SECURITY CODE

Secret Net Studio

Administrator's manual

Update server. Installing and configuring

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

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 on the deployment and configuration of the automatic update tool for antivirus databases on workstations in a local network.

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
Update server architecture

Secret Net Studio includes update servers for Antivirus. The update servers are designed to centrally update antivirus databases on protected computers. The updates are downloaded from the KOD server.

System requirements

The update server may be installed on computers running the following operating systems:

- Windows Server 2008 x64 R2 SP1;
- Windows Server 2012/Server 2012 R2.

The update server may only be used with IIS server version 7 and later.

Note. SSL certificate installed for IIS server is a self-signed certificate.

Note. In Secret Net Studio 8.2, the incoming network traffic on local update servers consists of update packages and update utilities (see p. 14).

Deployment options

Depending on network configuration and size, you can use various deployment schemes for the update server.

A secure network with five or less workstations

To use this option, configure the update parameters to update antivirus databases from the KOD server via the Control Center (see the document Setup and Operation. Antivirus and Intrusion Detection Tool).

A secure network with more than five workstations

In this case, install the update server software on a dedicated server in a secure network. The installed update server will download updates from the KOD server and provide updates to the Clients in the network and other update servers used in cascading mode (without using any external traffic). Configure the update parameters to update antivirus databases from the local server via the Control Center (see the document Setup and Operation. Antivirus and Intrusion Detection Tool).

A secure network is not connected to the Internet

Install a separate server with Internet access. On this server, install the update server. Also, install the update server on the server in the restricted access network.

The update server with Internet access will download the updates from the KOD server and store them. Transfer the updates manually from that server to the server in the restricted access network.

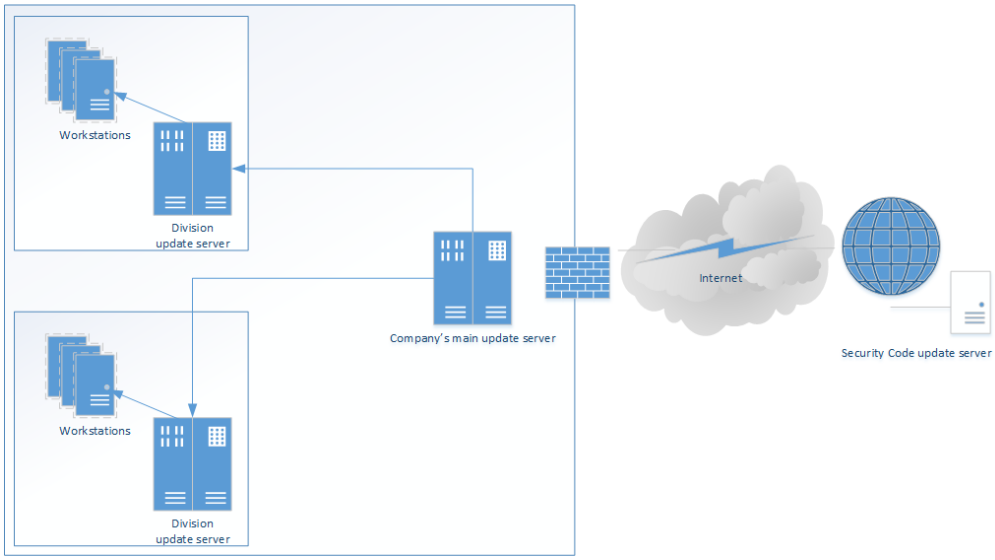
In the Control Center configure update parameters to update antivirus databases from the local server in the restricted access network (see the document Setup and Operation. Antivirus and Intrusion Detection Tool).

Server cascading

Create the following cascade of servers - one root server to download the updates from the KOD server, and child servers to download updates from the root server and other child servers.

