



SECURITY CODE

Secret Net Studio

Administrator's manual

Setup and operation. Antivirus and intrusion detection tool



© **SECURITY CODE Ltd., 2017. All rights reserved.**

All rights to the operating instructions are reserved.

This document is part of the product package, and it is covered by all terms and conditions of the license agreement. This document or any part of it in printed or electronic form cannot be copied or made available to third parties for commercial purposes without express written consent of the SECURITY CODE Ltd.

The information contained in this document can be changed by its developer without advanced notice. This shall not be a violation of obligations with respect to users on behalf of the SECURITY CODE Ltd.

Mailing address: **P.O. Box 66, Moscow,
Russian Federation, 115127**
Telephone: **+7 495 982-30-20**
Email: **info@securitycode.ru**
Web: **<https://www.securitycode.ru/>**

Table of contents

List of abbreviations	4
Introduction	5
General information	6
Antivirus	6
Detecting and preventing intrusions	6
Antivirus	8
Configuring group policies	8
Configuring scan profiles	9
Schedule-based scanning	11
List of exclusions	13
Event registration	14
Managing antivirus on protected computers	14
Antivirus Management Utility	16
Intrusion detection and prevention tool	17
Configuring group policies	17
Network attack detector	18
Signature analyzer	21
Managing the intrusion detection tool	21
Update	23
Update the antivirus database	23
Update utility	24
Updating a decision rule base	24
Documentation	26

List of abbreviations

DB	Database
DRB	Decision Rule Base
SW	Software

Introduction

This manual is designed for Secret Net Studio administrators (hereinafter "Secret Net Studio, the System"). It contains information for administrators about the setup and management of antivirus and intrusion detection mechanisms. Before reading this manual, read the following documents: [1], [3].

Conventions

In order to highlight certain elements in the text, a series of conventions is used.

Internal links usually indicate the required page number.

Important and additional information in the document is presented as notes. Icons in the margins indicate the importance of the information they contain.



- This icon highlights additional information that may contain examples, links to other documents, or other parts of the manual.



- This icon highlights important information that must be taken into account.



- This icon highlights a warning.

Exceptions. Some notes may not have any icons. Apart from note icons, the margins may also contain other graphical elements, for example, buttons that are explained in adjacent paragraphs.

Other information sources

If you have Internet access, you can visit SECURITY CODE Ltd. website (<https://www.securitycode.ru/>) or contact a company's representatives via email (info@securitycode.ru).

Chapter 1

General information

The System includes the following anti-malware tools:

- Antivirus.
- Intrusion detection and prevention.

Antivirus

Secret Net Studio makes it possible to perform heuristic data analysis and automatically check for malware registered in the signature database. During a computer scan, hard drives, network folders, external data storage media and other objects are scanned. It ensures detection and blocking of external and internal network attacks at the protected computers.

Antivirus parameters are configured by the security administrator using group and local policies in the Control Center.

All subsystem activity data is registered in the Secret Net Studio log.

The following virus protection functions are available.

Function	Description
Real-time protection	Real-time file checking. Detection of computer viruses using signature and heuristic methods when attempting to access executable files, documents, images, archives, scripts, and other types of potentially dangerous files
Context scanning	A scan initiated by the user from the context menu of Windows Explorer
Schedule-based scanning	The parameters of the scans are set up by the administrator in the Control Center. A skipped scheduled scanning (for example, if the computer was turned off) starts automatically when the computer resumes operations
Removable media scanning	The System supports automatic scans of removable media when they are connected to the computer
Exclusions	Creating a list of files that are not scanned during real-time file scanning and scheduled scanning. The list of exclusions is applied globally for all types of scanning and cannot be set up independently for different modes
Operations with detected viruses	The following operations can be performed regarding infected objects: removal, isolation (moving to quarantine), blocking of access (only in continuous protection mode), repairing. Responses to detected malware are chosen in the antivirus parameter settings
Update	Automatic database update from the server in a background mode or manual database update from a chosen folder
Signature integrity control	Verifying signature database integrity when loading a service or updating. A log record is created in case of an unauthorized database modification

Detecting and preventing intrusions

Secret Net Studio ensures the detection and blocking of external and internal intrusions into a protected computer.

Subsystem parameters are configured by the security administrator using group and local policies in the Control Center.

All information about the activity of the mechanism for detecting and preventing intrusions is registered in the Secret Net Studio log.

Function	Description
Network attack detectors	Filtration of incoming traffic used to block external attacks. Attack detectors operate on the application level of the OSI model. Incoming data is analyzed by examining behavior
Signature analysis	Monitoring of incoming and outgoing network traffic for elements registered in the decision rules database. Attacking computers can be blocked for a predefined time period

Chapter 2

Antivirus

You can configure the antivirus in the centralized mode using the Control Center, which can be performed at different levels of the control object structure:

- at the Domain, Security Server and Organizational unit object levels you can configure the antivirus parameters based on group policies. The parameter values set for the Security Server level have a higher priority over those set for the Computer object level;
- at the Computer object level you can configure the antivirus parameters for a single computer and to perform certain antivirus operations (e.g. scan, manage quarantined objects, etc.) on this computer.

