КОД БЕЗОПАСНОСТИ

Средство защиты информации

Secret Net Studio

Сведения о вспомогательных утилитах и файлах настройки

Почтовый адрес:	**115127, Россия, Москва, а/я 66 ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
e-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio" (далее — Secret Net Studio). В нем содержатся сведения об использовании вспомогательных утилит и файлов настройки (далее — вспомогательные средства), необходимых для работы с Secret Net Studio.

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (https://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Общие сведения

Вспомогательные средства позволяют осуществлять настройку и управление Secret Net Studio в тех случаях, когда по каким-либо причинам недостаточно стандартных средств управления или требуется выполнить дополнительные служебные операции.

В документе содержится описание и примеры использования для работы со следующими вспомогательными средствами:

- средства для работы с хранилищем объектов централизованного управления (ЦУ);
- средства для работы с системой управления базами данных (СУБД);
- средства для получения и сохранения сведений;
- средства для подсистем контроля целостности (КЦ) и замкнутой программной среды (ЗПС);
- средства для подсистем полномочного и дискреционного управления доступом;
- средства для подсистемы контроля устройств;
- прочие вспомогательные средства.

Средства для работы с хранилищем объектов ЦУ

Утилита SnDSTool.exe

Утилита SnDSTool.exe предназначена для выполнения действий с хранилищем объектов ЦУ и предоставляет следующие возможности:

- очистка хранилища от сведений о неиспользуемых идентификаторах, которые остаются, например, после удаления доменного пользователя с присвоенными идентификаторами на компьютере без установленного клиента Secret Net Studio;
- получение сведений о доменах безопасности;
- активация признака "Доверять парольной аутентификации Windows при следующем входе" для заданного пользователя в режиме усиленной аутентификации по паролю. При установленной подсистеме сетевой защиты дополнительно устанавливаются необходимые параметры для синхронизации пароля пользователя с данными сервера аутентификации.

Данная утилита находится на установочном компакт-диске системы Secret Net Studio в каталоге \Tools\SecurityCode\SnDSTool\. В зависимости от разрядности ОС — в подкаталогах Win32 и x64.

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
SnDSTool.exe [-lds <сервер> <доменDN> [<порт>]] [-ssl]
-duei|-pds|-rpwd –u <домен\пользователь> -a
<администратор> -p <пароль>
```

Описание команд представлено в следующей таблице.

Команды	Назначение
-?	Получение сведений об использовании утилиты
-lds <сервер> <доменDN> [<порт>]	Подключение к заданному LDS-серверу. Параметр **<сервер>** — имя LDS-сервера. Параметр **<доменDN>** — доменное имя основного домена безопасности в LDS. Если эти параметры не указаны, то будет произведена попытка их чтения из реестра. Параметр **<порт>** — номер порта для подключения к LDS-серверу. Порт не указывается, если по умолчанию используется стандартный номер порта 50002 или используется протокол SSL с номером порта 50003
-ssl	Использование протокола SSL во время соединения по LDAP
-duei	Очистка от сведений о неиспользуемых идентификаторах в текущем домене безопасности
-pds	Вывод сведений обо всех доменах безопасности
-rpwd -u <домен\пользователь> -a <администратор> -p <пароль>	Активация признака "Доверять парольной аутентификации Windows при следующем входе" для заданного пользователя. Для активации признака необходимо указать 3 параметра: • **u <домен\пользователь>** — имя доменного пользователя, для которого активируется признак; • **a <администратор>** — имя администратора LDS; • **p <пароль>** — пароль администратора LDS

Примеры команд:

```
SnDSTool.exe –duei
```

Выполняется очистка от сведений о неиспользуемых идентификаторах в текущем домене безопасности.

```
SnDSTool.exe –lds –duei
```

Выполняется очистка от сведений о неиспользуемых идентификаторах в домене безопасности, параметры соединения с которым хранятся в системном реестре.

```
SnDSTool.exe –lds LdsSrv –pds
```

Выполняется вывод списка имен для всех доменов безопасности в лесу, где размещается сервер безопасности с именем LdsSrv.

