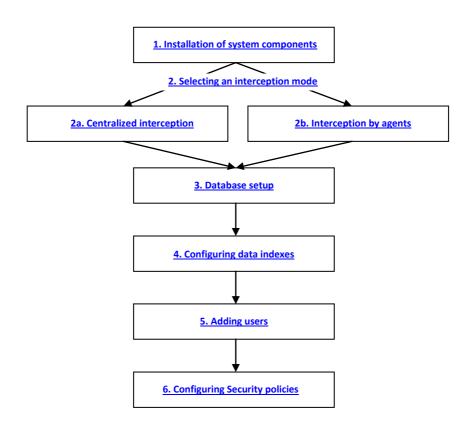


System setup process chart

The following chart represents the minimum required sequence of actions for SecureTower initial setup. For information on optional features and for detailed instructions on all system functions, refer to Falcongaze SecureTower User Guide and Falcongaze SecureTower Administrator Guide, supplied with the system installation package (the guides can be accessed by hitting F1 in the SecureTower Client and Administrator Consoles, respectively).





1. Installation of system components

- 1. When running the Installation Wizard, you will be prompted to select the components you want to install on your PC. If you want to use the entire functionality of the system, install all the components available.
- 2. After you have installed the all product components, the shortcuts for two consoles will appear in the Start menu (the main menu of the Windows operating system): Administrator Console and Client Console. The Administrator console is used for centralized setup of all system components. The **Client Console** is used to work with the data (including security policy configuration, browsing through the user activity data, search in the intercepted data archive).
- 3. When you launch the Administrator or Client Console, you will be prompted to select a server to connect to. If all the components were installed on the local computer, select the option Connect to the local computer. Click Connect to server.

Select a server	×			
Selecting the se Specify the comput	erver ter name to connect to and setup the server 💱			
Specify or select a compu	uter name to establish connection to the necessary server:			
Connect to the local	Onnect to the local computer			
Connect to the spece	Connect to the specified computer			
Computer name:	T			
	Use ping to check computer availability			
Connect to this server	on next startup Connect to server Cancel			



2. Selecting an interception mode

SecureTower system can capture network traffic in two ways: in a centralized mode (via a SPAN port of your network switch), or by agents at endpoints. When selecting an interception mode, please mind the following: centralized interception mode allows capturing only the data transmitted over non-encrypted protocols. Agents can capture all traffic - both encrypted (transferred over SSL/TLS-encrypted protocols HTTPS, FTPS, SMTPS, POP3S, IMAP4S, encrypted messenger protocols, including Skype) and non-encrypted. Besides, the agents perform additional functions for user activity monitoring - take screenshots at predefined intervals, collect statistics on application activity, etc. It is possible to use both interception modes simultaneously, but in this case you should configure agents to intercept only encrypted traffic - this will help avoid replication of non-encrypted traffic due to double capturing - first by an agent, then via the SPAN port on your network switch.



Please note that the trial version of SecureTower has a limitation to 25 controlled computers in the network. In case of both centralized interception, and interception by agents on endpoints, you need to explicitly specify the computers you wish to control (see instructions below). Otherwise, the system will intercept traffic for the first 25 computers that connect to the network and exchange any data every day. As a result, the list of controlled endpoints can vary in a random manner every day.



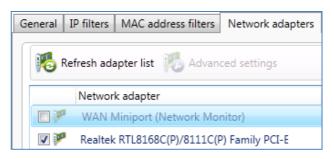
2a. Centralized interception

- Before you proceed to configuring centralized interception in SecureTower, you need to setup traffic mirroring to one of the ports (SPAN port) in your network switch (please refer to you device documentation to setup traffic mirroring) and connect the SPAN port to the network adapter on the server where SecureTower is installed.
- 2. Run the Administrator Console and go to the **Data Interception** section (select in the **left pane** of the main program window).