Note.

the System also includes the Local Control Center. This component allows managing the antivirus on a protected computer.

Configuring group policies

Antivirus functional parameters are divided into the following groups:

- scan profiles. A scan profile is a set of predefined scanning parameters to be applied for a system check in the respective mode;
- the scan schedule determines time and period of the check respectively with a selected scanning profile;
- exceptions determine the list of files and folders to ignore during the check.

To configure these parameters:

1. Open the Control Center.

Tip.

To configure antivirus settings directly on a protected computer, in the Local Control Center, on the Settings tab, in the Policies section, click Antivirus. Further configuration is similar in centralized mode.

The main program window appears.

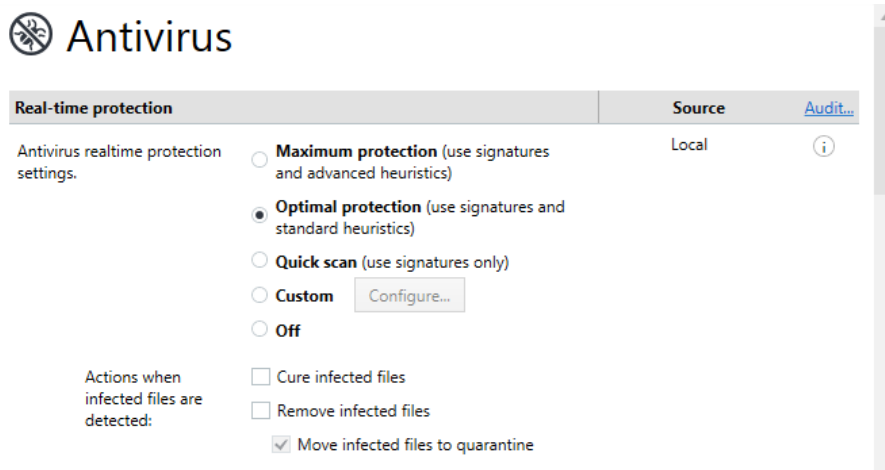
2. Click Computers on the Computers panel, right-click the needed object and click Properties.

An information message showing the computer status appears as in the figure below.



3. On the Settings tab, in the Policies section, click Antivirus.

A dialog box appears as in the figure below.



4. Configure the required parameters and click Apply.

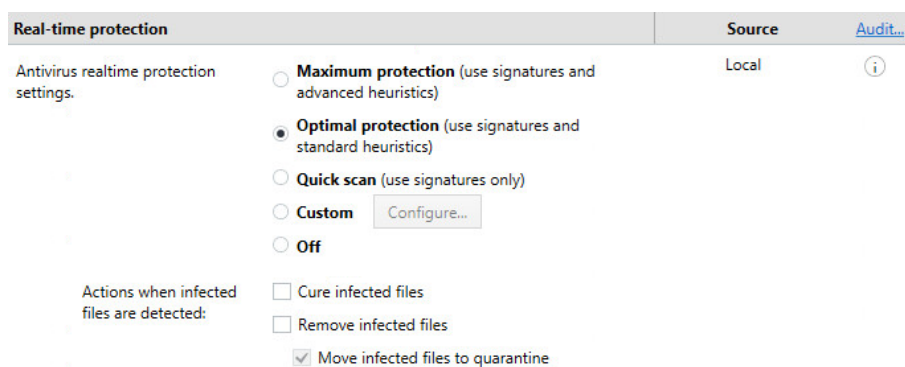
Configuring scan profiles

The System contains the following scan mode profiles.

Name	Purpose
Real-time protection	This profile defines the scanning parameters for system objects in real-time
Scanning removable media	Defines automatic scanning parameters for all removable media
Context scanning	This profile defines the parameters for a scanning initiated by the user via the Windows Explorer context menu
Full scan	This profile defines the parameters for a scanning initiated by the administrator through the Control Center or schedule. In this mode, all active processes, automatic startup parameters and boot sectors are checked
Quick scanning	This profile defines the parameters for a quick scanning initiated by the administrator through the Control Center or schedule. In this mode, the system is quickly scanned to detect any vulnerabilities. System vulnerabilities include active memory processes, vulnerable files and folders, as well as removable media

Select a category to configure in the parameter settings menu.

Real-time protection



To configure real-time protection parameters:

1. Define the antivirus protection level during a real-time scan.

Parameter	Description
Maximum protection	The System searches for files infected by commonly known malware. The System checks all internal and external drives. The scanning involves advanced heuristic analysis of new threats (see p. 12). Files and archives larger than 100 MB are skipped
Optimal protection	The System checks files during any access attempt, and checks all fixed and removable drives. The scanning involves heuristic analysis in normal mode (see. p. 12). Files larger than 100 MB and archives larger than 50 MB are skipped
Quick scan	The System searches for files infected by commonly known malware and only checks fixed drives. Files larger than 50 MB are skipped
Custom	User-defined real-time protection parameter-based scan
Off	Real-time object scanning will not be performed

2. For a user-defined scan profile, click Configure (see p. 11).
3. Choose an action to perform.

Parameter	Description
Cure infected files	Choosing this option will initiate an attempt to cure infected files
Remove infected files	Infected files will be deleted
Move infected files to quarantine	Deleted files will be moved to quarantine. Quarantined files can be restored in the future, if necessary

Note.