```
SnDSTool.exe –rpwd –u Domain\Ivanov –a Administrator
–p Password
```

Выполняется активация признака "Доверять парольной аутентификации Windows при следующем входе" для доменного пользователя Ivanov. При установленной подсистеме сетевой защиты дополнительно устанавливаются необходимые параметры для синхронизации пароля пользователя с данными сервера аутентификации.

Средства для работы с СУБД

Файлы для очистки базы данных сервера безопасности

Набор файлов, состоящий из командных файлов clear.cmd, rebuild.cmd и дополнительных файлов, предназначен для очистки базы данных (БД) сервера безопасности, размещенной на сервере СУБД MS SQL (SQL-сервер). Процедура очистки БД может потребоваться для восстановления работы SQL-сервера в случае переполнения БД сервера безопасности.

Данный набор файлов находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\ClearMSSQL\.

Рекомендуется регулярно выполнять архивирование журналов в БД сервера безопасности и другие необходимые действия для поддержания приемлемого объема этой БД. Очистку БД с использованием указанных файлов следует выполнять только в случае, если произошло переполнение БД и сервер безопасности не может продолжать функционировать. Очистка приведет к потере всей хранящейся в БД информации, включая содержимое журналов, поступивших на централизованное хранение.

На SQL-сервере также рекомендуется периодически запускать команду перестроения индексов с использованием файла rebuild.cmd. При длительной эксплуатации и частом архивировании БД производительность сервера снижается из-за сильной фрагментации данных. Процедура перестроения индексов не требует остановки функционирования сервера, однако для оптимального быстродействия рекомендуется запускать команду в моменты наименьшей нагрузки.

Внимание! Для выполнения процедуры очистки БД требуются права локального администратора на компьютере сервера безопасности и учетные данные администратора БД на SQL-сервере.

Для очистки БД сервера безопасности:

1. На сервере безопасности остановите работу служб IIS (служба веб-публикации) и Secret Net Studio Security Server (служба сервера).
2. На SQL-сервере создайте каталог на локальном диске и скопируйте в него с установочного компакт-диска Secret Net Studio содержимое каталога \Tools\SecurityCode\ClearMSSQL\.
3. Откройте для редактирования скопированные файлы с расширением *.cmd и укажите в них пароль администратора БД, заданный при установке SQL-сервера. Пароль должен быть указан вместо подстроки manager.
4. Запустите на исполнение отредактированный файл clear.cmd. После успешного завершения обработки этого файла запустите файл rebuild.cmd.
5. Перезагрузите сервер безопасности.

Средства для получения и сохранения сведений

Утилита SnDiagReport

Утилита SnDiagReport предназначена для сбора диагностической информации, необходимой разработчикам для изучения проблемных ситуаций.

Данная утилита находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\SnDiagReport\. В зависимости от разрядности ОС — в подкаталогах Win32 и x64. Разрядность утилиты должна соответствовать разрядности установленного продукта.

Внимание! Для работы утилиты с командами -i, -t, -d требуются права локального администратора, для команд -h, -m, -e требуются права локального пользователя.

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
SnDiagReport.exe [-<команда> [параметры]] [-e]
```

Описание основных команд представлено в следующей таблице.

Команды	Параметры	Описание
-h	**-**	Получение сведений об использовании утилиты
-i	**-**	Сбор всех необходимых для диагностики Secret Net Studio файлов и данных в архив SnDiagInfo.cab. Файл архива помещается в каталог пользователя %temp%\SnDiagInfo<дата_и_время_создания>. Является режимом работы утилиты по умолчанию
-t	**on [<путь к каталогу>]**	Включение трассировки Secret Net Studio с параметрами по умолчанию. Для включения требуется перезагрузка компьютера. Параметр <путь к каталогу> — расположение записей журнала трассировки. По умолчанию %systemdrive%\Logs
	off	Отключение трассировки Secret Net Studio. Для отключения требуется перезагрузка компьютера
-d	**-**	Настройка для сбора системной и пользовательской отладочной информации об ошибке, возникшей в процессе работы программы
-m	**-**	Просмотр трассировки Secret Net Studio

Описание дополнительных команд представлено в следующей таблице.