FalconGaze SecureTower Admin Console							
File Tools Help							
FalconGaze SecureTower Admin Console							
Services					n service		ons meters and tune up
Protocols	General		MAC addre	ess filters	Network ada	pters	
Data Indexing	Data sto	orage settir Current da	igs ta storage se	tings:			
🔮 Digital Fingerprints		Plugin n	ame:				
Users & Authentication		Server n	ame:				
Statistics		Databas	e name:				
Events & Notifications		User nar	ne:				
EndPoint Agents			С	onfigure o	data storage	Selec	t data storage

- 3. In the General tab you have to configure a database that will be used to store the traffic captured from the SPAN port. To do this, click Select data storage in the Data storage settings section, then select the type of database you wish to use (Oracle, Microfost SQL Server, PostgreSQL or SQLite) and specify additional access settings (for instructions on database setup, refer to section 3. Database setup hereof).
- 4. The IP filters and MAC address filters tabs are used to setup exclusions from centralized interception. In case SecureTower is used to control only part of a local network, you must use IP or MAC-based filtering to specify what computers will be controlled. Otherwise, the system will only intercept data from first 25 (in trial version) computers that connect to the network and exchanged any information (see detailed description of the filtering functions in the Administrator Guide).
- 5. In the **Network adapters** tab you need to select the network adapter that is used to receive mirrored traffic from the SPAN port.





Note: If you have installed the Interception Server, make sure that the Large Send Offload option is disabled in the advanced settings of the network adapter allocated for receiving the intercepted traffic.

Realtek RTL8168C(P)/8111C(P) Family PCI-E Gigabit Ethernet <mark>?</mark> 🗙				
General Advanced Driver Details Power Management The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.				
Property: Value: Jumbo Frame Image Send Offload (IPv4) Large Send Offload v2 (IPv4) Image Send Offload v2 (IPv4) Large Send Offload v2 (IPv4) Image Send Offload v2 (IPv6) Network Address Priority & VLAN Receive Buffers Receive Side Scaling Shutdown Wake-On-Lan Speed & Duplex TCP Checksum Offload (IPv4) Image Send Offload (IPv6) Transmit Buffers Image Send Offload (IPv4) UDP Checksum Offload (IPv4) Image Send Offload (IPv4)				
OK Cancel				

6. After you have specified all settings for centralized interception, click Apply changes in the lower right part of the main application window.



2b. Interception by agents

1. To intercept traffic at endpoints, agents have to be installed on all controlled computers in the network. If you want to test the system on 25 workstations of your network (not on the local computer only), go to the Services section (select in the left pane of the main program window). Select the Endpoint Agent Control server and click Service startup parameters.

EndPoint Agents Control server					
This server allows working with endpoint agents installed on remote computers across network Status: Status:					
	Start service	Stop service	Service startup parameters		

2. In the new window, check the Start under the specified account option and specify the account that has administrator rights to access local workstations in your domain (domain administrator) and its password. Click OK.

Service startup parameters					
Service startup parameters Configure service startup process					
Service startup settings					
Disabled					
Automatically star	rt on system startup				
Manually start by	user				
Service startup account s	Service startup account settings				
Start under local s	Start under local system account				
Start under the sp	ecified account				
Account name:	BusinessPro\Administrator Browse				
	Account name should in the "DomainName\UserName" form for an domain user and in ".\UserName" form for a local user				
Password:	•••••				
	OK Cancel				

3. Go to the EndPoint Agents section (select in the left pane of the main program window). In the Endpoint agents options tab select a strategy of agent installation.



SecureTower Quick Start Guide

💱 Services	See Endpoint agent control center	
Data Interception	On this page you can install and control endpoint agents on remote computers	
	Endpoint agents options Agents schema Endpoint agents installation strategy Secure Tower provides remote agents installation based on the selected installation strategy. To start distributing remote andpoint agents, please select the installation strategy below: Install agents only on specified computers Use this strategy if you need to install endpoint agents only on some computers. Based on this strategy, Secure Tower will install endpoint agents and monitor their status only on the computers that you specified. Any other available computers in the network will be ignored. Computers to install agents only	- M
EndPoint Agents Mail processing Licence information	Install agents on all available computers in network Use this strategy if you need to spread endpoint agents on all computers across network. Based on this strategy, SecureTower will install endpoint agents and monitor their status on any computers detected in the network. Any new computers that will appear in the network will be automatically detected, and endpoint agents will be automatically installed on them. Computers that should not have any endpoint agents installed must be included in the list of exceptions. Computers to exclude from agents installation	

If you select the option to install agents only on specified computers, you need to specify the computers the agents will be installed on. Click Computers to install agents on. In the new window, make a list of computers using the Add computers to list button and entering computer names (enter *localhost* to install an agent on the local computer).