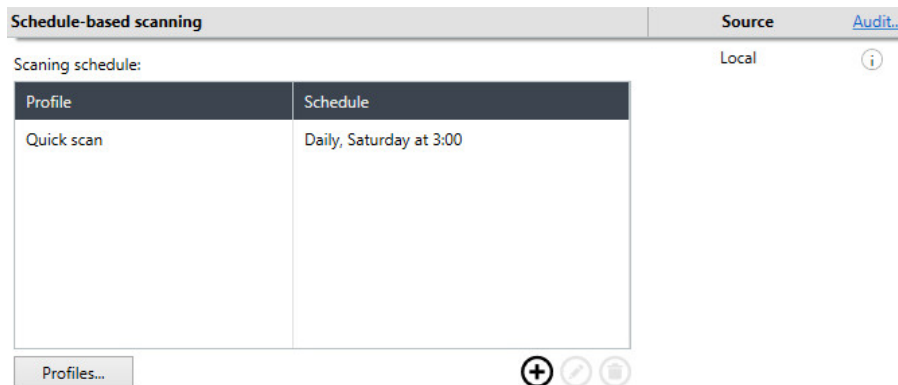
If the "Cure infected files" and "Remove infected files" actions are selected simultaneously, an attempt will be made to clean the infected files upon detection, and if this fails, the files will be deleted.

4. Click the Audit link to configure antivirus event logging parameters.
The other profiles can be configured in the same way as for Real-time protection.

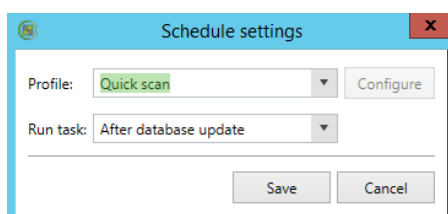
Schedule-based scanning

To configure schedule-based scanning:

1. In the antivirus settings area, go to the Schedule-based scanning section.



2. To add a new scanning routine to the schedule, click Add. A dialog box appears as in the figure below.



3. Select the scan profile and scanning frequency from the drop-down list and click Save.

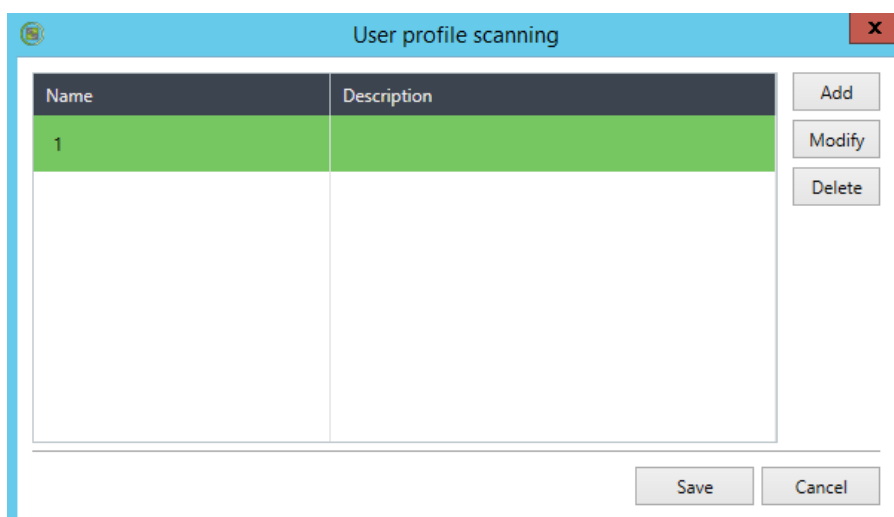
Note.

Click the Configure button to configure a custom profile.

To create a new scan profile:

1. Click Profiles.

A dialog box appears as in the figure below.

