoint agents keep track of data exchanged by Skype users or transferred over SSL protocols and forward them to the server for processing. The server, in its turn, sends the information to the database.
Besides, the Endpoint agent control server monitors the status of all the agents installed across the network, and, in case some agents are not present, failed or were removed by some users, it will automatically reinstall the agents on the corresponding workstations.

2.1.4.1. Endpoint agents

Endpoint agents keep track of data exchanged by Skype users or transmitted over SSL protocols and transfer them to the Endpoint agent control server.
SSL traffic interception through agents is based on a certificate replacement principle. An endpoint agent automatically imports the **Falcongaze** root certificate into the certificate storage of Mozilla Firefox, Mozilla Thunderbird and Opera, as well as of the programs that use Windows certificate storage.
As for the rest of the programs or web-services, when the endpoint agent attempts to replace the certificate, the program displays to the user a notification that an invalid certificate is used. At this point, the user can add the new certificate to the list of trusted certificates in order to use the program. Otherwise, the program or web-service will not start.
There are also programs or web-services that cannot operate with their certificates replaced. Such sessions will not start, and no data will be transferred over these channels. However, the system allows exclusion of certain processes or servers (by IP address) from certificate replacement.

2.1.5. Mail processing server

This server component is responsible for the interception of mail servers' traffic. The system can be integrated with mail severs based on MS Exchange, Lotus Domino, Kerio Connect and other mail server software using POP3 and SMTP protocols. The traffic is intercepted in the following way: a special user account should be created to journal all correspondence, which is then automatically collected by **SecureTower** for subsequent analysis.

2.1.6. Authentication and user information service

The service enables managing local network users data, creating user cards, unite users by certain user groups, as well as is responsible for providing user information upon request.
The program applies a user card system in which each local network user is assigned with an identification card containing personal and contact user information (name and last name, job title, e-mail addresses, ICQ UINs, user accounts in IM programs, user names in social networks, etc.). Besides, user cards provide group membership information.
The user database is developed and maintained by an administrator with the help of the Administrator Console (see section **2.2.1 Administrator console** of this Guide).
The service supports import of users from the local network domain controller (Active Directory).
This service is installed together with any server component of **SecureTower** and cannot be installed separately.

2.2. Client-based Components

The client-based part of the product includes administrator and security officer consoles that serve as the program's GUI.

2.2.1. Administrator Console

Administrator console is used for adjusting operation settings of all the product's services: Interception, Search and Indexing, Endpoint Agent Control, and User Identification services. One can set and change interception parameters and indexing frequency. The console provides access to setting various filtering options for data capturing.

It also allows one to view capture statistics in a real-time mode, arrange delivery of notifications about the system operation (such events as interception system or database overloading) and install remote endpoint agents to network computers to arrange interception of Skype and encrypted traffic.

2.2.2. Client Console

The Client console is the main graphic representation of the program that provides tools for using the program's features. The console is used to analyze traffic of certain users, carry out full-text keyword search, and view the captured data in a convenient presentation.

Apart from that, one can configure Security Center performance and delivery of security breach notifications and view the results of its work (special user privileges are required to enable this function).

2.3. Product's Component Relations Diagram

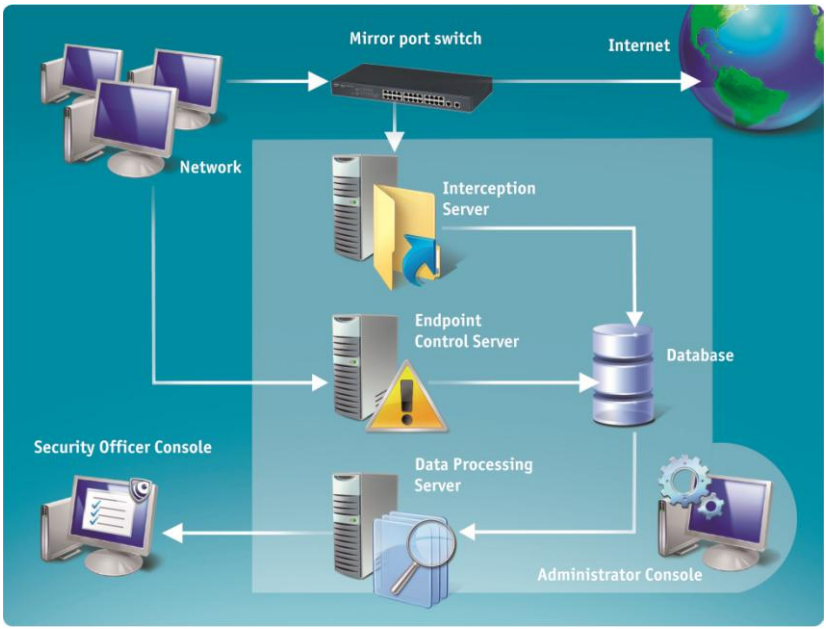


Figure 1. The product's component relations diagram

2.3.1. The system's operation algorithm (Figure 1):

1. The entire external traffic is replicated to the interception server by a mirror port switch.
2. An interception server analyses the received traffic to retrieve the necessary information from it (such as e-mail or chat messages, files, etc.) and save it to an external storage directory.
3. The Endpoint agent control server installs agents on local network computers in a remote mode. The agents monitor data exchanged by Skype users or transferred over SSL protocol and forward them to the server for processing. The server, in its turn, sends the information to the database.
4. The Endpoint agent control server can work regardless of whether the rest of the system components are installed, except for the database and administrator console.
5. The data processing server performs indexing of information stored in the database and saves indexes into the data processing server storage. Later on retrieval shall be performed only within the search index files but not the entire scope of information

contained in the database. Security Center (installed on the data processing server) interacts with the search service and security officer console. The service submits automatic search requests to the search service. Upon detecting data satisfying the stipulations of the security department rules, the Security Center generates reports and sends them to specified e-mail addresses. The security officer console is used to adjust the necessary operation settings of the Security Center, to assign the list of search rules, and to view the log of Security Center performance events.