Computers list		x
The list of computers to install e Endpoint agents will be installed on comp		
🖥 😽 Add computers to list 👌 Remove computer f	rom list	-
Computer name		
LOCALHOST		
Computers in list: 1		
	OK Car	ncel

The second strategy is installing agents on all computers available in the network. In case you use this strategy, if the number of computers in your network exceeds the number of purchased licenses (25 for the trial version), agents will only be installed on the first 25 computers (or other number according to purchased licenses), the endpoint control server connected to. To restrict agent installation in this strategy, click the Computers to exclude from agent installation button and make a list of computers that will not have agents installed.



Note:

The system relies on the Windows Active Directory accounts to deploy agents. If you do not have Active Directory domain in your network, you have to follow the instructions below for agent installation:

create a user with the same username and password on every workstation of the network and specify this account in the Endpoint Control service startup parameters.

Service startup parameters				
Service startup Configure service	• parameters startup parameters to tune up the service startup process			
Service startup settings				
Disabled				
Automatically sta	rt on system startup			
Manually start by	user			
Service startup account s	settings			
Start under local	system account			
Start under the sp	pecified account			
Account name:	BusinessPro\Administrator Browse			
	Account name should in the "DomainName\UserName" form for an domain user and in ".\UserName" form for a local user			
Password:	••••••			
	OK			

4. In the Endpoint Agent Control center, scroll down the main window and in the Data storage settings section click Select data storage. Connection to a database for agents is configured the same way as for the Interception server (see section 3. Database setup hereof).

Data st	orage settings				
	Current data storage settings:				
	Plugin name:				
	Server name:				
	Database name:				
	User name:				
		Configure data storage	Select data storage		

5. In the same window, scroll down to the Endpoint agent information area (right under Data storage settings) and click Agent Advanced Settings.



Going global with security

Endpoint agent information

Endpoint agents transfer the intercepted information through network to the Endpoint agent control server. Endpoint agents installed on remote computers can be automatically updated to latest version available on the server. Computer can be excluded from the automatically agent updating process.					
Agent version:	9.1.292.8930	Agent update settings			
Endpoint agents intercept information on the computers based on the specified settings. Settings can be specified separately for computers, users or other objects from Active Directory.					
	Agent settings manager				

- 6. In the new window, you can specify additional agent settings:
 - Skype interception tab is used to enable/disable text and voice interception in Skype and specify additional settings of Skype traffic interception;
 - Lync interception tab is used to enable/disable message interception in Lync;
 - Network traffic interception tab is used to configure the types of data that will be intercepted by agents. In case you use centralized interception via a mirroring port alongside with endpoint interception, you need to select a mode to intercept only encrypted traffic. This will help avoid duplicating data due to double interception;
 - Screen capture tab is used to enable/disable the screenshots feature, and to specify the period of taking screenshots on endpoints;
 - Desktop activity tab is used to enable/disable the feature of endpoint activity monitoring (periods of computer activity/idle time, applications run by users and the duration of their use);
 - Printers interception tab is used to enable/disable interception of documents sent to local and network printers;
 - USB interception tab is used to enable/disable and to configure interception of data sent to USB;
 - Network shares tab is used to enable/disable interception of data sent to network shares;
 - **SIP interception** tab is used to enable/disable text and voice interception in SIP and specify additional settings of SIP traffic interception;
 - **Exclusions** tab is used to configure exclusion of individual user account in Skype or ICQ, processes, IP addresses and users from data interception by agents;
 - Data blocking tab is used to block malware HTTP or SMTP traffic.
 - **Other** tab is used to enable/disable agent protection and local data storage on endpoints.



Warning: In some cases agent protection options may cause conflict with antivirus applications. Refer to the Administrator Guide for detailed information.



3. Database setup

All intercepted traffic is stored in a database. SecureTower system supports the following types of databases: Oracle, Microsoft SQL Server, PostgreSQL, My SQL and SQLite. Please note that in case you wish to use one of the first three types of databases, you first need to install a corresponding database management system on your server (please refer to the documentation of the corresponding DBMS). In case you use an SQLite database, you don't need to take any preliminary actions to setup a DBMS, you will be able to set everything up right in the SecureTower Administrator Console. This guide only provides instructions for SQLite database setup, since it is most appropriate for testing purposes. You can find instructions for setting up other types of databases in the SecureTower Administrator Guide.

