SECURITY CODE

Secret Net Studio

Administrator's manual

Development principles

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

AD	Active Directory
API	Application Programming Interface
BIOS	Basic Input/Output System
FAT	File Allocation Table
GPT	GUID Partition Table
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IMAPI	Image Mastering Application Programming Interface
MBR	Master Boot Record
MS	Microsoft
MSDN	Microsoft Developers Network
NTFS	New Technology File System
PCMCIA	Personal Computer Memory Card International Association
PKI	Public Key Infrastructure
ReFS	Resilient File System
SSL	Secure Socket Layer
TLS	Transport Layer Security
UDF	Universal Disk Format
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VPN	Virtual Private Network
XML	Extensible Markup Language
XPS	XML Paper Specification
AS	Automated system
DB	Database
CSE	Closed software environment
IS	Information system
IC	Integrity Control
OS	Operating System
OM	Operational management
SW	Software
DAC	Device Access Control
SS	Security Server
DBMS	Database Management System

Introduction

This manual is designed for Secret Net Studio administrators (hereinafter "Secret Net Studio, the System"). It contains information that administrators need to know in order to use the product, as well as Secret Net Studio application options.

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

About Secret Net Studio

Secret Net Studio ensures the security of information systems on computers running MS Windows 10/8/7/Vista and Windows Server 2012/2008 operating systems.

If the respective subsystems are used, the System ensures:

- protection against unauthorized access to informational resources on computers;
- control of devices connected to computers;
- network traffic firewalling;
- network authentication;
- intrusion detection;
- antivirus protection.

You can manage Secret Net Studio centrally or locally.

Main functions

The Secret Net Studio system performs the following main functions:

- user login control (user identification and authentication);
- discretionary control of access to file resources, devices, printers;
- mandatory control of access to file resources, devices, printers, and network interfaces, including:
  - data flow control;
  - control of data output to removable media;
- control of computer device state, with the following options:
  - computer locking in case of the condition of defined devices changes;
  - locking the connection of an unauthorized device (devices from an unauthorized group);
- shadow copying of information being transferred onto external media or to be printed;
- automatic marking of documents being printed;
- integrity control of file objects and registry;
- providing application execution control for users (control over starting of executable modules, loading of dynamic libraries, execution of scripts using Active Scripts technology);
- RAM and external memory wipe at its reallocation;
- process isolation (executable programs) in RAM;
- protection of local hard disks, in case of an unauthorized operating system starts;
- antivirus protection;
- intrusion detection;
- network traffic firewalling;
- network authentication;
- functional control of key security subsystems;
- registration of security events;
- centralized and local control of security mechanism parameters;
- centralized and local control of user's work parameters;
- monitoring and operational management of protected computers;
- centralized collecting, storage and archiving of logs.

Components of the System

The Secret Net Studio system components are as follows:

1. "Secret Net Studio" (hereinafter – "the Client").
2. "Secret Net Studio — Security Server" (hereinafter – "the Security Server").
3. "Secret Net Studio — Control Center" (hereinafter – "the Control Center").

Client

The Client protects the computer it is installed onto. Protection is carried out by security mechanisms that expand and supplement Windows OS security features. Security mechanisms are a set of configurable tools included in the Client that ensure the secure use of resources.

The Client may function in the following modes:

- stand-alone (autonomous) mode – provides local control of security mechanisms;
- network mode — provides local and centralized management of protection mechanisms, as well as centralized retrieval of information and changing protected computer state.

The operation mode can be selected during the installation of the Client.

Security Server

The Security Server makes it possible to centrally control the Clients in network operation mode. This component ensures:

- storage of centralized control data;
- coordination of component operations during centralized system management;
- retrieval and processing of information from the Clients about protected computer;
- user and network authentication management;
- centralized collecting, storage and archiving of logs.

Control Center

The Control Center is used for the centralized management of the Security Servers and Clients in network operation mode. This component ensures:

- object parameter control;
- display of information about protected computer state and recent security alerts;
- loading of event logs;
- operational computer management.

Subsystem licensing

In order to use the security mechanisms of Secret Net Studio, you need to purchase the registered licenses for the respective subsystems. Licenses are required for the following mechanisms:

- basic protection mechanisms (mandatory license);
- discretionary access control;
- device control;
- data wipe;
- application execution control;
- authorized access control;
- printer control;
- disk protection and data encryption;
- firewall;
- network authentication;

- detecting and preventing intrusions;
- antivirus.

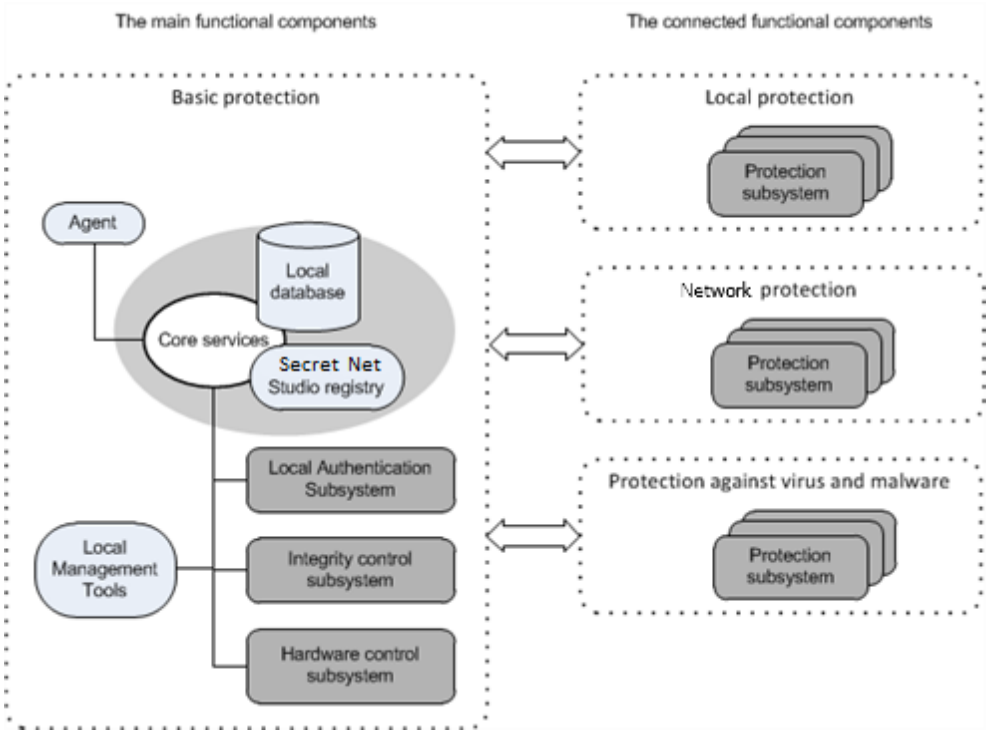
Chapter 2
System components

Client subsystems

The Client contains the following subsystems:

- basic software services, modules and security subsystems (basic protection);
- plugins divided into the following groups:
  - local protection;
  - network protection;
  - malware protection.

The generalized structure of the Client is presented in the figure below.