6. Operation of the security officer console is based on interaction with the data processing server. The search service processes requests generated by the security officer console and presents search results to the user.
7. Administrator console is used for setting operation parameters for all the product's components: Interception, Data processing, Endpoint Agent Control, and User Identification services.

3. System installation guidelines

To arrange traffic interception with the help of the program, the whole traffic should be redirected to one or several network interface cards of servers specially allocated for this purpose (so called interception points). The ways to redirect the traffic transmitted within a LAN to a certain network adapter vary depending on the LAN equipment and layout.

3.1. Ways of traffic redirection to the interception point

3.1.1. Network monitoring using hubs

In a LAN using hubs, all the incoming packets received by a hub are broadcasted to all the ports regardless of their destination address (Figure 2). Network adapters of local workstations are normally configured to receive only the packets they are addresses to, while ignoring the rest of the packets sent. Interception server puts the network adapter into the mode that enables it to receive packets addressed to other ports, meaning the whole traffic. The network card of an interception server will receive the data of any computers connected to the hub.

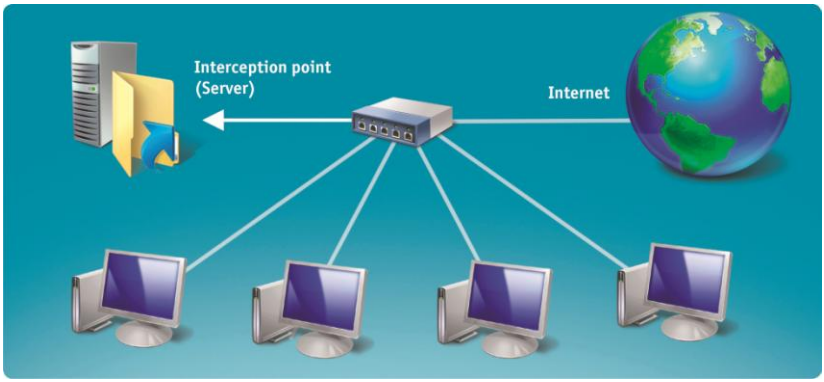


Figure 2. Network monitoring using a hub

Monitoring network using a hub is not considered rather a convenient option since hubs produce excessive pressure for the network by unreasonably duplicating traffic when broadcasting it to the ports it is not addressed to.
It is also important to remember about the so-called “intellectual”, or “commuting”, hubs when arranging monitoring of LANs using hubs. In practice, such hubs actually turn out to be switches although their accompanying documentation might have no such indication.

However, using managed switches supporting a mirror port function is the most recommendable practice for network monitoring, therefore, we strongly advice that you install such a switch even if you already have a hub.

3.1.2. Network monitoring using switches

Switches are more intellectual devices than hubs as they analyze all the incoming packets by comparing the source and destination MAC-addresses and forward the packets only to the ports they are addressed to. There are switches that support port mirroring – a function that enables a switch to replicate all the incoming traffic to a certain port.
Thus, network monitoring is possible upon connecting a traffic interception server to the port of a managed switch to which traffic is replicated (Figure 3). This method of traffic interception is deemed most preferable from the viewpoint of performance efficiency.
There are certain ways to capture traffic without using a managed switch. For instance, certain network attacks might cause a switch to behave as a hub and to start broadcasting traffic to all the LAN ports. However, these methods are not recommendable.

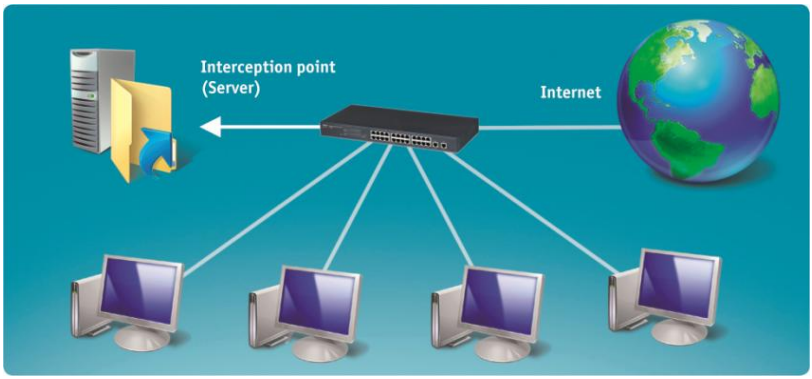


Figure 3. Network monitoring using a switch

3.1.3. Monitoring a wireless network

In case of a wireless network, monitoring can be arranged by a physical connection of a wireless access point to a network device (hub, switch, or router) that has one of the above implementations of traffic redirection to a traffic interception point (Figure 4).

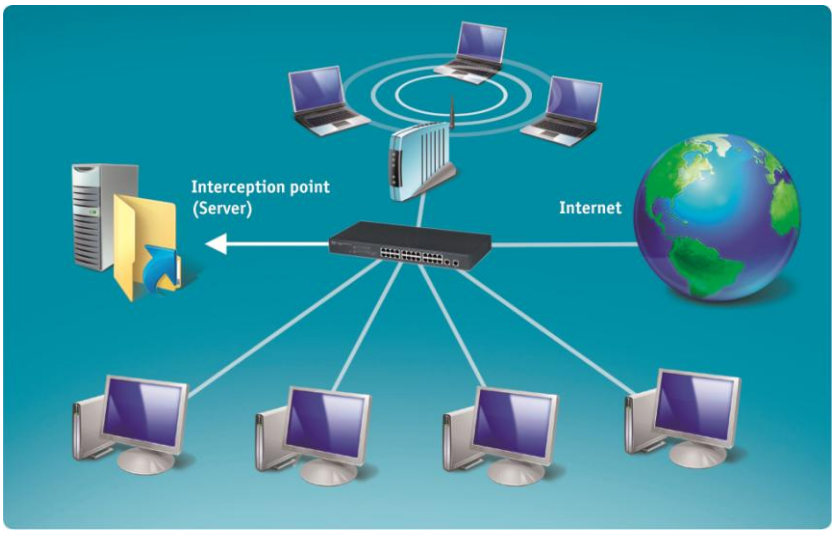


Figure 4. Wireless network monitoring

3.2. Interception point location

The locations of an interception point vary subject to a LAN layout and workload, as well as to which traffic is to be observed (the one transmitted within the LAN, within a certain LAN segment or exchanged between workstations and Internet).