Дополнительные команды	Описание
-e	Выход из утилиты после выполнения команды. Комбинируется с любой командой, описанной в таблице выше

Если выполнен запуск утилиты без указания команд, происходит переход в режим работы по умолчанию.

Примеры команд:

```
SnDiagReport.exe –i –e
```

Выполняется сбор всех необходимых для диагностики Secret Net Studio файлов и данных, которые затем помещаются в файл SnDiagInfo.cab. Файл располагается в каталоге пользователя %temp%\SnDiagInfo<дата_и_время_создания>. После завершения операции осуществляется выход из утилиты.

```
SnDiagReport.exe –t on C:\Datalogs
```

Выполняется включение трассировки Secret Net Studio с параметрами по умолчанию. Записи журнала трассировки будут размещаться в каталоге C:\Datalogs. Трассировка будет включена после перезагрузки компьютера.

Утилита GetEventLog.exe

Утилита GetEventLog.exe предназначена для создания архива журнала Secret Net Studio и копии хранилища теневого копирования. Также предусмотрена возможность очистки журнала и хранилища.

Данная утилита находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\GetEventLog\. В зависимости от разрядности ОС — в подкаталогах Win32 и x64.

Внимание! Создать архив журнала Secret Net Studio может пользователь с привилегией на просмотр журнала. Очистить журнал после создания архива может пользователь с привилегией на управление журналом.

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
GetEventLog.exe -n <имя файла> [-c|-s]
```

Описание команд представлено в следующей таблице.

Команды	Описание
-?	Получение сведений об использовании утилиты
-n <имя файла>	Создание архива журнала Secret Net Studio в файле с расширением .evt или .evtx. В имени файла указывается полный путь к нему. Обязательный параметр
-c	Очистка журнала Secret Net Studio и хранилища теневого копирования после создания архива журнала и копии хранилища теневого копирования. Копия хранилища теневого копирования создается в том же каталоге, что и архив журнала Secret Net Studio. Необязательный параметр
-s	Создание копии хранилища теневого копирования. Не выполняется очистка журнала Secret Net Studio и хранилища теневого копирования. Необязательный параметр

Примеры команд:

```
GetEventLog.exe –n c:\EvtLog\SnEventLog.evtx –c
```

Выполняется создание архива журнала Secret Net Studio в файле SnEventLog.evtx и копии хранилища теневого копирования в том же каталоге. Выполняется очистка журнала и хранилища после создания архива и копии.

```
GetEventLog.exe –n c:\EvtLog\SnEventLog.evtx –s
```

Выполняется создание архива журнала Secret Net Studio в файле SnEventLog.evtx и копии хранилища теневого копирования. Очистка журнала и хранилища не выполняется.

Средства для подсистем контроля целостности и замкнутой программной среды

Утилита SnIcheckCmdTool.exe

Утилита SnIcheckCmdTool.exe предназначена для выполнения действий с локальной БД КЦ-ЗПС, в которой хранится модель данных, и предоставляет следующие возможности:

- запуск полной синхронизации изменений, сделанных в центральной БД КЦ-ЗПС;
- подготовка ресурсов для ЗПС;
- вывод сведений об объектах группы по умолчанию;
- перерасчет эталонов ресурсов;
- обновление хранилищ эталонов, содержащих зафиксированные эталонные значения ресурсов Secret Net Studio для метода контроля "Содержимое" и алгоритма CRC32 (используются при КЦ ресурсов Secret Net Studio и могут быть заменены только при установке авторизованных обновлений ПО системы защиты).

Утилита размещается в каталоге установки клиента Secret Net Studio, по умолчанию — C:\Program Files\Secret Net Studio\Client.

Внимание! Для работы с утилитой требуются права локального администратора.

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
SnIcheckCmdTool.exe /<команда> [<атрибут>
<имя объекта>]
```

Описание команд представлено в следующей таблице.