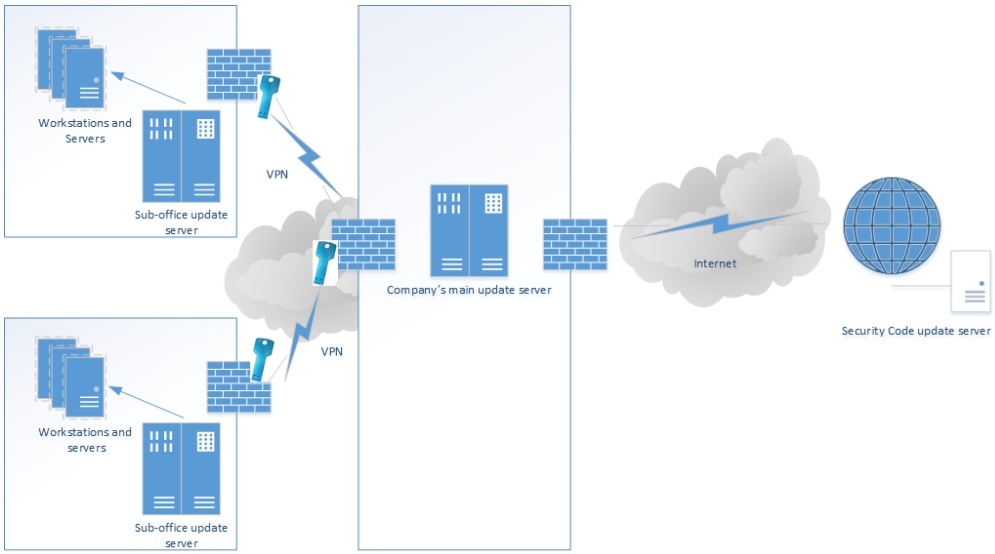
Example 1. The company uses several subnets.

Install the primary update server that downloads updates from the KOD website. Install an update server, configured to download updates from the primary server, in each subnet. Subnet workstations will download updates from these servers.



Example 2. The company has several sub-offices.

Install an update server in each sub-office. Each server will download available updates within the parent organization via the corporate network.



Chapter 2
Installing and configuring the update server

To deploy the update server:

1. Install the Secret Net Studio update server (see p. **8**).
2. Configure update downloading from the KOD server (see p. **13**) or from a local update server (see p. **13**).
3. Configure an update schedule (see p. **14**).

Installing the update server

Installing the update server for Antivirus (ESET technology)

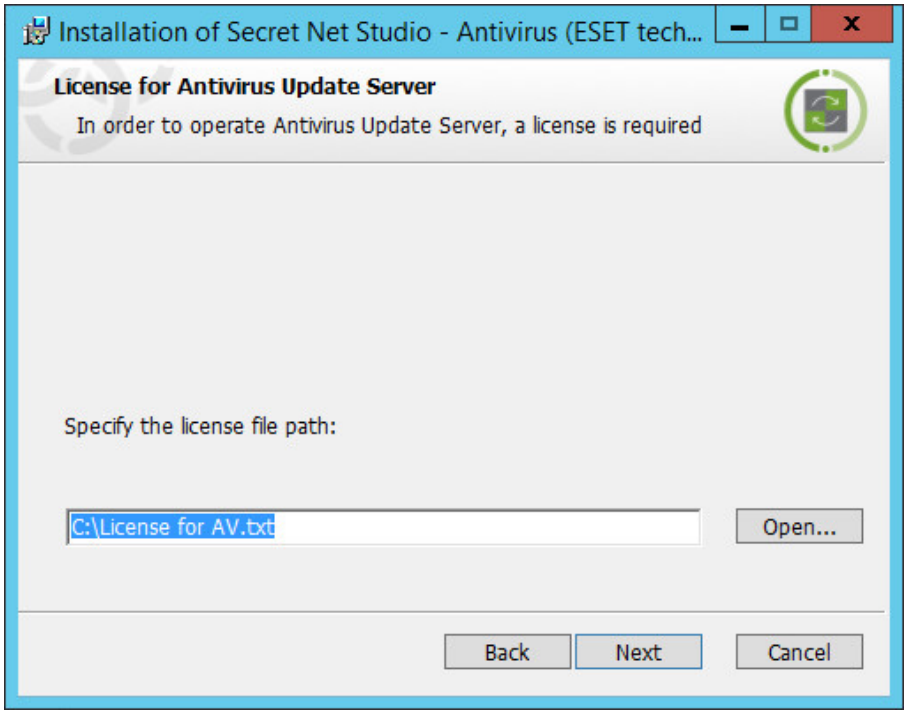
To install the update server:

1. Log in as a computer administrator.
2. Run AvUpdateServer.msi as administrator.

   The program begins preparations. After all preparations are complete, the installation program will display its welcome dialog box.
3. Click Next.