To set up an SQLite database, navigate to the corresponding section of the Administrator console (Traffic Interception section for centralized interception, and EndPoint Agents section for interception via agents), subject to the interception mode you are using (if you use both modes, you have to set up the same database in both sections).

Find the Data storage settings area in the corresponding section and click Select data storage.

Data st	orage settings				
	Current data storage settings:				
	Plugin name:				
	Server name:				
	Database name:				
	User name:				
		Configure data storage	Select data storage		

Select the SQLite plugin option and click Select. A dialog window will open, where you have to enter a full path to the directory, where you wish to create a database, and a database file name with ".db" extension (e.g. C:\SecureTower\test.db).

S Configure connection to the SQLite database	×
SQLite database connection parameters Configure connection to the SQLite database	
Database file name:	
C:\SecureTower\test.db	
Test connection	OK Cancel

After you click OK, a database will be created in the specified folder. To save your settings, click Apply changes in the lower right part of the main application window.



4. Configuring data indexes

- 1. Go to the Data Indexing section (select in the left pane of the main program window) and click Create index.
- 2. Enter the name of the index to be created in the **Index name** text box of the **Create index** window. For example, "SecureTower index". In the Index Store Path text box, specify a path on a local disk where this index will be stored. The index store path can also be selected by clicking the network folder icon to the right from the store path entry field.

Create index					×		
Index proper Specify index op		index and to make i	t available for search		5		
Properties Schedule	er						
	To properly configure index you must specify index name, index location (on a remote server disk), and type of data you want to add to this index to make them searchable. You will be able to change these options at any time:						
Index name:	SecureTower index						
Index store path:	ex store path: C:\Test\Index\						
Sources of intercept	Sources of intercepted data to be included into the index:						
	Protocol data	Server name	Data storage				
	Add data source 🕶	Remove data source					
				Create	Cancel		

- At the bottom of the same window, click Add data source in the Sources of intercepted data 3. to be included into the index section. Select From Falcongaze SecureTower servers (network protocols).
- In the Add data sources window, select localhost in the Server name drop down menu. Click 4. Connect to server next to the selected server name.
- Upon successful connection, you will see the list of available protocols in the Available data 5. sources window. If you want to search all the protocols listed, just click Select.



ecify and connect	to the server and check the sources of data you want to in	clude into the index	
Server name:	localhost	 Connect to server 	
Available data	Protocol data	Interception mode	Data storage
sources:	🕼 🔇 Skype	From agent	SQLite plugin; C:\1.db
	📝 🙀 POP3 protocol	From agent	SQLite plugin; C:\1.db
	SMTP protocol	From agent	SQLite plugin; C:\1.db
	📝 🁙 OSCAR protocol (ICQ and etc)	From agent	SQLite plugin; C:\1.db
	🗷 🌖 HTTP protocol (visited urls, posts, post files)	From agent	SQLite plugin; C:\1.db
	☑ ✔ XMPP protocol (GTalk and etc)	From agent	SQLite plugin; C:\1.db

6. In the Scheduler tab of the index creation window you can set up a schedule for index updates and other operations (storage clearing, defragmentation). By default, for every new index a schedule is created to update every 5 minutes. The more often the index is updated, the sooner the data will be available for analysis. To modify a schedule, select it in the list and click Modify schedule. See detailed information on scheduler setup in the Administrator Guide.

😻 Create index				×	
	Index properties Specify index options to create new index and to make it available for search				
Prop	Properties Scheduler				
On	On scheduler page you can configure index update or data storage clearing schedules. You will be able to change these options at any time:				
	Schedule name	Job type	Schedule start		
2	Update index	Index updating	Start at 22.02.2012 0:00 and repeat every 1 day(s) and repeat every 5 Min		
2	Clear data storage	Storage cleaning and index	Start at 2:00 on Sun every 1 week(s)		
2	Index defragmentation	Index defragmentation	Start at 23.02.2012 5:00 and repeat every 1 day(s)		
Add	Add schedule Modify schedule Delete schedule				
			Create	ncel	

7. Click Create. After you have finished entering the necessary settings in the Administrator Console, click the Apply changes button located in the bottom right corner of the program's main window.



5. Adding users

To correctly identify senders/recipients of the intercepted data, local users should be added into SecureTower. To do this, go to the Users & Authentication section of the main window of Administrator console and select the Users tab.