Команды	Описание
-?	Получение сведений об использовании утилиты
/fullsync	Запуск полной синхронизации изменений в ЦБД КЦ-ЗПС
/fullsynccentral	Запуск полной синхронизации изменений в ЦБД КЦ-ЗПС с использованием функции рассылки оповещений об изменениях для данного компьютера (компьютер должен быть представлен в централизованной модели данных в качестве отдельного субъекта)
/reloaduel	Запуск процедуры подготовки ресурсов для ЗПС. Процедура выполняется для всех пользователей, имеющих открытые сеансы работы на данном компьютере в текущий момент
/defgroup	Вывод списка идентификаторов безопасности (SID) компьютеров, входящих в группу по умолчанию SecretNetICheckDefault или SecretNetICheckDefault64 (в зависимости от разрядности версии ОС на компьютере)
/recalc	Перерасчет эталонных значений указанного ресурса для метода контроля "Содержимое" и алгоритма CRC32 и сохранение их в ЛБД КЦ-ЗПС. Для запуска команды необходимо указывать дополнительные атрибуты, представленные в таблице ниже
/etalon	Запись новых эталонных значений указанного ресурса в локальную базу эталонов дистрибутива Secret Net Studio. База содержит зафиксированные эталоны всех ресурсов Secret Net Studio для метода контроля "Содержимое" и алгоритма CRC32. Для запуска команды необходимо указывать дополнительные атрибуты, представленные в таблице ниже
/etalonxml	Запись новых эталонных значений указанного ресурса в xml-файл с эталонами дистрибутива Secret Net Studio. Для запуска команды необходимо указывать дополнительные атрибуты, представленные в таблице ниже
/defmodel	Импорт модели по умолчанию в базу КЦ

Команды	Описание
/transformxml	Преобразование исходных xml-файлов с данными дистрибутива Secret Net Studio в один отформатированный конечный файл
/rebuild	Повторное открытие сценариев для задач по умолчанию

При запуске с параметрами /recalc, /etalon, /etalonxml необходимо указать дополнительные атрибуты. Сведения об использовании утилиты с указанными параметрами (формат запуска с описанием применяемых атрибутов) выводятся при запуске утилиты с параметром без атрибутов. Предусмотрены следующие атрибуты:

Атрибуты	Описание
f <имя объекта>	Выполнить команду для заданного файла
c <имя объекта>	Выполнить команду для заданного каталога
k <имя объекта>	Выполнить команду для заданного ключа реестра
v <имя объекта>	Выполнить команду для заданного параметра реестра
a <имя объекта>	Выполнить команду для всех файлов в заданном каталоге
r <имя объекта>	Выполнить команду для всех параметров в заданном ключе реестра
w <имя объекта>	Используется при расчете контрольных сумм для 32-разрядных исполняемых файлов, предназначенных для использования в 64-разрядных ОС (не используется для параметра /recalc)

Примеры команд:

```
SnIcheckCmdTool.exe /recalc f snicheckapi.dll
```

Выполняется перерасчет эталонного значения файла snicheckapi.dll.

```
SnIcheckCmdTool.exe /recalc a c:\
```

Выполняется перерасчет эталонных значений всех файлов в корневом каталоге диска C: и их сохранение в ЛБД КЦ-ЗПС. Перерасчет выполняется для эталонов, рассчитанных по алгоритму CRC32.

```
SnIcheckCmdTool.exe /etalonxml c C:\admin
```

Выполняется запись новых эталонных значений указанного каталога admin в xml-файл с эталонами дистрибутива Secret Net Studio.

Средства для подсистем полномочного и дискреционного управления доступом

Утилита SnMCUtil.exe

Утилита SnMCUtil.exe предназначена для формирования списка путей к каталогам перенаправления в режиме контроля потоков и управления правами пользователя. Она предоставляет следующие возможности:

- проверка заданных путей с автоматическим созданием дополнительных каталогов для различных категорий конфиденциальности (в случае отсутствия таких каталогов у заданных путей);
- добавление в список новых путей (создание правил перенаправления);
- удаление путей из списка (удаление правил перенаправления);
- управление уровнем допуска и привилегиями пользователя.