Basic protection

Basic protection contains of the following software services, modules and security subsystems:

- Core;
- Agent;
- Local Management Tools;
- Local Authentication Subsystem;
- Integrity Control Subsystem;
- Hardware Control Subsystem.

Core

The core service starts automatically when the protected computer is turned on, and functions permanently during computer operation.

The core controls basic protection subsystems and ensures their interaction by performing the following:

- data exchange between the Client subsystems and command processing;

- remote access to information stored in the Local database;
- the System event processing and registering.

Secret Net Studio registry manages the System event logging. Such events are registered in the Secret Net Studio log. This information comes from the Secret Net Studio subsystems that monitor the occurring events. The list of Secret Net Studio events to be logged is defined by the security administrator.

The Local database contains information about the System settings required for the operation of the protected computer. The local database is stored in the Windows OS register.

Agent

The Agent is the Client's module that ensures interaction with the Security Server. The agent receives commands from the Security Server and sends back computer's status information.

The Agent is only enabled in the network operation mode.

Local Management Tools

The Local Management Tools ensure:

- management of security objects (devices, files, folders);
- management of user parameters and security mechanisms;
- creation of integrity control tasks;
- local log viewing.

Local Authentication Subsystem

The Local Authentication Subsystem is used in the login security mechanism. The subsystem aids Windows OS in:

- checking login availability;
- notifying other modules about the beginning and end of a user session;
- locking out the user;
- loading data from user ID tokens;
- providing advanced logon authentication.

When processing a user login, the user context is created: user's privileges, access level, etc. Additionally, the login module performs the Secret Net Studio health control.

Integrity control subsystem

The integrity control subsystem checks the retention of the following computer resources: folders, files, keys and register values. As part of the integrity control mechanism, the subsystem protects resources from substitution, by comparing them with certain reference values. This subsystem does not perform control functions when the user interacts with resources. Control is performed only in case of the system events (loading, user login, scheduled control).

Hardware support subsystem

The Hardware support subsystem is used as a part of the login protection mechanism that controls hardware devices. It ensures the interaction of the Secret Net Studio with a certain devices, and comprises of the following modules:

- the module providing a single interface for handling all supported devices;
- device modules (each module ensures operations with a specific device);
- hardware device drivers (if necessary).

Additional functional components

Local protection

The local protection group includes subsystems that use the following security mechanisms:

- device control;
- printer control;
- application execution control;
- mandatory access control;
- discretionary access control;
- local disk protection;
- data encryption in encrypted containers;
- data wipe.

Network protection

The network protection group includes the subsystems that use the following security mechanisms:

- network authentication;
- firewall.

Malware protection

Malware protection group includes the subsystems that use the following security mechanisms:

- intrusion detection and prevention;
- antivirus.

Chapter 3
Client protection mechanisms

Secure login

Secure login prevents the unauthorized access to the System. The security login mechanism includes the following tools:

- user identification and authentication tools;
- computer locking tools;
- hardware to prevent the start of an OS from removable media.

User identification and authentication

Users are identified and authenticated every time they log into the System. The standard Windows login procedure prescribes entering a user name and password or using hardware tools supported by the operating system.

In the Secret Net Studio system, user identification can be performed in the following modes:

- By name – in order to log in, the user can enter his/her account data (name and password) or use hardware tools supported by the OS;
- Mixed – in order to log in, the user can enter his/her account data (name and password) or use a personal identifier supported by the Secret Net Studio system;
- Only by identifier – in order to log in, each user must log in using his/her personal identifier supported by the Secret Net Studio system.

In order to secure entry to the System, identification and authentication the following tools may be used: eToken, iKey, Rutoken, JaCarta, ESMART identifiers. These devices must be registered (assigned to users) in the System.

Additionally, advanced authentication mode is provided for additional user password checks by the System. In the advanced authentication mode, user passwords are checked for compliance with the current password policy in both the operating system, and in the Secret Net Studio system.

Computer protection can be improved using the following modes:

- interactive login mode for domain users only. In this mode, the login of local users is blocked (local accounts);
- repeated logins prohibited mode. In this mode, it is impossible to execute commands and network connections with the entry of another user's account data (who has not performed an interactive login into the System).

Computer locking

Computer locking tools are designed for the prevention of unauthorized computer use. In this mode, the input devices (keyboard and mouse) and a monitor screen are locked.

Locking as a result of unsuccessful login attempts

You can limit the number of failed login attempts per user. In addition to standard Windows options (blocking user accounts after a certain number of failed password attempts), the System can control unsuccessful system login attempts, if the advanced password authentication mode is enabled. If a user enters a password a certain number of times that is not saved in the System database, the system locks the computer. Computers are unlocked by the administrator. The counter for failed attempts is reset in case of a successful user login or after the computer is unlocked.

Temporary computer locking

Temporary locking mode is enabled in the following cases:

- if the user performs an operation that locks the computer;
- if the preset inactivity interval (idle period) of the computer has ended.

In order to enable locking, the user can use the standard method for computer locking or remove the user's identifier from the reader. To enable locking when removing an identifier, the administrator should configure a response to the operation in the group policy using the Control Center. Locking during the removal of an identifier is enabled as long as the user logs into the System using the identifier.

Locking after a certain period of inactivity is enabled automatically and applied to all computer users.

In order to disable temporary locking, enter the current user password or produce the user's identifier.

Computer locking during the operation of security subsystems

Computer locking is also included in security system operation algorithms. This type of locking is used in the following situations:

- if the functional integrity of the Secret Net Studio system is compromised;
- if the hardware configuration of the computer is changed;
- if the integrity of controlled objects is compromised.

Unlocking the computer in the said cases is performed by the administrator.

Computer locking by the operational management administrator

In network operation mode, a protected computer may be locked and unlocked remotely by a Control Center user command.

Hardware security features

The Secret Net Studio system supports operations with the hardware tools listed in the following table.

Hardware	Main tasks
Identification and authentication tools based on eToken, iKey, Rutoken, JaCarta and ESMART identifiers	• Identification and authentication during user login after the OS is loaded. • Identification and authentication during user login from a remote computer. • Unlocking the computer. • Password and cryptographic key storage in the identifier

The following tools can be applied for user identification and authentication:

- USB keys Rutoken, Rutoken S, Rutoken ECD, Rutoken Lite, JaCarta PKI, JaCarta PKI Flash, JaCarta GOST, JaCarta GOST Flash, eToken PRO, eToken PRO (Java), ESMART Token, ESMART Token GOST;
- contact smart cards Rutoken ECD, Rutoken Lite, JaCarta PKI, JaCarta GOST, eToken PRO, eToken PRO (Java), ESMART Token, ESMART Token GOST with any compatible USB readers.

Functional control of subsystems

The purpose of functional control is to ensure that all key security subsystems are loaded up and functioning at the moment of user login (i.e. at the moment the user begins using the System).

Successful completion of functional control is logged by the System.

If functional control is unsuccessful, the Secret Net Studio system logs this fact and specifies the reasons (possible if the Secret Net Studio core is operable). User login is allowed only for users who are members of the computer's administrator group.