In most instances, an interception point is installed between the LAN and internet, and between certain LAN segments in case with an interception system scaling. It is important to remember that in LANs that have a gateway, installing an interception point between the gateway and internet is not recommendable. Otherwise, all the packets will have the same IP-addresses – that is the IP-address of the network gateway. This will make it impossible to define the workstation to which any given packet belongs. Therefore, it is advised that the interception point is located between the LAN and the gateway.

In other cases, the interception point can be installed:

3.2.1. Between the LAN and Internet

3.2.1.1. In small LANs

Locating an interception point in LANs with a simple layout where all the workstations are connected to the mirror port device enables capturing the whole internet-traffic as well as data exchanged between local workstations. In this case, it is sufficient to connect the network device to a computer to which the entire network traffic will be redirected (Figure 5).

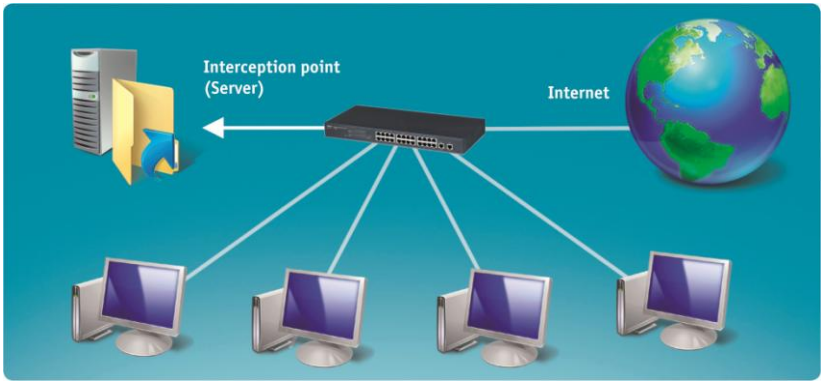


Figure 5. Interception point location in a small LAN

3.2.1.2. In big LANs

In a multi-segment LAN, the interception point is normally inserted between the network and Internet. In such a case, only external traffic is captured, while the data transmitted within the LAN without passing through the network device will not reach the interception point (Figure 6). If monitoring data exchanged between local workstations is important, system scaling can be applied, for example, installing additional interception points in specified LAN segments (see Figure 7).

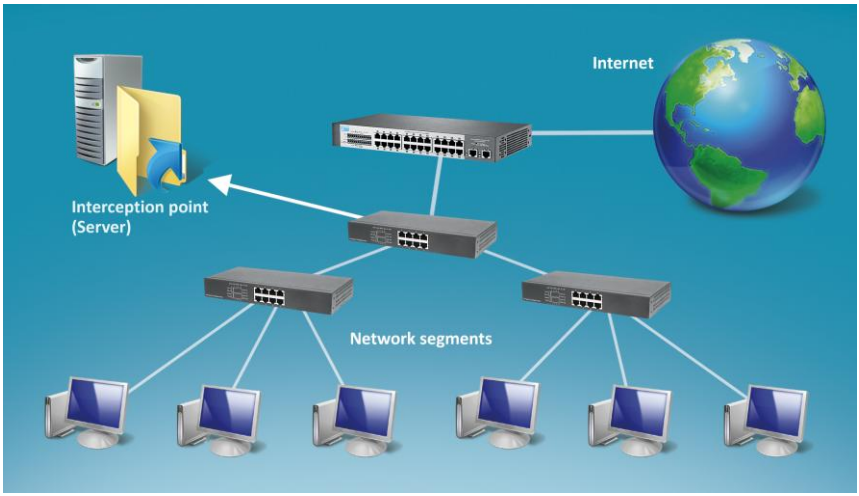


Figure 6. Interception point location in a big LAN

3.2.2. Between LAN segments. System scaling in big LANs

If monitoring data exchanged between local workstations is important, system scaling can be applied, for example, installing additional interception points in specified LAN segments.

Interception system scaling is also suggested in order to avoid system overloading when monitoring a LAN with a complicated layout and a great number of workstations. System scaling allocates traffic interception and processing workload to several physical servers.

Installation of several interception points within separate LAN segments will allow monitoring traffic transmitted between local workstations of a huge LAN and in general will enhance the reliability and performance efficiency of the interception system (Figure 7).

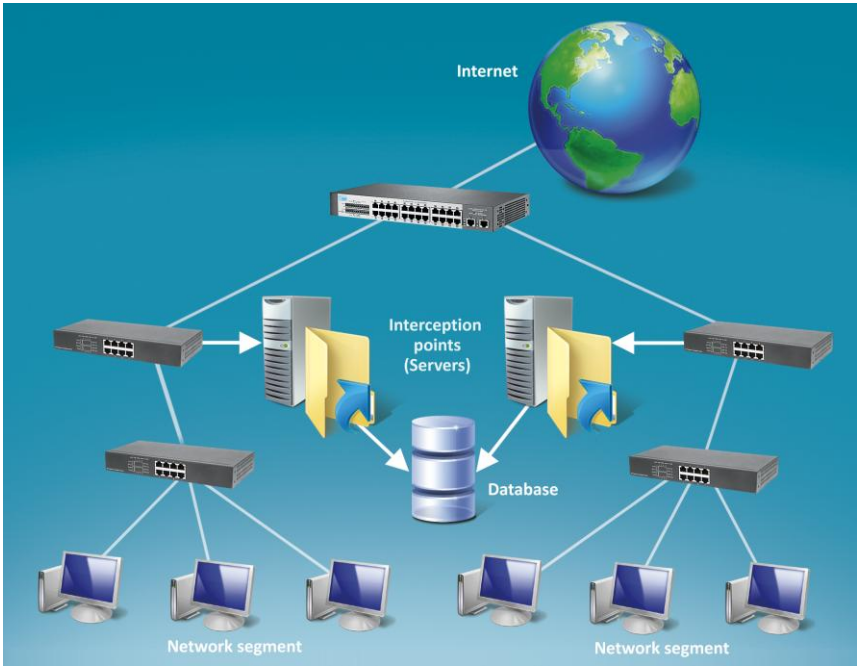


Figure 7. Interception system scaling

3.3. Recommended system component layout

The specifics of interception system installation depend on the LAN's individual characteristics, such as its workload, number of workstations, capacity of network and its segments, computing resources of the server, etc.