Данная утилита находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\SnMCUtil\. В зависимости от разрядности ОС — в подкаталогах Win32 и x64.

Запуск утилиты может выполняться в сеансе пользователя или в контексте системной учетной записи (например, Планировщиком задач ОС Windows либо через групповые политики). В сеансе пользователя основные функции утилиты доступны при соблюдении тех же условий, какие требуются для работы с программой настройки подсистемы полномочного управления доступом:

- пользователь входит в локальную группу администраторов;
- пользователю назначен наивысший уровень допуска к конфиденциальной информации;
- пользователю предоставлена привилегия "Управление категориями конфиденциальности";
- механизм полномочного управления доступом включен;
- режим контроля потоков отключен.

Внимание! При запуске в контексте системной учетной записи необходимым условием является только включенное состояние механизма полномочного управления доступом.

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
SnMCUtil.exe -<команда> -<параметр> [<аргумент>]
```

Описание команд и параметров представлено в следующей таблице.

Команды	Параметры	Описание
-?	**-**	Получение сведений об использовании утилиты
-redir	**-list**	Отображение имеющихся путей перенаправления
	-add <путь к каталогу> [-apply <путь>]	Добавление нового пути перенаправления. Пути для перенаправления добавляются по одному. Строка может содержать как полный путь, однозначно определяющий данный каталог, так и шаблон (часть пути), позволяющий определить подмножество путей к каталогам. Подмножество путей должно начинаться символом "\", а путь к каталогу указывается без символа "\" в конце. Если в каталоги перенаправления не требуется копировать файлы из исходного каталога — добавьте в конце пути символы "**". Если в каталоги перенаправления не требуется копировать подкаталоги исходного каталога — добавьте в конце пути символы "*". Дополнительный аргумент: **-apply** <путь> — выполнить проверку и обработку для нового пути перенаправления. Параметр <путь> позволяет сузить область проверки до отдельного локального диска (например, C:\) или каталога (C:\Users)

Команды	Параметры	Описание
	-del <путь к каталогу>	Удаление пути перенаправления из списка. Пути для перенаправления удаляются по одному
	-check <путь к каталогу>	Проверка имеющихся путей перенаправления и создание отсутствующих каталогов и файлов
-user	**-get <имя пользователя>**	Отображение текущего уровня допуска и привилегий пользователя. Если имя пользователя длиннее 20 символов, его нужно указывать в формате: "long_user_name@domain"
	-set <имя пользователя> [-level <уровень допуска>] [-privs <набор привилегий>]	Изменение уровня допуска и привилегий пользователя. Дополнительный аргумент: **-level** <уровень допуска> — новый уровень допуска пользователя. Число уровней зависит от настройки системы. По умолчанию заданы 3 уровня: • 0 – неконфиденциально; • 1 – конфиденциально; • 2 – строго конфиденциально. Дополнительный аргумент: **-privs** <набор привилегий> — новые привилегии пользователя. Может принимать значения: • значение не задано – отменить все имеющиеся привилегии пользователя; • ConfManage – управление категориями конфиденциальности; • ConfOutput – вывод конфиденциальной информации; • ConfPrint – печать конфиденциальной информации

Примеры команд:

```
SnMCUtil.exe -redir -add
"\appdata\local\roaming\microsoft product"
```

Выполняется добавление правила перенаправления для шаблона пути "\appdata\local\roaming\microsoft product" без создания самих каталогов перенаправления.

```
SnMCUtil.exe -redir -add
"\appdata\local\roaming\microsoft product" -apply
```

Выполняется добавление правила перенаправления для шаблона пути "\appdata\local\roaming\microsoft product", затем выполняется поиск на всех локальных дисках каталогов, соответствующих шаблону, и создаются нужные каталоги перенаправления.

```
SnMCUtil.exe -redir –check c:\
```

Выполняется поиск на диске C: уже заданных путей перенаправления и создаются недостающие каталоги перенаправления.

```
SnMCUtil.exe -user –get Petrov
```

Выполняется отображение текущего уровня допуска и привилегий пользователя Petrov.