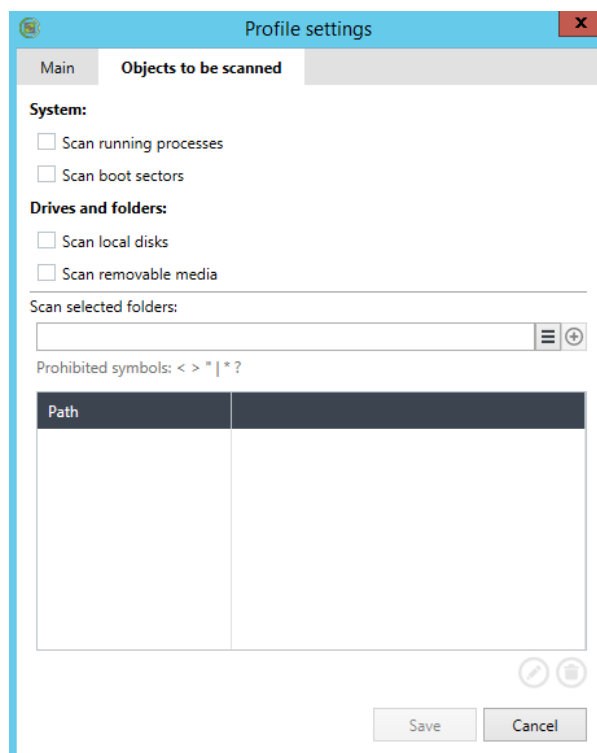


2. Click Add. The Profile settings dialog box appears as in the figure below.

3. On the Main tab, specify the following parameters.

Parameter	Description
Name	Scanning profile name
Description	Profile description
Heuristics	<ul style="list-style-type: none"> Advanced — a high probability of detecting unknown viruses, high false-detection rate. The scan in this mode is slower than in normal mode; Standard mode — limited heuristics: lower probability of detecting unknown viruses, lower false-detection rate; Off — heuristic scan is disabled
File exclusions	Configure files/file types to be ignored during scanning. <ul style="list-style-type: none"> Skip compressed files — archives will be ignored during the antivirus scan; Skip files larger than — specify the size of files to be ignored during the scan; Scan files with the following extension only — only files with particular extensions will be scanned; Specify file extensions (use a comma to separate)
Action when infected files are detected	Actions to be performed upon detection of infected files (see p. 9)

4. Select the "Objects to be scanned" tab.
A dialog box appears as in the figure below.

**Note.**

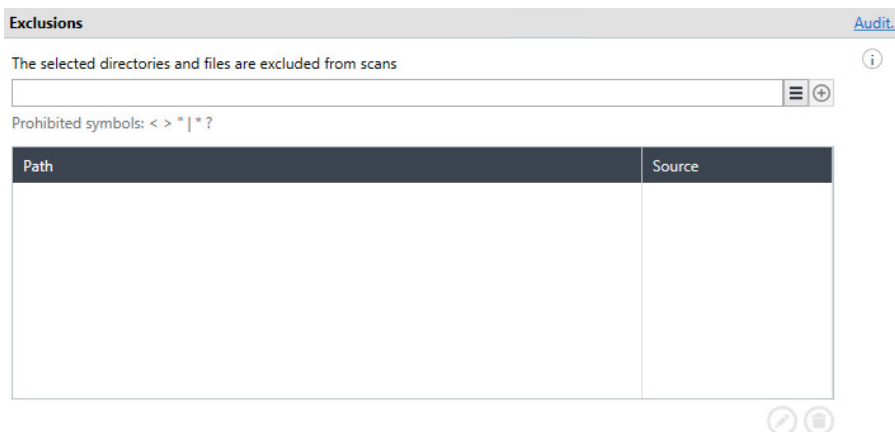
When configuring real-time scan parameters (Real-time protection profile), the "Objects to be scanned" tab is not available.

5. Configure the parameters.

Parameter	Description
System	Select objects to be scanned
Drives and folders	<ul style="list-style-type: none"> Select drives and folders to be scanned when using this profile. Specify the path to the folder to be checked and click Add. If necessary, use environment variables from the drop-down list. Click Modify to edit the path. Click Delete to remove the folder from the list

List of exclusions**To configure the list of exclusions:**

- Go to the Exclusions section in the antivirus parameters settings.



- To add a folder or a file, specify its path to it and click Add. If necessary, use environment variables from the drop-down list. Objects from the list of exceptions are ignored by any scan profile.

Note.


To change the path to an object, select it from the list and click Edit. To remove an object from the list of exceptions during the checks, select it and click Delete.

Event registration

To configure event registration parameters:

- In the list of parameters and policies, go to the Event registration section and select the Antivirus option.

A dialog box appears as in the figure below.

Antivirus	Source
Registration level: <input type="radio"/> Extended <input checked="" type="radio"/> Optimal <input type="radio"/> Low <i>Settings will be applied after agent restart</i>	Local 

- Select the event registration level.

- Advanced.
The System registers all events.

**Attention!**

The number of registered events can be very large.

- Optimal.
The System registers all important and some informational events.
- Low.
The System registers only important events.

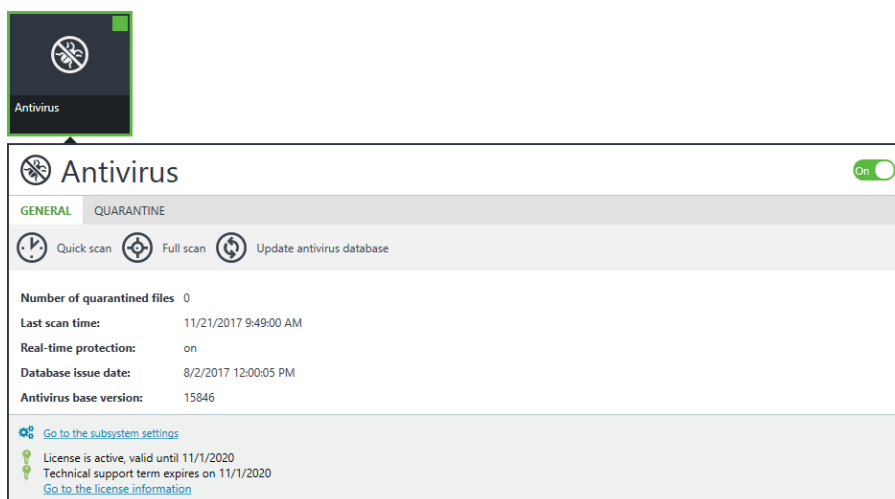
Managing antivirus on protected computers

Using the Control Center you can perform the following actions on an individual computer:

- run the scanning procedure;
- view and manage quarantined objects;
- run the antivirus database updates procedure;

To manage antivirus:

- Right-click the needed object and click Properties.
An information window appears, showing the status for this computer.
- Select the Antivirus object on the Status tab.
A dialog box appears as in the figure below.