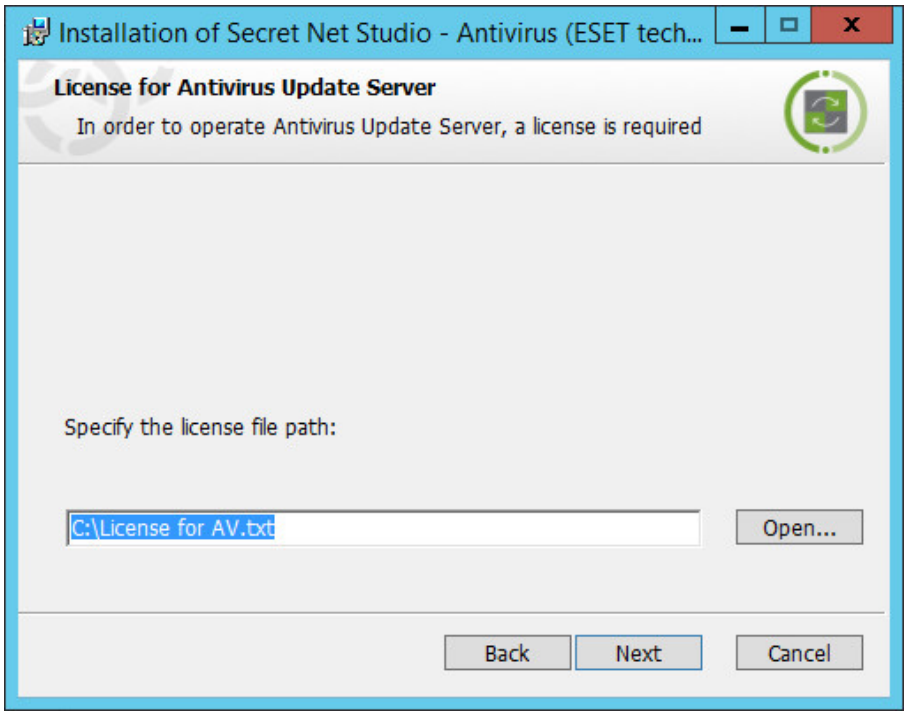
   The license agreement dialog box appears.
4. Read the license agreement, select "I accept the terms of the license agreement" and click Next.

   Tip. To get a paper copy of the license agreement, click Print.
5. A dialog box appears as in the figure below.



Select or type the path to the file with the update server license and click Next.

6. A dialog box for configuring HTTPS connections appears as in the figure below.



The default port is 43443.

Click Next. A dialog box appears saying that everything is ready for installation.

7. Click Install.

   The System begins copying files to the hard drive and configuring installed components. This process is displayed in the progress bar in the installation program dialog box.

   After successful installation and configuration of the component, the System will display a dialog box.

8. Click Finish.

Installing the update server for Antivirus

To install the update server:

1. Log in as a computer administrator.
2. Run AmUpdateServer.msi as administrator.

   The program begins preparations. After all preparations are complete, the installation program will display its welcome dialog box.

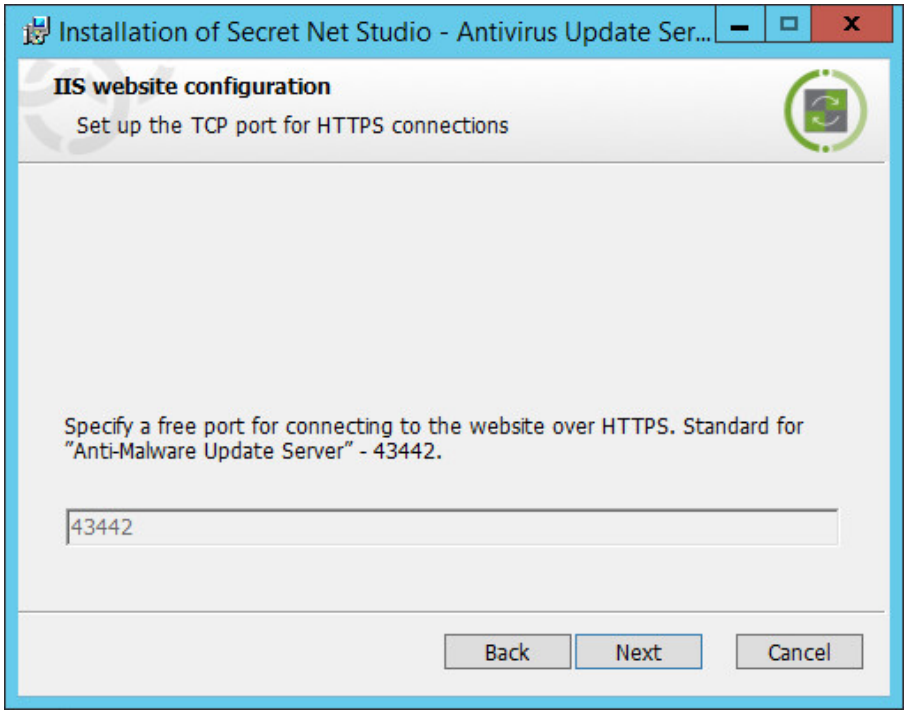
3. Click Next.