💱 Services	🕵 Users & Authentication
To Data Interception	On this page you can assign users, user groups and specify the authentication mode
Protocols	Authentication Users Groups Active Directory & Domains integration Journal
Data Indexing	SecureTower provides authentication based on Windows accounts and SecureTower internal accounts. Based on the authentication mode selected, the user will need to use either an Active Directory account or a internal user account to get access to the system functions.
Digital Fingerprints	Authentication enabled
Sers & Authentication	Authentication mode:
Statistics	SecureTower internal accounts authentication
Levents & Notifications	Authentication options:
The second secon	Disable login with empty password
	Authentication module disables a user account for a several minutes if an incorrect password is entered 3 times
Mail processing	Allow to disable users
📦 ICAP server	Windows Active Directory authentication
Image recognition	
Licence information	

SecureTower allows importing users from the local Active Directory domain with following synchronization. To do this, click Import users from AD (the Functions button in the Users tab) and follow the Import Wizard instructions.

Alternatively, you can add users manually: clicking the Add user button and fill out the User card.

See additional information on user cards in the Administrator Guide.

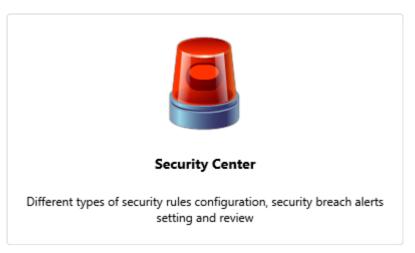


6. Configuring Security policies

1. Run the SecureTower Client Console, select the **Connect to the local computer** radio button. Click Connect to server.

🤤 Select a server	x			
Selecting the server Specify the computer name to connect to and setup the server	3			
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:				
Connect to this server on next startup	2			

2. On the program start page, select the Security Center section.



In the Security Center toolbar, click Settings and configure SMTP parameters for the delivery 3. of security notifications. In the Sender mail address text box, enter the e-mail address that will be used for sending security notifications. Click Test settings. In case of a successful test completion, a test message will be sent to the specified e-mail address.

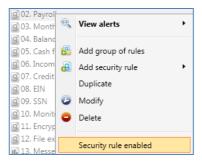


Configuring e-mail notifications	×			
Configuring e-mail notifications Specify settings for sending e-mail notifications				
Enable sending notifications with settings specified				
SMTP server address (or name):	smtp.gmail.com			
Sender e-mail address:	security.center@falcongaze.com			
SMTP server requires authenti	ication			
Login:	security.center@falcongaze.com			
Password:	•••••			
Use SSL				
Language:	English			
Test settings				
	OK Cancel			

- In the Security Center, you will see the list of default security rules in folders (En folder for 4. English-language rules). There are three types of security rules:
 - Q General. This type of rule is used for content analysis of data flows by keywords, regular expressions, etc., as well as for context analysis by attributes.
 - Control by thesaurus. This type of rule is used to automatically detect words and expressions included into special subject thesauri, in the traffic flow.
 - Statistical. This type of rule is used for statistic analysis of user traffic (e.g. the 16 intensity of IM or e-mail use, etc.)
 - **Digital fingerprints**. This type of rule is used for traffic analysis based on digital 5 fingerprints of files and databases.

You can use the default security rules, modify them or create your own. The default rules are disabled upon system installation. To turn them on, right-click on a security rule and select Security rule enabled in the context menu.





- 5. To create new rules, click Add security rule in the Security Center window. Besides, to quickly create a new rule based on one of the existing rules, you can duplicate a default rule and then change its parameters as needed. To do this, right-click an existing rule and select **Duplicate** in the context menu. A window will open where you can change the parameters of a new rule. Make sure the **Enable security rule** box is checked and click **OK**.
- 6. In order SecureTower could send automatic notifications in case of a security rule breach, you need to specify subscriber e-mails for separate rules or groups of rules (folders). If you wish to add a subscriber for a rule (folder), right-click on the corresponding rule (folder) and select the **Modify** option in the context menu. In the **Subscribers** tab (area) click **Add** subscriber, specify the subscriber e-mail and click **OK**.

🚱 Notification subscriber e-mail address	x
Notification subscriber e-mail address	\mathbf{N}
Enter e-mail address:	
cio@falcongaze.com	
OK Canc	·al
UK Can	.ei

Please see detailed information on security rule setup in the SecureTower User Guide.