3. Perform the required actions using the "Quick scan", "Full scan" and "Update antivirus database" option buttons (see p. 23). Scanning parameters are configured by using the policies (see p. 8).

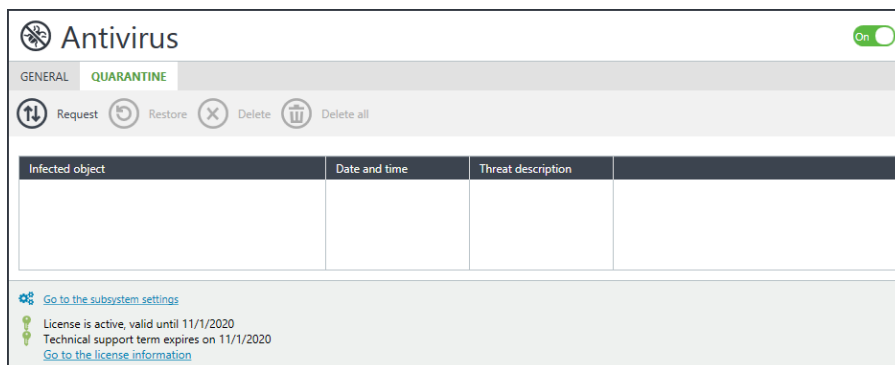
Note.

Click the "Go to the subsystem settings" link to to configure local antivirus policies.
Click the "Go to the license information" link to see current license information.

To manage quarantine:

1. Open the antivirus control panel and select the Quarantine tab.

The Quarantine tab allows you to browse files and folders moved to quarantine on a particular computer. It also has list element control buttons.



2. Perform the required actions:

Parameter	Description
Request	The list of quarantined files on the given computer will be loaded
Restore	The selected file will be restored from the quarantine
Delete	The selected file will be deleted from the quarantine
Delete all	Quarantine will be cleared



Attention!

Objects restored from the quarantine are added to the exceptions list for all scanning profiles. This is done to prevent an object from being moved to quarantine again during subsequent scanning.
Files stored in quarantine for over 30 days will be deleted automatically. Use the antivirus management utility (av_cli.exe) included in the product to configure this parameter.

Antivirus Management Utility



Attention!

The antivirus management utility is designed for technical support specialists. WE DO NOT RECOMMEND using this utility for standard antivirus program configuration.

Secret Net Studio includes `av_cli.exe`, an antivirus program management utility.

To call up detailed information about the program, open the command prompt and type the following command:

```
av_cli.exe
```

Note.

The utilities `av_cli.exe` utility and `avus.exe`, an update server management utility, (see "Configuring the Update Server" section in the Setup and Operation. Antivirus and Intrusion Detection Tool document) use the same settings for managing updates.

Chapter 3

Intrusion detection and prevention tool

The intrusion detection and prevention tool is managed in the centralized mode using the Control Center and can be managed at different levels of the control object structure:

- at the Domain, Security server and Organizational unit object levels it is possible to configure the parameters of this mechanism based on group policies. The parameter values set for the Security Server level have a higher priority over those set for the Computer object level;
- the Computer object level enables you to configure the parameters of this tool for a single computer and to manage the tool on this computer.

Note.

the System also contains the Local Control Center. This component allows you to directly the manage intrusion detection and prevention tool on a protected computer.

Configuring group policies

The intrusion detection and prevention tool enables the following:

- use of an attack detector to block attacks and detect port scanning attempts;
- use of a signature analyzer to scan incoming and outgoing traffic for registered signatures.

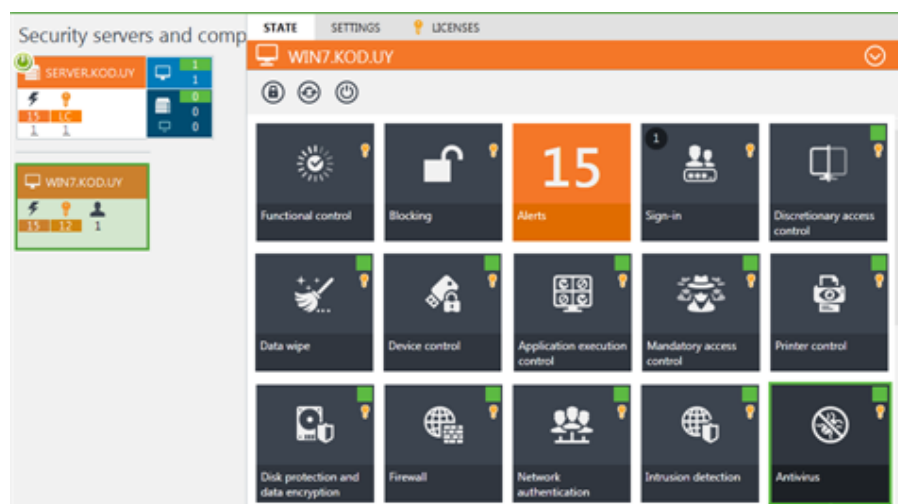
To configure and manage the tool:

1. Open the Control Center.

Tip.