Below is an example of a recommendable installation of the product's components in an existing LAN.

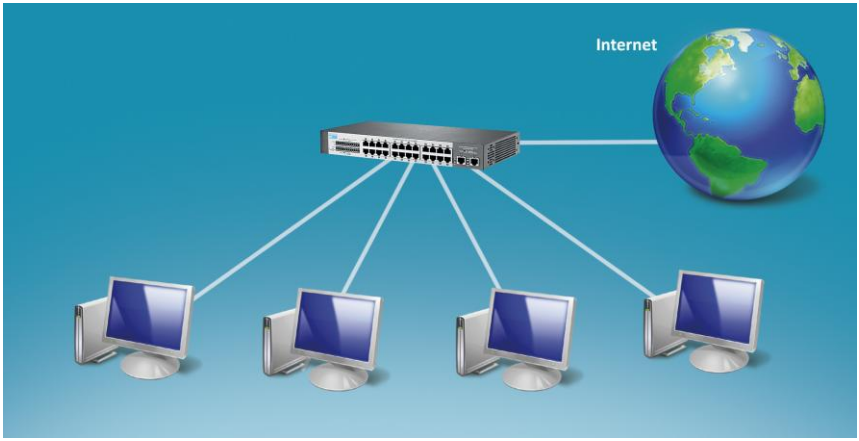


Figure 8. The simplest example of an existing LAN (before the interception system installation).

Both workstations (in case with a small LAN) and entire sub-networks (in a big LAN) can be connected to the network device).

In case of the shown LAN, an additional switch that supports port mirroring is installed between the existing switch and internet with the rest of the services being connected to the managed switch. In that, all the workstations can equally be connected both to the existing switch and to the mirror port switch (Figure 9).

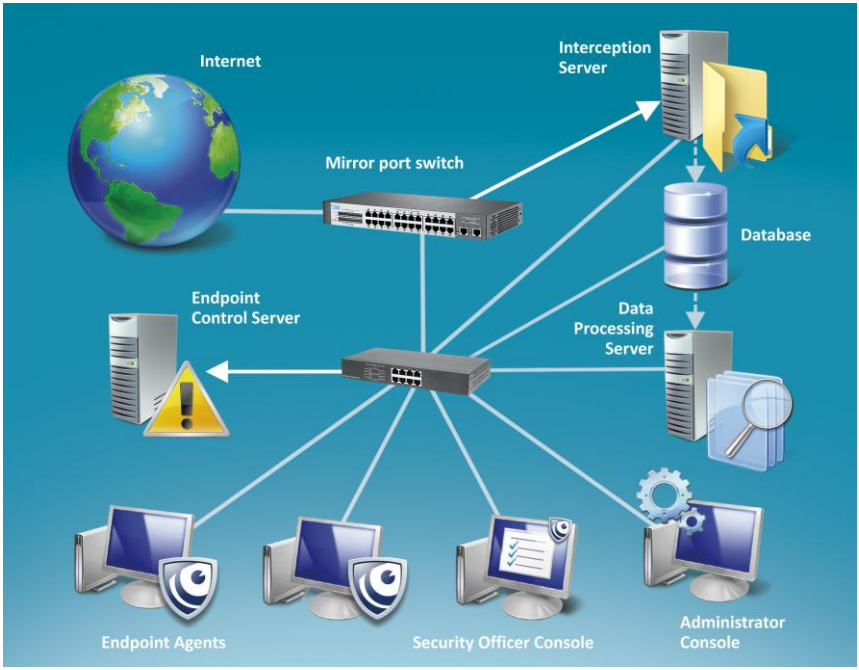


Figure 9. Interception system layout in an existing LAN

Such a layout will allow capturing the whole external traffic. The traffic is replicated to the interception server over the mirror port.

The main considerations upon the above system installation layout:

1. The major recommendation upon the system installation is allocating a dedicated server (or several servers) for the system's main component – an interception server. This component is not recommended to be installed on a domain controller or server than already runs some other tasks besides interception. In such a case, in big LANs, the server's computing power for processing huge volumes of data might be insufficient during stress periods.
2. The best recommendable practice for the system components installation – installing the interception server, database, data processing and Endpoint agent control servers each on different physical servers, as well as allocating a separate LAN segment for all the services in order to avoid additional workload for the interception point upon their

traffic exchange. For this, it is important to ensure that all the four servers are connected to the existing switch and not to the mirror port switch.

3. The interception server should have two network interface cards: one – for receiving the incoming mirrored traffic, the other – to interact with the product's other services and clients.
4. The information retrieved from traffic and received from endpoint agents is saved to the database over the network. Here, it is not recommendable to direct the traffic and Skype data through the interception device since they will be passing over the mirror port once again and, thus, will create additional workload for the interception server.
5. Administrator and security officer consoles can be installed on any workstations of a LAN. Their traffic will also be intercepted.

The above layout of the system installation is recommendable as it provides optimal distribution of functions of all the product's services across the network and allows avoiding additional workload for the interception server.

4. System installation

4.1. Interception server

4.1.1. Interception server installation guidelines

Dedicated server for the interception server

The major recommendation upon the system installation is allocating a dedicated server (or several servers) for the system's main component – an interception server. This component is not recommended to be installed on a domain controller or server than already runs some other tasks besides interception. In big LANs, the server's computing power for processing huge volumes of data might be insufficient during stress periods.

Setting network adapters

The interception server should have two network interface cards: one – for receiving the incoming mirrored traffic, the other – to interact with the product's other services and clients (see Figure 9).