One of the main tasks of functional control is to ensure the protection of the computer's resources when the OS is loaded in Safe Mode. Safe Mode is not considered a standard mode of the Secret Net Studio system's operations. However, the

administrator can use it to fix problems, if necessary. Since some security functions are disabled in Safe Mode, functional control is completed with an error in such situations. As a result, the login of any users, except for administrators, is blocked. Therefore, if security rules are properly followed (when no ordinary user has administrator privileges), access to the computer's resources with a bypass the security mechanisms is impossible.

Event registration

During the operation of the Secret Net Studio system, events occurring in the computer and related to system security are logged by the System. All log records are stored in a file on the system disk. The data format is the same as in the Windows security log.

Configuration options are available for the list of logged events and log storage parameters. This way, you can store the optimal amount of data taking into account the log size and system load.

Integrity Control

The integrity control mechanism keeps track of the inalterability of controlled objects. The objects are controlled automatically, in accordance with a predefined schedule.

Controlled objects may include files, folders and system registry elements. Each object type has a set of controlled parameters. For example, files can be controlled for content integrity, access rights, attributes, as well as their existence, i.e. the availability of files for a specified path.

The System provides for a selection of control time. In particular, control can be performed when the OS is booting up or when a user logs into the System, based on a predefined schedule.

Integrity control can use various scenarios of system response to control tests. One can configure registration of certain types of events (success or failure of a test of an individual object or the whole set of tests) and actions, in case of integrity is compromised (ignore the error, lock the computer or accept the new value as a reference).

All information about objects, methods, control schedules is concentrated in the **data model**. The data model is stored in the local database, and represents a hierarchical list of objects with a description of the links between them. The following categories of objects in ascending hierarchical order, are used:

- resources;
- groups of resources;
- tasks;
- jobs;
- activity agents (computers, users, groups of computers and users).

The data model is common for integrity control and application execution control mechanisms.

Control over local data models on protected computers can be centralized (for clients in network operation mode). Two models of data are created for centralized management in the global catalog: one for computers with 32-bit Windows operating systems and one for computers with 64-bit versions of operating systems. Such a division makes it possible to take into account specific features of the software in use on protected computers with various platforms.

Each of the centralized data models is common for all protected computers with the respective bitness of the Windows operating system (32-bit or 64-bit). When centralized model parameters are modified, the modifications are synchronized locally on the protected computer. New parameters from centralized storage are transferred to the computer, inserted into the local data model, and used afterwards by security mechanisms.

Synchronization may be performed at the following moments:

- during computer booting;
- during user login;
- after login (in the background mode, while the user is working);
- periodically at predetermined time intervals;
- forcibly on the administrator's command;
- immediately after adding changes into the IC-CSE central database.

Centralized model editing has the following features: it is possible to modify a data model with the same Windows OS bitness that is on the administrator's computer. A data model with a different bitness is read-only (it is also possible to export data from that model to another one). Thus, if there are protected computers in the System that have OS versions with a different bitness, the administrator should set up two computers for centralized model control – one on a machine with a 32-bit Windows OS and one on a machine with a 64-bit Windows OS.

Discretionary control of access to file system resources

The Secret Net Studio system includes a control mechanism for discretionary access to file system resources. This mechanism ensures:

- restriction of user access to folders and files on local disks based on an access matrix for actors (users, groups) regarding access objects;
- control of access to objects during local or network access, including access from a system account;
- denial of access to objects bypassing predefined access rights (if standard OS tools or application programs without their own drivers for working with the file system are used);
- independence of operations from the built-in Windows mechanism of discretionary access control. This means that predefined rights to access file objects in the Secret Net Studio system do not effect similar access rights in the Windows OS and vice versa.

Similar to its implementation in the Windows OS, the access matrix in the Secret Net Studio system is a list of file objects in which accounts with access rights are defined. These rights permit or prohibit the execution of certain operations. The list of existing access rights can be found in the following table.

Access right	Folder action	File action
Reading (R)	Permits or prohibits viewing file and subfolder names	Permits or prohibits data reading
	Permits or prohibits viewing file object attributes	
Writing (W)	Permits or prohibits the creation of subfolders and files	Permits or prohibits making changes
	Permits or prohibits changing file object attributes	
Execution (X)	Permits or prohibits moving files within the structure of subfolders	Permits or prohibits execution
Deletion (D)	Permits or prohibits file object deletion	
Access rights change (P)	Permits or prohibits changing rights to access a file object. A user with permission to change access rights to a resource is conventionally considered the resource administrator	

File object access rights can be assigned expressly or inherited from a higher hierarchy element. Expressly assigned rights have a higher priority compared to inherited ones. Access rights are considered being expressly assigned if rights inheritance mode is disabled for an object.

In order to control access lists for files, a special privilege exists: Discretionary Access Control: Access Rights Management. Users who have been granted this privilege can

change access rights for all folders and files on local disks (irrespective of the predefined access rights for objects).

By default, the privilege to control access rights is granted to users included in the local administrator group. In addition, all these users have rights to access resources for reading, writing, execution and deletion purposes (RWXD). These rights are inherited from the root folders of logical partitions. In order to avoid an unintentional lock of the OS that may result from an incorrectly defined right to access resources, it is not possible to change access rights for the root folder of the system disk (%SystemDrive%) or the entire system folder (%SystemRoot%).

File object copying and moving

When a file object is being copied, the access rights inheritance mode is enabled for its copy, even if some expressly assigned rights are assigned to the original object.

The expressly assigned access rights of a file object are retained when the object is moved within its logical partition. If inheritance mode is enabled for the object, the rights of the folder to which the object has been moved will take effect after the move. When moving the object to another logical partition, the rights inheritance mode is enabled.

Audit of file object operations

With the discretionary access control mechanism is operating, the following events can be registered in the Secret Net Studio log: successful access to objects, denial of access, or a change of rights. By default, successful access events are not logged, but access denial and rights change events are logged for all file objects. Logging such events is enabled and disabled by the security administrator when configuring group policy parameters.

You can detail file object audits based on executable operations that require certain access rights. For example, you can enable successful access audit when writing to a file or deleting it. The operations audit can be enabled or disabled by the resource administrator when configuring additional parameters for a file object's access rights.

Overwriting deleted information

Overwriting deleted information makes it impossible to recover and reuse data after its deletion. Guaranteed deletion is achieved by writing a sequence of random numbers instead of the removed information in the freed memory area. An additional level of security can be achieved through several erasure cycles.

When the mechanism is configured, the number of data deletion cycles is specified for the following types of devices that are connected to the computer:

- local disks;
- removable media;
- RAM.

Attention!

Deletion of the swap file is performed using standard Windows tools, when the computer is being turned off. If the Secret Net Studio swap file deletion mode is enabled, we recommend additionally enabling the standard Windows security parameter "On shutdown: clear the virtual memory paging file" (located in Computer Configuration\Windows Parameters\Security settings\Local policies\Security settings).

Files are not deleted when moved to the Recycle Bin, because files are not deleted from the disk at this time. Such files are deleted when the Recycle Bin is cleared.

Control over the connection and change of computer devices

The control mechanism of the connection and change of computer devices ensures:

- timely detection of computer hardware configuration changes, and responses to these changes;
- updated lists of computer devices that are used by the device control mechanism.

Hardware configuration changes are monitored by the security system for devices with the "device is always connected to the computer" control mode enabled.