   The license agreement dialog box appears.

4. Read the license agreement, select "I accept the terms of the license agreement" and click Next.

   Tip. To obtain a paper copy of the license agreement, click Print.

5. A dialog box for configuring HTTPS connections appears as in the figure below.



The default port is 43442.

Click Next. A dialog box appears saying that everything is ready for installation.

6. Click Install.

   The System begins copying files to the hard drive and configuring installed components. This process is displayed in the progress bar in the installation program dialog box.

   After successful installation and configuration of the component, the System will display a dialog box.

7. Click Finish.

Configuring the update server

The installed update server for Antivirus (ESET) is located in C:\Program Files (x86)\Secret Net Studio\Server\Antivirus Update Server; for Antivirus, in C:\Program Files (x86)\Secret Net Studio\Server\Antimalware Update Server.

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

```
avus.exe
```

Note. You need administrator rights to change any parameters via avus.exe. Commands that do not modify update server settings can be executed by any user.

Use the following parameters to configure the update server.

Note. avus.exe, a utility for managing the update server, and av_cli.exe, a utility for managing the antivirus programs on protected computers, use the same parameters to manage updates.

Command	Available arguments	Action
-c:list_update	**-package_id:** — package number	Get information on the update package
-c:list_update_job	**-update_job_id:** — job number	Get information on the job
-c:list_update_jobs		Get the list of existing update jobs
-c:list_updates		Get the list of update packages in the system
-c:new_update_job		Start update
-c:new_update_rollback_job	**-package_id:** — update number	Roll back the system update
-c:cancel_update_job	**-update_job_id:** — update job number	Cancel update job
-c:current_update_id		Get the number of current update
-c:get_update_parameters		Get global server settings
-c:get_update_schedule		Get the update schedule
-c:get_update_source_parameters		Get update source parameters
-c:set_update_schedule	**-by_time:** — startup time for update download; **-enabled:** — available values: • yes — update job will be enabled; • no — update job will be disabled	Configure scheduled updates

Command	Available arguments	Action
-c:set_update_ source_parameters	**-source:** — type of update source. Available values: • https — download updates from the KOD server or other local update servers (for cascading mode); • directory — download updates from a local folder; **-updates_host:** — update server address; **-updates_port:** — update server port; **-eset_user_name:** — user name for ESET license. This parameter does not require configuration; **-download_block_size:** — block size in bytes for downloading from an HTTP source. When the block size is large (in terms of megabytes) and connection is slow, the command may be frequently interrupted due to network time-outs. With a faster connection (at least 100 Mbps), you can specify the value of 1048576 bytes (1MB); **-download_timeout:** — download time-out in seconds; **-time_between_retries:** — time between download retries in seconds; **-download_retry_count:** — number of download retries; **-proxy_mode:** — proxy server mode. Available values: • custom_settings — configure proxy server manually; • direct_connection — use direct Internet connection; • system_proxy — use proxy server settings transmitted over the network via DHCP/DNS. We do not recommend using these settings; **-proxy_address:** — proxy server address (IP address or server name); **-proxy_port:** — proxy server port; **-proxy_authentication:** — type of proxy server authorization. Available values: • no — authorization not required; • yes — authorization required; **-proxy_user_name:** — user name for proxy server authorization; **-proxy_password:** — password for proxy server authorization; **-updates_source_directory:** — path to the local update server folder	Configure update source parameters
-c:set_update_ parameters	**-keep_packages:** — number of stored update packages. If serviced clients use a local (fast) connection, the recommended number of packages is 4; for remote clients using a slow connection, the recommended number is 10; **-max_update_job_storage_time:** — number of days for storing information on completed update jobs in the system. Recommended values are 20-40 days	Change settings for storing update packages and update utilities