In order to ensure operation of the interception server, the **Large Send Offload** option should be disabled in the advanced settings of the network adapter allocated for receiving the intercepted traffic. This option is responsible for the reduction of the CPU workload upon the transmission of large IP packets. If it is disabled, IP packets are divided by the operating system into numerous 1.5 Kb sized packets before being sent to the network adapter. If this option is enabled, large IP packets are sent to the network adapter directly without being first processed by the operating system. Taking into account that the only task performed by the interception server is receiving and processing network traffic, there is no need in enabling this option. Disabling the **Large Send Offload** option is a critical requirement for the operation of the interception system, since the interception server does not support working with large IP packets, which may lead to some part of traffic being skipped.

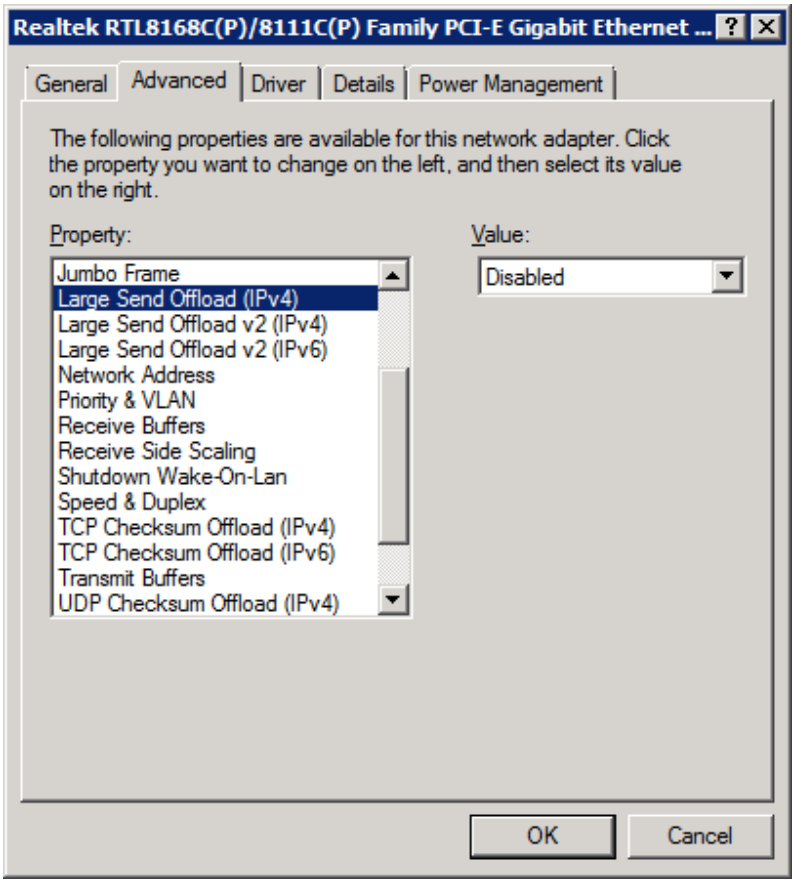


Figure 10. Network adapter advanced settings window

4.1.2. Minimum system requirements for the Interception server

Processor: Pentium® 2 GHz and higher
Two network adapters: 100 Mbit/1 Gbit
RAM: Minimum 4 Gb (+0.5 Gb for each 100 monitored workstations)
HDD: 100 Mb of free space
Operating system: Microsoft® Windows® Server® 2003/ Server® 2008 (x86 or x64)

4.1.3. Recommended system requirements for the Interception server

Processor: Xeon® 2 GHz and higher
Two network adapters: 100 Mbit/1 Gbit
RAM: Minimum 4 Gb (+0.5 Gb for each 100 monitored workstations)
HDD: 100 Mb of free space
Operating system: Microsoft® Windows® Server® 2008 R2 (x64)

4.2. Database installation guidelines

The program supports the following DBMSs: Microsoft SQL Server 2005/2008, Postgre SQL and Oracle.
The DBMS is recommended to be installed on a separate physical server of high capacity, and on a server cluster – upon especially huge traffic volumes. In that, it is advised that the data exchanged between the database and other services of the product are transmitted over high-speed channels. Otherwise, the interception server might be overloaded due to the insufficient speed of the information transfer and storage to the database.

The traffic flowing from the database to the rest of the system's components should not be directed through the interception device. Otherwise, it will be passing over the mirror port once again and, thus, will create additional workload for the interception server.

4.3. Data processing server

4.3.1. Data processing server installation guidelines

Data processing dedicated server

As applicable for the other product components, the data processing server is recommended to be installed on a different physical server. The data processing server includes indexing and search services, Security Center, and user identification service. These components are all to be installed on a single physical server.

Direct connection to the database

While the data processing server works directly with the database, it should be connected to the DBMS. In that, it is advised to ensure that the information retrieved by the search server from the database does not pass through the traffic-mirroring device.

Indexing as the data are received

To guarantee fast indexing of traffic data, it is advised to use a high-capacity server. In stress periods, the search server's computing power should be sufficient to perform operative updating of search index files as new information is received by the database.

Fast data operations

To ensure storage reliability for the index data as well as an improved input/output performance, it is recommendable to use a high-speed fault-tolerant storage on a data processing server. It is preferable that the HDD where data indexes are stored to could immediately save all the updates of the search index file and ensure their fast output upon being accessed by the search service.
The technology of RAID-arrays can be applied with this purpose.

Hard drive space

Data indexes occupy minimum one thirds of space of the data being indexed, therefore, it is important to allow for the availability of the corresponding free space on the data processing server's hard drive.

Virtual machine requirements

In case the server is installed on a virtual machine, make sure that the virtual machine you use supports tunneling of physical USB devices to the virtual system. This is required to ensure operation of the license server that reads license information from a license dongle.

4.3.2. Minimum system requirements for the Data processing server and Endpoint agent control server

Processor: Pentium® 2 GHz and higher
Network adapter: 100 Mbit/1 Gbit
RAM: minimum 4 Gb
HDD: 110 Mb of free space for the program files and minimum 30% of the intercepted traffic space for index files
Microsoft .Net Framework: 4.0 and higher (for Endpoint agent control server)[1]
Operating system: Microsoft® Windows® Server® 2003/ 2008/ 2012 (x86 or x64)

[1] During the installation of Microsoft .Net Framework 4.0 you may see the following message: "You must install the 32-bit Windows Imaging Component (WIC) before you run Setup. Please visit the Microsoft Download Center to install WIC, and then rerun Setup." In this case visit http://go.microsoft.com/fwlink/?LinkId=162643 to download and install the "wic_x86_enu.exe" file. Once it is installed, rerun .NET Framework 4 setup.