Initial hardware configuration of the computer is determined during the System installation stage. Control parametrs values are set by default. A control policy can be set up individually for each device, or parameters can be applied that are inherited from models, classes and groups the devices are related to.

The following configuration control methods are used:

- Static configuration control. Each time the computer is started, the subsystem is informed about the actual hardware configuration and compares it with the reference configuration.
- Dynamic configuration control. When the computer is operating (also when it comes out of sleep mode), the device filtering driver monitors device connections, disconnections, and parameter modifications. In case of a configuration change, the filtering driver outputs the respective notification, and the System performs specific actions.

In case of a hardware configuration change, the System waits for the approval of these changes by the security administrator. A hardware configuration approval procedure is required to validate the identified modifications and accept the current hardware configuration as the reference.

Device Control

User access to devices is based on device lists that are created by the device control mechanism (see p. **17**).

The Secret Net Studio system offers the following device control options:

- assignment of standard permissions and restrictions for operations with respect to devices;
- assignment of confidentiality categories and allowed user session confidentiality levels in order to isolate access using mandatory access control.

Access control options depend on the device type. No full or partial isolation of access is applied to devices of specific use or those required for the computer's operation. For example, there are no access restrictions to the processing unit and RAM, but options for the isolation of access to input/output ports are restricted.

If control is disabled for a device, or no connections are allowed for such a device, there is no access isolation for assigned permissions or operation restrictions. User rights to access such devices are not controlled.

When installing the Client, access rights are set for all detected devices that support such access isolation. By default, full access is granted to three standard user groups: "System", "Administrators" and "All". This means that unlimited access is granted to all users for all devices detected on the computer. Then, the security administrator limits user access to certain devices, in compliance with security policy requirements. For this purpose, access rights can be configured directly for devices, or for classes and groups the devices are related to.

By configuring access rights for classes and groups, you can prepare the security system for the possible connection of new devices. Once connected, the new device is included in the respective group, class and model (if any). User access to such a device will be restricted automatically in accordance with the rules set for the group, class or model.

User access to devices with assigned confidentiality levels or session confidentiality levels is controlled by the mandatory access control mechanism.

Application execution control

Application execution control makes it possible to create for any computer user an individual list of allowed software. The security system controls and prohibits the use of the following resources:

- program startup files and libraries that are not included in the list of programs allowed to be started and do not meet certain criteria;
- scenarios that are not included in the list of scenarios allowed to be started and not registered in the database.

Note.
A scenario (also referred to as a "script") is a sequence of executable commands and/or activities in text format. The System controls the execution of scripts using the Active Scripts technology.

Attempts to start unauthorized resources are registered in the log as alerts.

During configuration of the mechanism, a list of resources allowed to be started and executed is created. This list can be created automatically, based on information about the programs installed on a computer, or on log records (security log, or Secret Net Studio log) containing information about started programs, libraries and scripts.

You can enable the integrity control mode for files included in the list (see p. **15**). For this reason, the application execution and integrity control mechanisms use a uniform data model.

The application execution control mechanism does not block the start of programs, libraries and scripts in the following cases:

- if the user has the "Application execution control: Not active" privilege (by default, this privilege is granted to the computer administrator), there is no control over resources started by the user;
- if the "soft" mode of the application execution control mode is enabled, the subsystem controls attempts to start programs, libraries and scripts but the use of all software is allowed. This mode is usually used when the mechanism is being configured.

Process isolation

This mode can be used by the System to isolate processes in order to prevent third party access to data of certain executable modules. If this mode is enabled, the following operations are controlled, with respect to the data exchanged by various processes:

- reading data from the clipboard;
- reading data in another process window;
- writing data to another process window;
- transfer of data between processes using the drag-and-drop method.

A process is considered isolated if isolation is enabled for the executable file of the process. Data exchange with other processes is impossible for an isolated process. The clipboard can be used only when writing or reading data from the same process. Non-isolated processes exchange data without any restrictions.

Process isolation mode can be used when the application execution control mechanism is enabled (the mechanism driver must be functioning). Also, in order to avoid starting copies of executable files in a non-isolated environment, we recommend you configure the AEC mechanism and enable the "hard" operation mode for the mechanism.

Mandatory access control

The mandatory access control mechanism:

- controls user access to information with an assigned confidentiality category (confidential information);
- controls the connection and use of devices with assigned confidentiality categories;
- controls confidential data flows in the System;
- controls the use of network interfaces where acceptable user session confidentiality levels are assigned;
- controls confidential document printing.

By default, the System provides the following confidentiality categories: "non-confidential" (for public information), "confidential" and "strictly confidential". If necessary, more categories can be added with different names, in accordance with the standards adopted by your company. Maximum number of categories is 16.

A confidentiality category can be assigned to the following resources:

- local physical disks (except for disks with logical partitions) and any devices included in the following device groups: USB, PCMCIA, IEEE1394 or Secure Digital;
- folders and files on disks.

The user is granted access to confidential information based on respective access levels. If the user's access level is lower than the resource's confidential category, the system blocks access to the resource. Once access to confidential information is granted, the confidentiality level of the program (process) is elevated to the resource's confidentiality level. This is required in order to avoid saving confidential data in files with lower confidentiality categories.

Mandatory restriction of access for devices is ensured as follows. If a device is connected during a session of a user with a lower access level than the device's category, the System will block the device's connection. If such a device is connected before the user session begins, the user will not be allowed to log in. In flow control mode, the user session confidentiality level must correspond to the categories of all connected devices.

Device operation is allowed irrespective of user access levels, if the "Device is available without regards to confidentiality categories" mode is enabled for the device. This mode is enabled by default.

Access to confidential file content is granted to the user, if the file's category is not higher than the user's access level. At the same time, the confidentiality category of the device where the file is located is also analyzed and has a higher priority compared to the file confidentiality category. If the file's category is lower than the confidentiality level of the device, the system considers the file's category to be the same as the device's category. On the contrary, when the file's category is higher than the device's confidentiality category, the situation is considered incorrect, and access to the file is not granted.

Flow control mode

When using the mechanism in confidential flow control mode, all data handling processes in the System are assigned a common confidentiality level. The required confidentiality level — out of those available to the user — is chosen before the beginning of the computer session. This level cannot be changed before the session ends.

In flow control mode, information can be saved only with a category equivalent to the session's confidentiality level. Access to data that has a category higher than the session's confidentiality level is prohibited altogether (even if the user's access level allows access to such data). Thus, flow control mode ensures strict compliance with the principles of mandatory access isolation, and prevents the unauthorized copying or moving of confidential data.

In flow control mode, the use of devices with a confidentiality category that differs from that of the chosen session level is not allowed. If at the moment of user login devices with different confidentiality categories are connected to the computer, access will be denied due to conflicts with the connected devices. Using devices with a higher confidentiality category than that of the user access level is restricted in the same way as when the flow control mode is disabled.

Flow control mode makes it possible to restrict the use of network interfaces. For each network interface, you can choose the confidentiality levels of sessions, where the interface will be available to the user. If a session with another confidentiality level is opened, the operation of the interface will be blocked by the security system. This makes it possible to organize the work of a user in various networks depending on the chosen session confidentiality level.