To configure the intrusion detection and prevention parameters directly on a protected computer, open the Local Control Center, on the Settings tab, in the Policies section, click "Intrusion detection". Further configuration is similar in the centralized mode.

A dialog box appears as in the figure below.



2. Click Computers on the Computers panel, right-click the needed object and click Properties.
A message box showing computer status appears.
3. On the Settings tab, in the Policies section, click "Intrusion detection".
A dialog box asking you to configure the selected parameters appears as in the figure below.

Intrusion Detection


Network attack detectors	Source	Audit...
<input type="checkbox"/> Enable attack detectors <input checked="" type="checkbox"/> Block attacking host if an attack is detected Blocking time: <input type="text" value="15"/> minutes	Local	

- Configure the required parameters and click Apply.

Network attack detector

To enable the network attack detector:

- In the Intrusion detection settings menu, select "Network attack detectors".

Network attack detectors	Source	Audit...																								
<input type="checkbox"/> Enable attack detectors <input checked="" type="checkbox"/> Block attacking host if an attack is detected Blocking time: <input type="text" value="15"/> minutes Activated network services :	Local																									
<table border="1"> <thead> <tr> <th>Addressing area</th> <th>Protocol</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td colspan="3">Service : ICMP receiver</td> </tr> <tr> <td>AF_INET</td> <td>1</td> <td></td> </tr> <tr> <td>AF_INET6</td> <td>58</td> <td></td> </tr> <tr> <td colspan="3">Service : SMB server</td> </tr> <tr> <td>Any</td> <td>IPPROTO_TCP</td> <td></td> </tr> <tr> <td colspan="3">Service : RDP server</td> </tr> <tr> <td>Any</td> <td>IPPROTO_TCP</td> <td></td> </tr> </tbody> </table>			Addressing area	Protocol	Ports	Service : ICMP receiver			AF_INET	1		AF_INET6	58		Service : SMB server			Any	IPPROTO_TCP		Service : RDP server			Any	IPPROTO_TCP	
Addressing area	Protocol	Ports																								
Service : ICMP receiver																										
AF_INET	1																									
AF_INET6	58																									
Service : SMB server																										
Any	IPPROTO_TCP																									
Service : RDP server																										
Any	IPPROTO_TCP																									

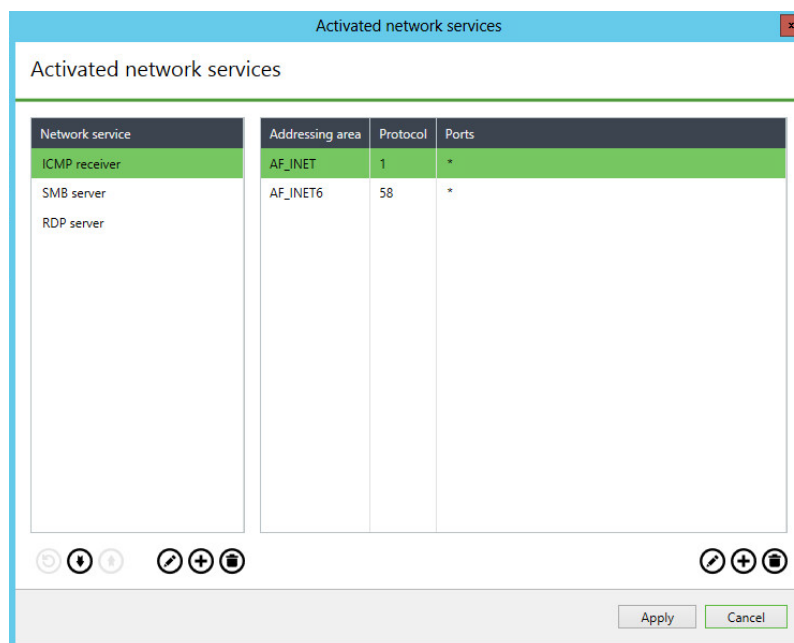
- Configure detector parameters.

Parameter	Description
Enable attack detectors	Select this option to activate the network attack detectors
Block attacking host if an attack is detected	If this option is selected, the IP address of the attacking host will be blocked
Blocking time (minutes)	Host block duration

Note.

For network service template settings, click the "network services" link.

- Click Edit to define individual DOS detector triggering parameters for different ports and protocols.
A dialog box appears as in the figure below.

**Note.**

To edit the list of network services, use the following buttons:

- Use the Up and Down buttons to manage the priority of used network services;
- To replace a network template, click Edit;
- To delete a network service, click Delete;
- To refresh the list of network services, click Refresh.

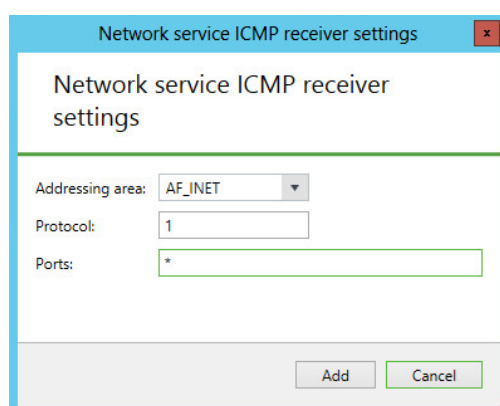
Note.