4.3.3. Recommended system requirements for the Data processing server and Endpoint agent control server

Processor: Pentium® 2 GHz and higher
Network adapter: 1 Gbit
RAM: minimum 4 Gb
HDD: 110 Mb of free space for the program files and minimum 30% of the intercepted traffic space for index files
Microsoft .Net Framework: 4.0 and higher (for Endpoint agent control server)
Operating system: Microsoft® Windows® Server® 2008 R2 (x86 or x64)

4.4. Endpoint agent control server installation guidelines

The Endpoint agent control server can work regardless of whether the rest of the system components are installed, except for the database and administrator console. To work with it, it is sufficient to configure connection to the database (with the help of the Administrator console) to which the information received by the server from agents will be stored.
If there is an interception system installed in the network, it is not recommendable to direct the data received by the server from agents through the interception device since they will be passing over the mirror port once again and, thus, will create additional workload for the interception server.

Operating system for endpoint agents: Microsoft® Windows® XP and higher.

For the system requirements to the Endpoint agent control server, see sections 4.3.2 and 4.3.3 of this Guide.

4.5. User interface (Administrator and Security Officer Consoles)

4.5.1. Minimum system requirements for the user interface

Processor: Pentium® 2 GHz and higher
Network adapter: 100 Mbit/1 Gbit
RAM: Minimum 4 Gb RAM
HDD: 300 Mb of free space
Microsoft .Net Framework: 4.0 and higher
Video adapter: supporting DirectX 7.0 and higher
Operating system: Microsoft® Windows® XP/ Vista / 7 / 8/ Server® 2003/ Server®2008 (x86 or x64)

4.6. System Installation Wizard

The product supports work on Windows XP, Windows 2003 Server, Windows 7, Windows 2008 Server (or higher). Depending on the operating system the product is installed on (x86 and x64 platforms), the program is supplied with 32- and 64-bit installation packages.

The Windows Installer that is included into the Windows operating system is used for the program installation. The minimum requirements for the system installation: Windows Installer 3.0, Net Framework 4.0 (required for all the system components, except for the interception server). In case .Net Framework is not installed on your system, it can be installed by running **dotNetFx40_Full_x86_x64.exe** from the **Common** folder.

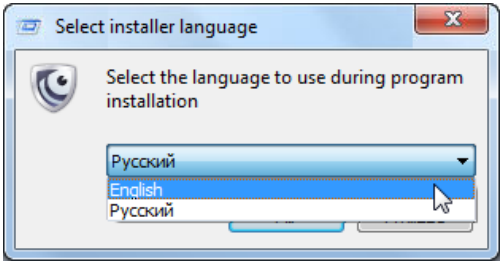
The Wizard will help you to install the product components to the computer on which the wizard is run. Taking into consideration the possibility of the system scaling*, its components can be installed on different physical servers. In such a case, the installation wizard should be individually run on the corresponding computers in each instance of installing some component onto a different server.

***Note:** In an isolated case or if you have a Small Office solution, all the system components can be installed on one server. Correspondingly, their installation shall be performed with the help of the wizard run on a single computer.

4.6.1. Installation of Falcongaze SecureTower system

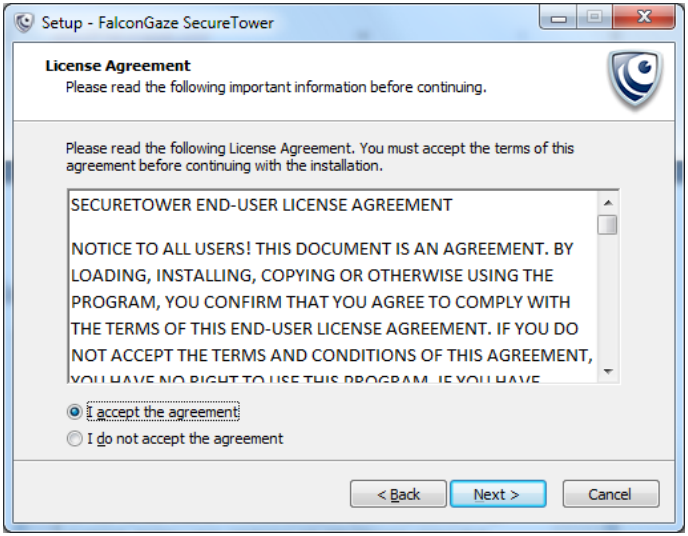
To start the product Installation Wizard, run **FalcongazeSecureTowerSetup.exe** from the distributive package.

1. When starting the Installation Wizard, you will see a dialog box in which you are to select a language to use while installation of the software. Choose one of the two available languages – Russian or English – from the dropdown menu and click **OK**.

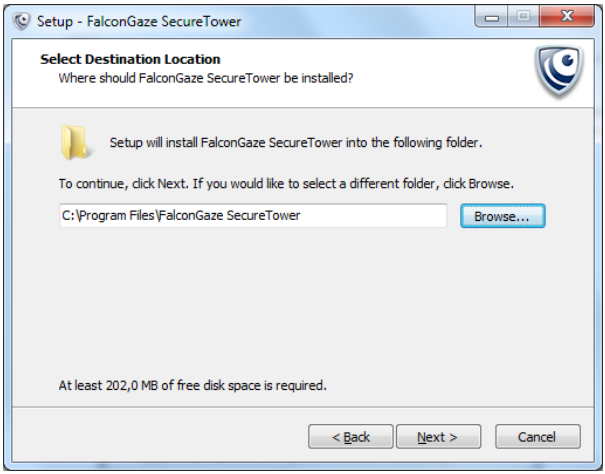


2. After you have chosen the installation language, a welcome screen will open in which you will be offered to continue or cancel the installation. Click the **Next** button if you wish to continue the installation of the Falcongaze SecureTower program to your computer.