The "Adapter is always available" mode is provided for network interfaces (enabled by default). In this mode, network interface operation is allowed irrespective of the session confidentiality level.

Output of confidential information

The mandatory access control mechanism controls the output of confidential information to external media. External media in the Secret Net Studio system are removable disks that have the "irrespective of confidentiality category" access mode enabled. When copying or moving a confidential resource, the initial confidentiality category of the resource on such a medium may be lost. Therefore, the user must be granted the respective privilege, in order to output confidential information to external media in the flow control mode.

In order to prevent the unauthorized output of confidential documents to local and network printers, printer control mode is used. This mechanism ensures the output of confidential documents for printing, only if the respective privilege is granted. Also, a special marker (handle) can be added to a printed document that automatically specifies the document's confidentiality category. Print events are registered in the Secret Net Studio log.

Printer control

The printer control mechanism ensures:

- control of user access to printers;
- registration of documents sent to printing in the Secret Net Studio log;
- printing out documents with a certain confidentiality category;
- automatic addition of markers to printers documents (document marking);
- shadow copying of printed documents.

In order to implement the marking and/or shadow copying functions for printed documents, "virtual printer" drivers are added to the System. Virtual printers correspond to real printers installed on the computer. The list of virtual printers is automatically created when the printer control or shadowing copying mode is enabled. In this case, printing is only possible to virtual printers.

When printing to a virtual printer, additional transformations are performed in order to obtain the image of the printed document in the XML Paper Specification (XPS) format. After this, the XPS document is copied to the shadow copying storage (if the shadow copy function is enabled for the printer), modified as needed, and then sent to the respective printer.

Shadow copying of output data

The shadow copying mechanism ensures the creation of a duplicate of system data output to be sent to removable storage devices. Duplicates (copies) are saved in a special repository that only authorized users have access to. This mechanism is applied to devices that have enabled the "saving of copies when information is being saved" mode.

If copy saving mode is enabled, data can be output to external devices only if the copies of such data are created in the shadow copying repository. If a duplicate cannot be created for some reason, the data output operation is blocked.

Shadow copying is supported for the following types of devices:

- external removable disks;
- floppy disk drives;
- optical disk drives that can write data;
- printers.

When data is output to an external removable disk (for example, a USB flash drive), the copies of files saved to the device during the output operation are saved in the shadow copying repository. If a file is opened for direct editing from the removable

device, its copy will be created in the repository when the new version of the file is saved.

For optical disk devices that can write data, the shadow copying mechanism creates a disk image in the repository if the Image Mastering API (IMAPI) interface is used for writing, or copies of files if the writing is performed in the Universal Disk Format (UDF) file system format.

Attention!
Some software packages that are able to write optical disks use their own device control drivers. Such drivers may access the device while bypassing the shadow copying mechanism. In order to ensure guaranteed control, disk writing should be performed by standard Windows tools only.

Shadow copying of printed documents is performed with the use of the printer control mechanism (see p. 21). An image of a printed document in the XPS (abbreviation of XML Paper Specification) format is saved as a copy of the information to be printed out. XPS is an open XML-based graphical fixed markup format developed by Microsoft.

Control over data output using the shadow copying mechanism is one of the tasks of the audit. Data output events are registered in the System log. Copies in the shadow copying repository are accessible in the log viewing program.

The administrator configures the operation of the shadow copying mechanism via the Control Center. During configuration, the shadow copying repository parameters are defined, and also the mechanism's operation is enabled or disabled for all devices or printers.

Protection of information on local disks

The data protection mechanism on the computer's local disks (disk protection mechanism) is designed to block access to hard disks during an unauthorized start of the computer. A start is considered authorized if it is performed by the OS with the installed Client. All other methods of starting the OS are considered unauthorized (for example, loading from an external medium or the start of another OS installed on the computer).

This mechanism ensures the protection of information during access attempts using standard OS tools.

Operations of the disk protection mechanism are based on the modification of the boot sectors of logical partitions on the computer's hard disks. The content of boot sectors is modified by coding using a special key that is automatically generated when the mechanism is enabled. At the same time, part of service data for the disk protection mechanism are saved in the System registry.

Modification makes it possible to hide information about logical partitions in case of an unauthorized start of the computer. Partitions with modified boot sectors will be considered by the System as unformatted or bad sectors. In case of the authorized start of the computer, the content of boot sectors of protected logical partitions is decoded automatically when they are interacted with.

The protection of logical partitions (i.e., the modification of boot sectors) is enabled by the administrator.

The disk protection mechanism can be used, if the physical disk, from which the OS is loaded, is one of the following types:

- GUID partition disks (GUID Partition Table — GPT) on a UEFI computer (Unified Extensible Firmware Interface). When the mechanism is enabled, a special loader is written to the Secret Net Studio disk in a hidden system UEFI partition, after which the loader is registered in UEFI;
- MBR (Master Boot Record) disk. When the mechanism is enabled, the MBR is modified on the disk as well as part of the space of the zero disk track.

Attention!
In the computer's BIOS settings, the boot virus scan function must be disabled. If such a function supports BIOS, set the "Disabled" value for the "Boot Virus Detection" parameter (the parameter name may differ depending on the computer model and BIOS version).

This mechanism ensures the protection of up to 128 logical partitions, and the total number of physical disks is 32. Logical partitions that have protection mode enabled must have the FAT, NTFS or ReFS file systems. Partitions may be on physical disks with the master boot record (MBR) or with a GUID partition table (GPT). Disks with other types of logical partitions are not supported (for example, dynamic disks).

When using protection mechanisms, there can be only one OS installed on the computer. If several OS are installed, the stable operation of other OS is not guaranteed after the mechanism is enabled.

Data encryption in encrypted containers

The Secret Net Studio system makes it possible to encrypt the contents of file system objects (files and folders). Special repositories are used for encryption and decryption operations – encrypted containers.

A physical encrypted container is a file that can be connected to the System as an additional disk. An encrypted container is a disk image but all operations related to it are performed by the encryption mechanism driver. The driver processes user data in containers, in "transparent encryption mode". This means that the user, once encrypted container has been connected as a disk, performs file operations on the disk and on any other storage medium. No additional operations are required to encrypt or decrypt files. All cryptographic file operations are performed automatically.

Encrypted container can be connected to the System of local disks, removable storage devices or network resources. The amount of available space to save data is specified during the creation of an encrypted container. The volume limit is determined based on the available resource space and file system type. Minimum container size – 1 megabyte.

In order to differentiate user access to encrypted containers in the System, the following rights are available:

- data reading – read-only access to files in the encrypted container;
- full access to data – the right to read and write files within the encrypted container;
- encrypted container management – makes it possible to manage the list of users with access to the encrypted container, as well as read and write files.

The right to create encrypted containers is available to users that have the respective privileges. This privilege is granted by default to accounts included in the local administrator group.

The user who creates an encrypted container is granted the right to manage it and can delegate (grant) access rights to another user. If necessary, the encrypted container creator can be removed from the list of users with access rights, as long as at least one user having the right to manage the encrypted container remains on the list.