To edit the network service settings, use the buttons on the right of the window:

- To add a new network service setting, click Add;
- To delete a network service, click Delete.

4. To add a new network service, click Add on the left of the window and select a template. To configure network parameters, select the name in the left of the window, then select the required set of parameters in the right of the window, and click Edit.

A dialog box appears as in the figure below.



5. Configure the network service parameters and click Apply.

Parameter	Description
Addressing area	Select an addressing area for the network service
Protocol	Select a protocol governed by the network service
Ports	Specify the number of the port governed by the network service

6. Enable the required detectors and configure their parameters.

Detector	Description
Port scanning	Select this option to enable port scanning detection
Detection period	The period during which the System calculates how many times the ports of protected computers have been addressed
Maximum number of calls to ports within the specified period	Once this number is reached, the server is considered as an attacking server
ARP-spoofing	Select this option to enable detection of Man in the middle type attacks used in ARP protocol-based networks
Period after ARP request during which ARP response is expected	Specify the time for the detector to wait for an ARP response. The attack detector will be triggered if more than one response is received
Action with ARP responses, without ARP requests	Specify the action for the detector to take regarding ARP responses without ARP requests: <ul style="list-style-type: none"> • Ignore; • Log — record an audit event; • Log and send ARP responses; • Active ARP-spoofing detector — an ARP request will be issued for each ARP response received without an ARP request; • Active countermeasures to ARP-spoofing — an ARP request will be issued for each ARP response received without an ARP request. Initial response will be blocked
SYN-FLOOD	Detection of Denial-of-service type attacks that send a large number of SYN requests in a short period of time
Period during which half-open connections will be taken into consideration	Define the time to consider new connections over TCP
Number of half-open connections required to consider host in attacker	Define the number of half-open connections to exceed in order to trigger the attack detector
Block packets if the detector is triggered	Select this option for packets to be blocked when the detector is triggered. In this case, if the number of half-open connections created within a specified period of time exceeds the specified value, no new connections will be created
Abnormal traffic	Select this option to detect abnormal traffic
Block packets if the detector is triggered	Select this option for abnormal traffic packets to be blocked when the detector is triggered
DDoS	Detection of attacks from multiple computers
Number of active remote hosts required to trigger the detector	The attack detector will be triggered once the specified number of remote addresses sending traffic to a protected computer has been reached
DoS	Detection of denial-of-service attacks
Time interval during which port calling is taken into account	Specify a time interval during which port calling will be taken into account
Number of packets required to detect an attack	The number of packets sent from a server, within the specified time interval, for a server to be considered an attacker if reached

Detector	Description
Amount of data required to detect an attack	The data size sent from a server within a specified time interval for a server to be considered an attacker if reached
Slow down traffic from the attacking host	Select this option to automatically reduce the transmission speed of data from the attacking server, losing a portion of packets

Signature analyzer

To configure the analyzer:

1. In the Intrusion detection settings menu, click "Signature analyzers".

2. Configure the parameters.

Parameter	Description
Enable signature analyzers	Select this option to launch the Signature analyzer
HTTP analyzer	Select this option to launch HTTP traffic analyzer
Incoming traffic control	Incoming traffic will be monitored for the presence of signatures registered in the decision rules base
Outgoing traffic control	Outgoing traffic will be monitored for the presence of signatures registered in the decision rules base
List of ports	Type the ports to be checked by the intrusion detection tool. Use a ";" (semicolon) character to separate values. By default, the list contains ports 80, 8080 and 3128

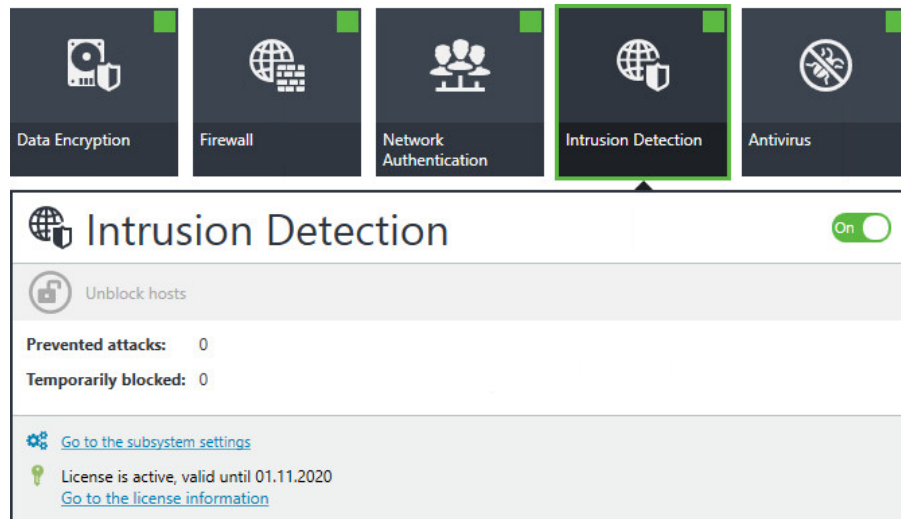
Note.