3. Before installing the program, you will be requested to read the End-User License Agreement. If you accept the license agreement conditions, select the corresponding option and click **Next**.

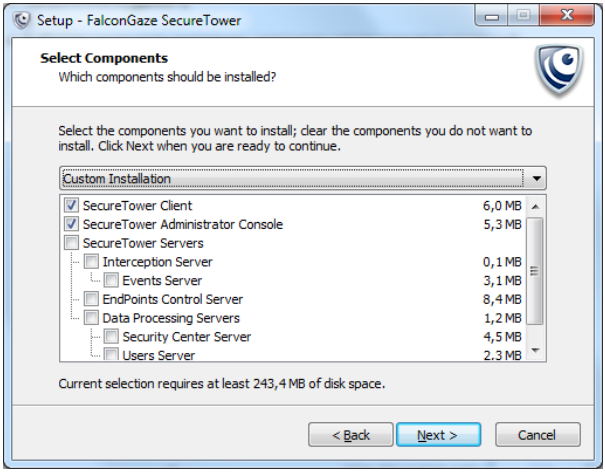


4. In the next window choose the directory to install **SecureTower**. To change current directory click the **Browse** button, navigate to the necessary folder in the folder browsing dialog box and click **OK**.

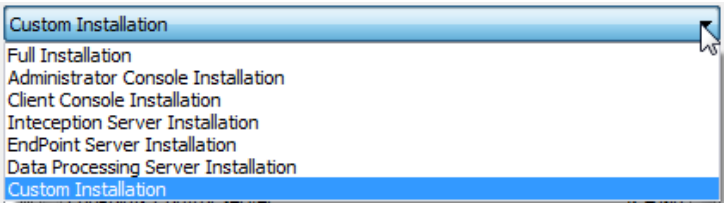


5. Click **Next.**

6. In the next window you will be offered to select the components of the program that you want to install on the local computer.

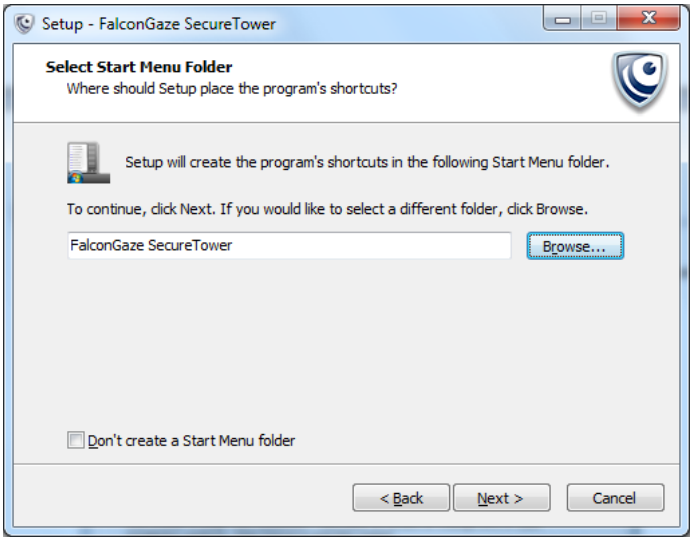


The components to install can be selected from the dropdown menu of installation options, or manually by checking the corresponding checkboxes:



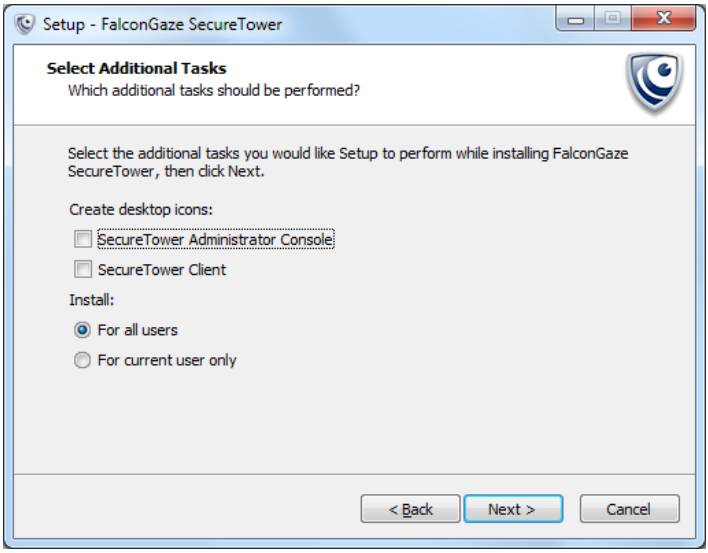
7. After selecting the needed components, click **Next.**

8. In the next window you will be offered to select a folder in the **Start** menu to store the program shortcuts. To change the current directory, click **Browse**, navigate to the necessary folder in the folder browsing dialog box and click **OK**. If you do not want to create any shortcuts in the Start menu, check the corresponding option in the lower part of the window.



9. Click **Next**.

10. In the next window you are offered to specify what shortcuts the program will place on your desktop by checking or unchecking the corresponding options. Also, choose one of the options – installation for all users or for current user only – by switching the radio button.



11. Click **Next**.

12. Click **Install** to install SecureTower on your computer or **Cancel** to cancel the installation. If you wish to change any installation options, click **Back.**

13. Once the installation of SecureTower is complete, click **Finish** to exit setup.

If you have installed the data processing server that includes the license server, after finishing the installation of the program you need to connect the license dongle (if any) to the server.

After this you can get down to configuring the components that you have installed or you may run the program installation wizard on another computer to continue the installation of the rest of the system components or their copies.