In order to work with encrypted resources, users must have encryption keys. Key generation and issue procedures are performed by the security administrator. Key pairs are created for users; each of the pairs consists of a public and a private key. Public keys are stored in a common repository (the local Secret Net Studio database is used for local user keys, while a global catalog repository is used for domain users). Private keys are stored in key carriers assigned to users. Private keys (key information) can be stored on identifiers or removable media, such as memory sticks, USB drives and so on.

General information about the key scheme

Certain sets of keys and additional values used for accessing the encrypted containers are generated and calculated during cryptographic operations.

An encrypted container contains the following groups of data:

- encrypted container control information – a structure of encrypted keys and values for accessing the encrypted container;

- encrypted user data – cryptographically transformed files encrypted in the container by users.

Control information is created when encrypted containers are created. Initially, this structure, together with other information, stores the public key of the user who created the encrypted container. Then, during the creation of the list of users with access to the container, the public keys of these users are also inserted into the structure. The respective parts of the structure are encrypted using public keys.

Files inserted in the encrypted container by users are encrypted using the encryption keys, calculated on the basis of a generic encryption key, which is the same for all users of the encrypted container. The generic encryption key is generated during the creation of a encrypted container. The key is calculated during access to the encrypted container by means of a user's private key.

To provide additional security for the generic encryption key, a special corporate key can be used. This key is generated when a encrypted container is created, provided the parameter "use corporate key" is enabled. The key is stored in the system registry, and used for generic key encryption and decryption.

Where a corporate key is used, access to the encrypted container is possible, if the key is stored in the system registry (in encrypted form). For this reason, to access an encrypted container located on another computer, the corporate key must be imported to the registry on that computer.

Key updating

When using the System, you need to regularly change user keys and generic encryption keys of encrypted containers.

User keys are changed by the user or by the security administrator. The periodicity of user key changes is controlled by the System and can be configured by setting maximum or minimum key validity periods. When changing user keys in the System, two key pairs remain in the System – the current and the previous pair. The previous pair is required for the re-encryption of the respective part of the control information in the user's encrypted containers using the new key. The control information re-encryption starts automatically after a key change.

Attention!

The encrypted container must be available for the automatic re-encryption of control information. For example, if an encrypted container is not available in the network or is located on a currently disconnected removable medium, no re-encryption will take place. In this case, once keys have been changed for the reencryption of control information, the usermust perform an operation involving the encrypted container(for example, connect the encrypted container) priorto the next key change. Otherwise, the previous key pairwill be replaced during the next key change, and the user will not be able to gain access to the encrypted container dueto a keymismatch. In orderto regain access, you will need to remove the userfrom the list of those with access to the encrypted container, and then add the user to the list again.

The generic key for an encrypted container can be changed by the user with the right to manage the encrypted container. In order to change the generic key, the user initiates a container re-encryption procedure. As a result, all encrypted data in the container will be re-encrypted using the new generic key. When using a corporate key, it is changed automatically when the generic one is changed.

Firewall

The Secret Net Studio system ensures network traffic control on the network, transport and application levels based on the created filtration rules.

The Secret Net Studio firewall subsystem carries out the following main functions:

- filtration on the network level with independent decision-making for each packet;
- filtration of service protocol packets (ICMP, IGMP, etc.) required for diagnostics and management of network device operations;
- filtration taking into account the incoming and outgoing network interface, for the authentication of network addresses;

- filtration on the transport level of requests for the establishment of virtual connections (TCP sessions);
- filtration on the application level of requests for application services (filtering by character sequence in packets);
- filtration on the basis of network packet fields;
- filtration on the basis of date/time.

Filtration of network traffic is performed in Ethernet (IEEE 802.3) and Wi-Fi (IEEE 802.11b/g/n) interfaces. Firewall-related events are registered in the Secret Net Studio log.

Network authentication

If the network authentication mechanism is enabled, an electronic signature is added to network packets, ensuring the authenticity and integrity of transferred data, as well as protection against Man-in-the-Middle type attacks.

The network authentication subsystem ensures:

- recieving connection authorization rules from the authorization server included in the Security Server (the list of connection parameters that should be signed);
- receiving the session data from the authorization server for a traffic signature;
- adding a signature to network traffic for packets that meet authorization rules;
- signature analysis for incoming packets and transfer of information about remote user context to the firewall subsystem, for rule-based filtration.

Network connections are authorized in Ethernet (IEEE 802.3) and Wi-Fi (IEEE 802.11b/g/n) interfaces.

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

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

Chapter 4
Setting up centralized system control

Interacting components

The Client in network operation mode

In order to implement centralized control over all protected computers, the Client must be installed in the network operation mode. These computers must be subordinated to the Security Server.

Security Server

Main functions of the Security Server:

- obtaining information from clients on protected computers about the state of workstations and user sessions;
- receiving and sending of information online about alerts logged in protected computers;
- sending control commands to protected computers;
- receiving information about the state of security subsystems on computers and sending commands to change the state of security subsystems;
- receiving and sending group policy parameters specified in the Control Center to protected computers;
- controlling the validity of licenses for the use of Secret Net Studio components;
- receiving logs from protected computers and sending contents of logs to the Security Server database;
- processing database calls;
- archiving and recovery of the contents logs in the database;
- logging of server calls.

The Security Server implements control and management functions with respect to protected computers as long as these computers are subordinate to it. Computers with the Client installed can be subordinate to the Security Server.

For the purpose of the Security Server operation, an MS SQL server-based database management system (DBMS) is required. The Security Server and the DBMS server can be installed on different computers (recommended) or on the same computer.

Authentication server

The Security Server software package also includes a separate application — the authentication server. This application ensures the operation of firewall and network authentication mechanisms. The authentication server is installed and removed together with the Security Server.

Control Center

The Control Center is installed on administrator workstations and used for the centralized control of protected computers. The program interacts with the Security Server and performs its required operations through it.

Security domains

In the Secret Net Studio system, the centralized control of computers and synchronization of security parameters are based on the concept of a security domain. Security domains are composed of objects included in certain Active Directory containers, in organizational units or in the entire AD domain. Like AD domains, several security domains (with their own Security Servers) may form a domain forest.

The first security domain in the AD domain is created when the first Security Server is installed.

The Security Server uses the database for easy access to Active Directory folders (Active Directory Lightweight Directory Services, AD LDS). The Security Servers controls and applies the parameters on protected computers.

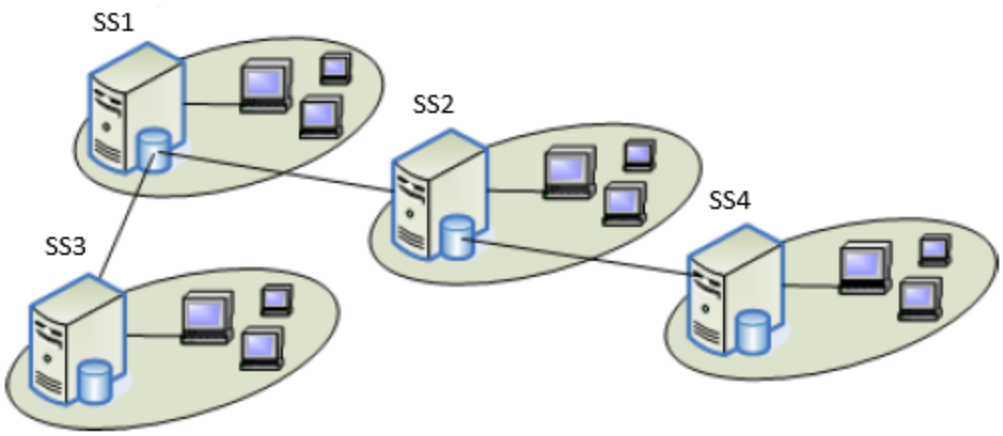
The security domain is created as part of the security domain forest structure. A group of users is assigned to the forest.The users will be granted privileges to create new security domains. This group will be the group of administrators for the security domain forest. When creating a security domain, a group of users is assigned who will be granted the privilege to administer the security domain called the security domain administrators group.