Downloading updates from the update server

Example 1

To configure antivirus database updates from a local update server located in the company network with 192.168.221.1 IP address:

```
avus.exe -c:set_update_source_parameters -source:https -
updates_host:192.168.221.1
```

Example 2

To configure antivirus database updates from the KOD server via a proxy server with authorization, type:

```
avus.exe -c:set_update_source_parameters -source:https -
updates_host:updates.securitycode.ru -proxy_mode:custom_
settings -proxy_address:192.168.50.150 -proxy_port:8080 -
proxy_authentication:yes -proxy_user_name:domain\TestUser -
proxy_password:Password123
```

Note.

- The proxy server only supports NTLM authorization.
- For the proxy server, we recommend allowing anonymous access to computers hosting the update servers by using MAC address verification.

Example 3

To configure antivirus database updates from the KOD server without using a proxy server:

```
avus.exe -c:set_update_source_parameters -source:https -
proxy_mode:direct_connection
```

Downloading updates from a folder

Example 1

Configuring antivirus database updates from a local folder:

```
AVUS.exe -c:set_update_source_parameters -source:directory -
updates_source_directory:C:\new
```

Note. Make sure that the computer account has access to the contents of this folder.

Configuring scheduled updates

You can specify the time to start downloading updates in the cron format using the following procedure:

```
* * * * *
- - - - -
| | | | |
| | | | ----- Weekday (0 - 7) (Sunday =0 or =7)
| | | ------- Month (1 - 12)
| | --------- Day (1 - 31)
| ----------- Hour (0 - 23)
------------- Minute (0 - 59)
```

Example 1

To create a job with instructions on downloading available updates every four hours daily, run the following command:

```
avus.exe -c:set_update_schedule -enabled:yes -by_time:"0 */4
* * *"
```

Example 2

To download the updates at 8 am on Saturdays:

```
avus.exe -c:set_update_schedule -enabled:yes -by_time:"0 8 *
* 6"
```

Example 3

To configure the number of stored update packages and information on storage time of completed updates:

```
avus.exe -c:set_update_parameters -max_update_job_storage_
time:40 -keep_packages:4
```

Update utility

Secret Net Studio includes a utility for standalone update of antivirus databases. When you run the utility, it checks antivirus database version of the installed antivirus program. If a newer version is available, the utility will update the databases.

You can download the update utility from the KOD website or the local update server (see Update utility in the document Setup and Operation. Antivirus and Intrusion Detection Tool).

Note.
In Secret Net Studio 8.2, the incoming network traffic on local update servers consists of update packages and update utilities (see p. 14).

Chapter 3
Updating the update server

To update the update server:

1. On computers with the installed update server, run the installation of a new version of the "Antivirus - update server" component (see p. **8**). The program begins preparations. After all preparations are complete, the installation program will display its welcome dialog box. After you confirm your acceptance of the license agreement, the installation program will automatically update the previous software version.
2. Follow the procedure for updating the antivirus database on protected computers (see Updating antivirus databases in the document "Setup and Operation. Antivirus and Intrusion Detection Tool").

Note. Updating version 8.2 antivirus databases Secret Net Studio from version 8.0 or 8.1 update servers is not supported.

Chapter 4
Uninstalling the update server

You can also use Programs and Features in the Windows Control Panel to uninstall the update server.

To uninstall the update server:

1. Click the Uninstall button in the Uninstall, Change, or Repair dialog box.

   A dialog box appears saying that everything is ready for uninstalling the program.
2. Click Uninstall.

   The uninstalling process starts. After successful completion of the uninstalling process, a dialog box with the respective message appears.
3. Click Finish.
4. Delete the folder C:\ProgramData\Security Code\Secret Net Studio\Server\ Antivirus Update Server (C:\ProgramData\Security Code\Secret Net Studio\ Server\Antimalware Update Server).