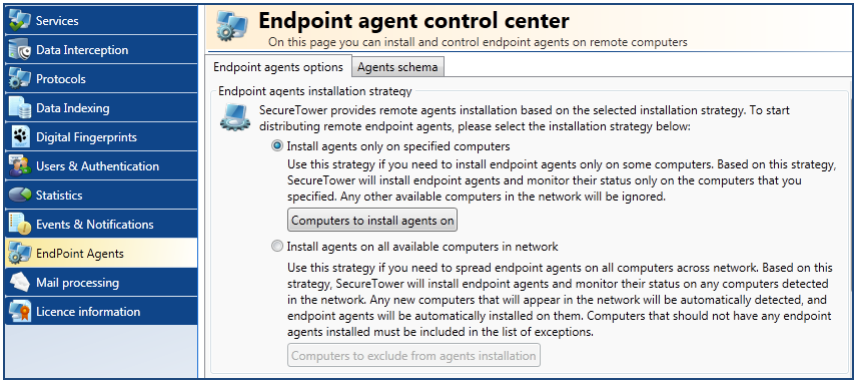
If you have installed the client components, their shortcuts will appear in the **Start** menu (the main menu of the Windows operating system) upon the installation completion (provided you did not cancel shortcut creation in the process of installation). It is recommendable to start with running the administrator console that will help you configure the performance of all the system components in a centralized manner. To do this, open the **Start** menu of the Windows toolbar, go to **All programs** and click **Falcongaze SecureTower Administrator Console**.

After customizing the program settings or to start using the program with default settings, run **Falcongaze SecureTower Client** from the **Start** menu. For this, open the **Start** menu of the Windows toolbar, go to **All programs** and click **Falcongaze SecureTower Client**.

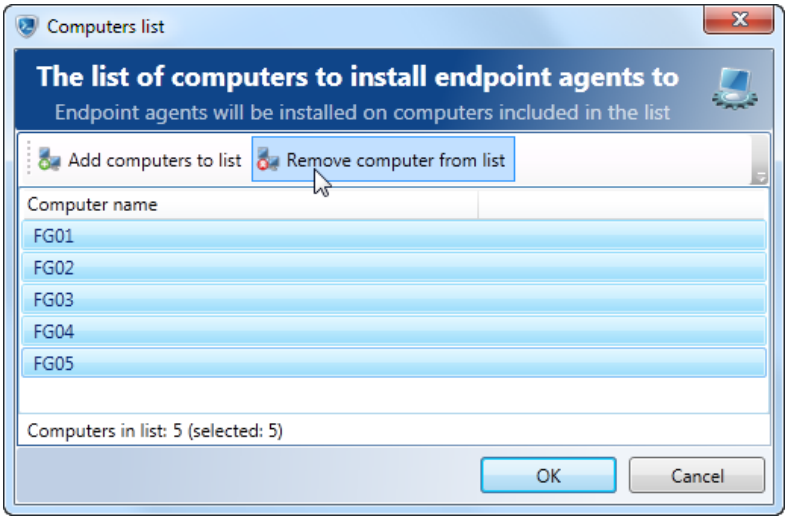
4.6.1. Uninstallation of Falcongaze SecureTower system

***Warning**: Before uninstalling **Falcongaze SecureTower** system components, it is important to remove endpoint agents from the computers they were installed on.*

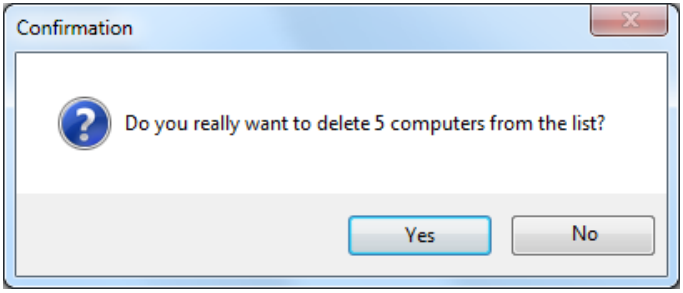
1. To remove agents from the endpoints, run the Administrator Console and navigate to the **Endpoint Agents** section.



2. To uninstall the agents you are to clear the list of computers they are installed on. To do this, click the button **Computers to install agents on.**



3. Select all computers in the list (press Ctrl+A) and click **Remove computer from list**.



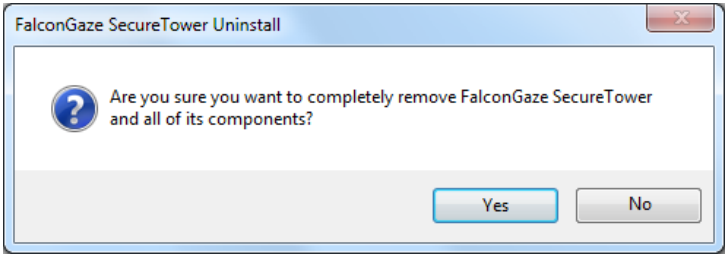
4. Confirm agent removal by clicking **Yes.**

5. Click **OK** in the **Computers list** window, and **Apply changes** button in the right lower part of the Administrator console main window.

6. Agent uninstallation can also be performed from the **Agents schema** tab of the **Endpoint Agents** section. To do this, right-click a computer name in the list and select **Remove agent and exclude computer from schema** in the context menu. Confirm agent removal by clicking **OK**, the click **Apply changes** in the lower right part of the window.

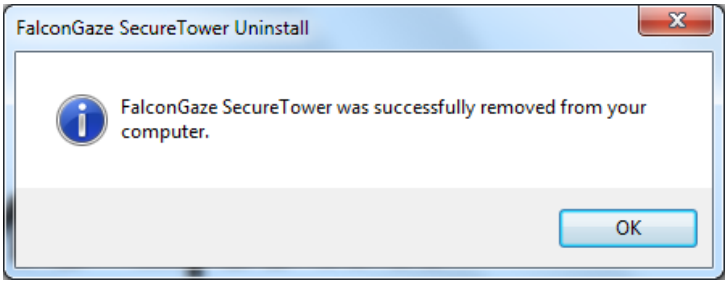
7. Make sure that agents are uninstalled from all computers they had been installed on. Upon successful removal of all agents the **Agents schema** should be clear.

8. To uninstall **Falcongaze SecureTower** system components, run the **unins000.exe** file located in the installation folder (**C:\Program Files\FalconGaze SecureTower** by default)



9. Confirm your intention to uninstall the system by clicking **Yes.**

10. Upon successful removal of all system components, a dialog window will open to inform of successful system uninstallation.



11. Click OK.

12. Repeat the uninstallation process on all computers having **Falcongaze SecureTower** server or client components installed on them.