Attention!
To ensure nonstop operations of the protected computers, a permanently running redundant Security Server should be available in the security domain.

Network structure

The Secret Net Studio system network structure is based on the subordination of the network's protected computers to the Security Server. A computer subordinate to the Security Server must be within the security domain.

Within the domain forest, you can organize operations for several Security Servers with hierarchical subordination. At the same time, the hierarchy of server subordination must correspond to the structure of domains in the forest. An example of using multiple servers (SS1 – SS4) is in the figure below.



Each server controls the operation of its own group of protected computers and has its own database. Some operations are also available for objects related to subordinate servers. As you can see in the figure, Security Servers SS2 and SS3 are subordinate to SS1, while SS4 is subordinate to SS2.

The network structure of the Secret Net Studio system can be formed taking into account various network formation features and the allocation of administrator authorities. One of the major factors effecting the network structure of the Secret Net Studio system is the allocation of authorities to security administrators. If you need to share administrator authorities, the security domains must be formed on the basis of organizational units. Doing this makes it possible to share the authorities of security administrators and Active Directory domain administrators as needed, because a security administrator can be assigned all the required administration rights within the organizational unit.

Data exchange between clients and the server is performed in the session mode. Data is transferred over the HTTPS protocol. A certificate must be installed on the server in order to secure server connections.

Domain user management

Domain user parameters are configured in the Control Center. The program is part of the control tools and allows users to create and delete, as well as allows them to configure main parameters of users and groups.

It is recommended to use standard OS tools (user management tools) only for configuring the parameters not available in the Control Center. When creating or deleting accounts using standard tools, some control functions may be unavailable until the changes are synchronized in the System.

Centralized data storage

The components of the System use the following centralized data storage structures:

- Security Server database on the DBMS server – contains centralized logs and operational information for system monitoring;
- AD LDS server database – containsSecret Net Studio system parameters related to accounts, lists of Security Servers, lists of electronic identifiers, and other objects required for the centralized management of the security system.

The partition of repositories is the result of specific ways of handling data. Access calls are performed by those components that are allowed to do so. Control and access limits are ensured by the System itself, therefore, administrators do not need to do anything else to ensure the security of data handling.

Appendix

Required rights for installation and management

Secret Net Studio ensures login and operation executions for any registered users, based on the permissions granted to them by the OS and by security mechanisms. To install Secret Net Studio components and manage the System, the users must also possess certain administrative permissions. Administrative rights and privileges depend on the executed operations.

You must be included in the local administrators group to install and use management functions of the Client in stand-alone mode. Some functions (e.g., Secret Net Studio log management) can be transferred to other users by granting them respective privileges.

Below you can see a list of key operations that you can perform using Secret Net Studio. The accounts with the privilege to execute operations are indicated next to each operation. The following symbols are used for accounts:

- **Security domain forest administrators** — users included in security domain forest administrators group. You can specify which of the existing user groups will become security domain forest administrators during the Security Server installation after selecting to add a new security forest;
- **Security domain administrators** — users included in a security domain administrators group. You can specify which of the existing user groups will become security domain administrators during the Security Server installation after selecting to add a new security domain);
- **Administrators** — users included in the standard local administrators group (Administrators);
- **Privilege <*privilege_name*>** — users to whom the specified privilege is assigned.

Installing and uninstalling components

The following tables contain the main operations for installing and uninstalling Secret Net Studio components.

Tab.1 Install and remove the Security Server

Operation	User accounts with execution rights
Create user groups for security domain forest administrators and security domain administrators	Users with permissions to create AD domain groups and to include users in groups
Add a domain in a new security domain forest a domain in an existing security domain forest	Administrators (domain user) + Security domain administrators
Add a security domain to an existing security forest	Administrators + Security domain forest administrators + Security domain administrators
Add the Security Server to an existing security domain	Administrators + Security domain forest administrators + Security domain administrators
Uninstall the Security Server and remove its information from OM structure	Administrators + Security domain administrators
Uninstall the Security Server without modifiying OM structure [1]	Administrators

[1] You will uninstall the Security Server from the computer, but server-related information will be retained in the OM structure. To remove the Security Server from the OM structure, you may use the Control Center (see p. **31**). This option is available if at least one Security Server

is available for connecting. In case of uninstalling the last domain server in the forest the security forest data is erased.

Tab.2 Install or uninstall the Client

Operation	Users accounts with execution rights
Install and connect the Client to the Security Server	Administrators + Security domain administrators
Install the Client without connecting to the Security Server [1]	Administrators
Uninstall the Client and remove its information from OM structure	Administrators + Security domain administrators
Uninstall the Client without modifying OM structure [2]	Administrators

[1] You will install the Client on the computer, but the Client will not be connected to the Security Server within the OM structure. You may use the Control Center to add the Client to the structure and to subordinate it to the Security Server (see p. **31**).

[2] You will uninstall the Client from the computer, but client-related information will be retained in the OM structure. You may use the Control Center to remove the Client from OM structure (see p. **31**).

Tab.3 Install and uninstall the Control Center

Operation	Users accounts with execution rights
Install	Administrators
Uninstall	Administrators

Configuring mechanisms and management of object parameters

The following table contains the main operations for configuring Secret Net Studio security mechanisms and editing object (user, computer) parameters.

Tab.4 Configuring mechanisms and management of object parameters

Operation	Users accounts with execution rights
Create and delete user groups	Users with permissions to create and delete AD domain accounts + Administrators
Create and delete users	Users with permissions to create and delete AD domain accounts + Security domain administrators + Administrators
Manage user parameters, assign and configure ID tokens	Security domain administrators + Administrators
Locally manage computer parameters, edit account information	Security domain administrators + Administrators
Manage Integrity Control and Application Execution Control parameters	Security domain administrators + Administrators

Using the Control Center

The following table contains the main operations of the Control Center.