The list of ports monitored by the HTTP analyzer cannot be empty.

Managing the intrusion detection tool

To manage this mechanism:

1. Click Computers on the Computers panel, right-click the needed object and click Properties.
A dialog box showing the computer status appears.
2. In the computer properties area, find and select the "Intrusion detection" object.
A dialog box appears as in the figure below.



3. To remove block from all hosts blocked by the intrusion detection tool on the computer, Click "Unlock hosts".

Note.

To go to the intrusion detection mechanism group policy configuration, click the "Go to the subsystem settings" link. (see p. 17).

To see current license information, click "Go to the license information" link.

Chapter 4

Update

To ensure full protection against malware, the following updates are available:

- signature base updates (see p. 23);
- decision rules base update (see p. 24).

Update the antivirus database

To configure the update parameters:

1. In the Policies section, click Update.

2. In the "Schedule of update checks" group, define how often the software will check for updates. In weekly mode, you can set the day and time of day for the software to update. For daily mode, you can set the exact time. If the "Scheduler is disabled" option is selected, the System will no longer check for updates automatically.
3. If the local network has a server containing updates for Secret Net Studio antivirus database, click "Update from local server" and type the path to the server. Otherwise, click "Update from the Secret Net Studio server" and, if necessary, type the path to the proxy server.

Parameter	Description
Direct access	Select this option if there is a direct connection with the update server (direct access)
Use system proxy settings	Automatic proxy-server detection is used
Manual proxy server setup	Select this option to configure the proxy server manually. Specify the proxy server address and port. If a proxy server requires authorization, type the username and password

Note.

Updates can be installed from the network folder. In this case, the computer account must be able to access the resource.

If the protected computer is not connected to the Internet, the antivirus databases can be updated by using the update utility (see p. 24).

Update utility

Secret Net Studio includes a standalone antivirus database update utility. When you run the utility, it checks the current version of the antivirus databases in the installed antivirus program. If necessary, it installs current updates contained in the utility.



Attention!

The utility only contains an update for one antivirus program.

When you install the update, the System checks the compatibility of the downloaded archive contents with the version of the product installed on the protected computer. It also verifies and checks the integrity of the archive.

You can download the utility from the KOD website or the local update server.

To download and run the utility:

1. Follow one of these links:
 - <https://updates.securitycode.ru:43442> for the antivirus program;
 - <https://updates.securitycode.ru:43443> for the antivirus program (ESET technology).
2. To download the utility, click the link:
 - Current update utility for the antivirus program;
 - Current update utility for the antivirus program (ESET technology);

Note.

The file name indicates the antivirus database version included in the utility.

3. Run to execute the downloaded utility file. A message appears describing the antivirus database update results.

Note.

If there is not enough free space on the drive, the updates will not be installed.

If there is an error when applying the update, the database will automatically roll back to the previous version. In all other cases, you only can roll back to previous versions of the antivirus databases by using the `av_cli.exe` utility (see [16](#)) or the `avus.exe` utility (see 'Configuring the update server' section in the Update Server. Installation and Set-up Guide document)

Updating a decision rule base

A decision rule base contains network attack signatures. A decision rule base update is created when new network attacks are discovered.

To update a DRB:

1. Download the available DRB update through your account on the KOD website (<http://www.securitycode.ru/>).
2. Check the downloaded data files for integrity. To do this, compare the checksum of the downloaded DRB files with the checksums provided on the KOD website.
3. Log in with administrator account credentials on a computer with the Client. Go to the command prompt and run the following commands:

```
cd "<path_1>"
```

```
ScLocalCfg.exe NIPS Set signatures /file <path_2>
```

where:

- **<path_1>** is the path to the setup folder of Secret Net Studio. By default, `C:\Program Files\Secret Net Studio\`. If the path to setup folder is changed, please specify the new path;
- **<path_2>** is the path to the downloaded DRB update file.

To perform a centralized DRB update, place the update file in a shared folder, then configure the Clients to perform scheduled updates from the specified folder.

To acquire a list of used signatures:

- Log in with administrator account credentials on a computer with the Client. Go to the command prompt and run the following commands:
cd "<path_1>"
ScLocalCfg.exe NIPS Get signatures /file <path_3>
where <path_3> is a path to DRB file.

To see the number of used signatures:

- Log in with administrator account credentials on a computer with the Client. Go to the command prompt and run the following commands:
cd "<path_1>"
ScAuthModCfg.exe /s

Documentation

1.	Secret Net Studio. Administrator's manual. Development principles
2.	Secret Net Studio. Administrator's manual. Installation and update
3.	Secret Net Studio. Administrator's manual. Setup and operation
4.	Secret Net Studio. Administrator's manual. Centralized management, monitoring and audit
5.	Secret Net Studio. Administrator's manual. Setup and operation. Local protection
6.	Secret Net Studio. Administrator's manual. Setup and operation. Network protection
7.	Secret Net Studio. Administrator's manual. Setup and operation. Antivirus and intrusion detection tool
8.	Secret Net Studio. User manual