Tab.5 Using the Control Center

Operation	Users accounts with execution rights
Connect to the Security Server and view information	Information viewing privilege for the connected server
Configure agents (add to OM structure, remove, subordinate and set up parameters in configuration mode)	Security domain administrators
Configure the Security Server (add to OM structure, remove, subordinate and set up parameters in configuration mode)	Security domain administrators
Correct OM structure after an abnormal uninstallation of the Security Server: uninstallation of the Security Server connected to another security domain in the same security forest [1]	Security domain administrators (in the connection server domain) + Security domain administrators (in the remote server domain)
Configure group policy parameters for domains and organizational units	Security domain administrators + Edit policies privilege for the connection server
Remotely configure local Secret Net Studio parameters: local security police, hardware configuration, security mechanism status	Edit Policies + Operative Command Execution privileges for the connection server
Execute operational management commands: lock, restart, update policy	Operative Command Execution privilege for the connection server
Collect logs from protected computers	On-command log collection privilege for the connection server
Archive logs in the Security Server database	Archiving/restoring logs privilege for the connection server
Acknowledge alarm events (confirmation of information receipt)	Alarm event acknowledgment privilege for the connection server

[1]The operation is necessary, if the Security Server was uninstalled without modifying the OM structure (see p. **30**) and the the Security Server is available for connecting in the Control Center in another security domain of the same security forest. If there is another Security Server in the same domain as the abnormally uninstalled one, removing the object from the OM structure requires the same priviledges as configuring the Security Servers (see above).

Assessing database size for the Security Server

To install and operate the Security Server you must first install a database server. For the best performance you must first estimate the size of the future database and the disk space required on the DBMS server computer. Based on the estimated results, you should choose database server edition (free versions have limited database size) and hardware configuration.

Main assessemnt criteria:

- Event flow rate is a number of registered events during a given period of time. Base value is estimated in Events Per Second (EPS). This includes the events registered in OS logs and in the Secret Net Studio log. Keep in mind that event flow considerably depends on the role of the computer in the system (server, workstation) and on the working and registration parameters set in the subsystems.
- The size of event records — the volume of information about events stored in the logs. Record size depends on the number of filled and empty fields: event descriptions, information about sources and objects, other relevant data. Event record size may vary widely, hence we recommend to estimate its average value.
- Log lifetime — determines the period of time the logs are stored in the database and archives. The logs must be accessible for a quick retrieval of data about incidents and security policy breaches to conduct audits and potential threats identification. Log lifetime should be sufficient to provide a retrospecrive analysis of system status.

Note.

To ensure operability of the database server and reduce database maintenance costs, you should regularly back up logs. By default, backups are stored in the \Archive subfolder of the Security Server installation folder. If necessary you can retrieve backups to the database to analyze the logs they contain.

Below is a sample calculation for a typical AS, protection class 1G, consisting of one Security Server and 100 Client computers. For the Security Server, Windows Server 2012 is used as the OS, for the Clients – Windows 8.

Tab.6 Event flow and average record size on the Security Server

Logs	Average events per second (EPS)	Average record size (bytes)
Standard OS logs	3	1000
Secret Net Studio log	0.05	800

Tab.7 Event flow and average record size on the Client

Logs	Average events per second (EPS)	Average record size (bytes)
Standard OS logs	1	1000
Secret Net Studio log	0.05	800

Tab.8 Logs volume

Logs	Events Per Day	DB population per day (MB) [1]	DB log volume per 7 days (MB) [2]	Archive log volume per year (MB) [3]
Security Server, 1 computer				
Standard OS logs	259,200	259.2	1,814.4	2,365
Secret Net Studio log	4,320	3.5	24.2	31.5
Secret Net Studio client, 100 computers				

Logs	Events Per Day	DB population per day (MB) [1]	DB log volume per 7 days (MB) [2]	Archive log volume per year (MB) [3]
Standard OS logs	8,640,000	8,640	60,480	78,840
Secret Net Studio log	432,000	345.6	2,419.2	3,153
Total				
		9,248.3	**64,737.8**	**84,390**

[1]Specified values refer to the size of tables containing event logs. The total size of the database depends on the sizes of transaction logs and database compressing/compacting operations.

[2]In MS SQL express 2012 (with 10 GB limitation on the database size) the number of data sources can be minimized by reducing the number of subordinate computers down to 10 or by disabling OS log in local log transfer parameters.

[3]Using an archive compression rate of 40:1.

Attention!
To maintain total DB size and performance level, you should regularly back up database server logs and optimize DB stucture to delete blank pages and defragment DB entries. In case of DB overflow (free DBs have limited size) you must perform DB cleaning procedures described in the release notes.

Applying parameters after configuration

Not all changes in security mechanism parameters take effect immediately after they are saved. Some parameters apply on protected computers at certain moments.

Parameters listed below come into effect after computer restart or at next logon. The remaining parameters take effect immediately after changes are saved.

Tab.9 The Control Center parameters

Parameter	Takes effect upon
Status tab — enable/disable security mechanisms	
Discretionary Access Control	After restart
Data wipe	After restart
Device control	After restart
Application Execution Control	After restart
Mandatory Access Control	After restart
Printer control	After restart
Disk protection and data encryption	After restart
Settings tab, Policies section — Logon group parameters	
Inactivity time limit before the screen is locked	At next logon
Deny secondary logon	After restart
Security token removal behavior	At next logon
Number of unsuccessful authentication attempts	At next logon
User identification mode	At next logon
User authentication mode	At next logon
Password policy	At next logon
Settings tab, Policies section — Log group parameters	
Maximum size of the security system log	If increased — immediately. If decreased — after clearing the log

Parameter	Takes effect upon
Accounts with the privilege to view security system log	At next logon
Settings tab, Policies section — User Keys group parameters	
All configurable parameters in the group	At next logon
Settings tab, Policies section — Discretionary Access Control group parameters	
Accounts with access rights management privilege	At next logon
Settings tab, Policies section — Mandatory Access Control group parameters	
Operation mode: Flow control is disabled	After restart
Operation mode: Flow control is enabled	After restart
Operation mode: Strictly control terminal connections	At next logon
Operation mode: Automatically select maximum session level	At next logon
Settings tab, Policies section — Application Execution Control group parameters	
Accounts excluded from Application Execution Control rules	At next logon
Settings tab, Policies section — Disk Protection and Data Encryption group parameters	
Accounts with privileges to create encrypted file containers	At next logon
Settings tab, Policies section — Application Control group parameters	
Redirection of clipboard in RDP connections	At next terminal logon
Settings tab, Policies section — Device Control group parameters	
Device redirection in RDP connections	At next terminal logon
Settings tab, Policies section — Print Control group parameters	
Document Marking	At next logon
Shadow copy	At next logon
Redirection of printers in RDP connections	At next terminal logon
Settings tab, Policies section — Traffic Encryption group parameters	
Accounts with privileges to manage settings of access server connections	At next logon
Settings tab, Policies section — Tracing management group parameters	
All configurable parameters in the group	After restart

Tab.10 Application and data control parameters

Parameter	Takes effect upon
List of resources when setting up AEC (Application Execution Control)	At next logon *
Dialog box for configuring parameters of the subject of control, Modes dialog box	
AEC mode enabled	At next logon*
Process isolation enabled	At next logon*

*To force changes on controlled objects in centralized mode right-click an object/objects, point to Commands and click Apply group policies.

Tab.11 User management parameters

Parameter	Takes effect upon
Account operations: delete, lock, password change	At next logon
User properties configuration window, Security Parameters dialog box— Identifier group parameters	

Parameter	Takes effect upon
User's security tokens	At next logon
User properties configuration window, Security Parameters dialog box— Access group parameters	
All parameters of Mandatory Access Control	At next logon

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