```
SnMCUtil.exe -user -set Petrov -level 2 -privs
ConfManage ConfOutput
```

Выполняется назначение уровня допуска "строго конфиденциально", а также предоставление привилегий "Управление категориями конфиденциальности" и "Вывод конфиденциально информации" пользователю Petrov.

Утилита SnSessLevel.exe

Утилита SnSessLevel.exe предназначена для отображения текущего уровня конфиденциальности сессии пользователя. Если возвращается значение "-1" — режим контроля потоков отключен.

Данная утилита находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\SnSessionLevel\.

Утилита SnSessLevel.exe выполняет действия в режиме командной строки от имени текущего пользователя. Запуск утилиты осуществляется без параметров.

Утилита SetSecAttrib.exe

Утилита SetSecAttrib.exe предназначена для управления параметрами полномочного и дискреционного доступа каталогов и файлов.

Утилита размещается в каталоге установки клиента Secret Net Studio, по умолчанию — C:\Program Files\Secret Net Studio\Client. Ее запуск осуществляется только из этого каталога.

Управление параметрами полномочного доступа

Для изменения параметров полномочного доступа каталога или файла пользователь должен обладать привилегией "Управление категориями конфиденциальности". При ее отсутствии пользователь может только повышать категории для файлов, но не выше своего уровня допуска, уровня конфиденциальности сессии пользователя и категории конфиденциальности каталога.

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
SetSecAttrib.exe <Имя ресурса> [-l <категория>]
[-f <флаг>] [-r <тип рекурсии>]
```

Описание команд представлено в следующей таблице.

Команды	Описание
-?	Получение сведений об использовании утилиты
<Имя ресурса>	Указание полного пути к файлу или каталогу, которому присваивается категория конфиденциальности и флаги наследования
-l <категория>	Присвоение категории конфиденциальности ресурсу. Число категорий зависит от настройки системы. По умолчанию заданы 3 категории конфиденциальности: • 0 – неконфиденциально; • 1 – конфиденциально; • 2 – строго конфиденциально
-f <флаг>	Установка флагов наследования. Только для каталогов. Параметр <флаг> может принимать значения: • флаги не заданы – удалить все флаги наследования; • IF – установить флаг "наследовать для файлов"; • IS – установить флаг "наследовать для каталогов"
-r <тип рекурсии>	Выполнение команд для дочерних объектов каталога. Параметр <тип рекурсии> может принимать значения: • F – обработка указанного каталога и файлов в нем; • S – обработка указанного каталога и подкаталогов без содержащихся в них файлов; • SF – обработка указанного каталога, подкаталогов и всех файлов в них

Примеры команд:

```
SetSecAttrib.exe C:\folder\file.txt
```

Выполняется отображение текущих параметров доступа файла file.txt.

```
SetSecAttrib.exe C:\folder\file.txt –l 1
```

Выполняется присвоение категории "конфиденциально" файлу file.txt.

```
SetSecAttrib.exe C:\folder –f IF IS
```

Выполняется установка флагов наследования для каталога C:\folder. В результате категория конфиденциальности каталога будет в дальнейшем автоматически присваиваться всем создаваемым в нем подкаталогам и файлам.

```
SetSecAttrib.exe C:\folder –l 2 –f IS –r SF
```

Пример использования рекурсии. Каталогу C:\folder, всем его файлам, подкаталогам и файлам в них присваивается категория "строго конфиденциально". Также для этого каталога и всех его подкаталогов устанавливается флаг наследования, требующий автоматического присвоения категории конфиденциальности каталога всем создаваемым в них подкаталогам.

Управление параметрами дискреционного доступа

Для изменения параметров дискреционного доступа ресурсов пользователь должен обладать привилегией "Управление правами доступа" или разрешением на управление правами доступа данного ресурса.

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
SetSecAttrib.exe <Имя ресурса> [-<команда> <блок параметров 1>;<блок параметров 2>;…<блок параметров N>] … [-r <тип рекурсии>]
```

Описание команд и параметров представлено в следующей таблице.

Команды	Параметры	Описание
-?	-	Получение сведений об использовании утилиты
<Имя ресурса>	-	Указание полного пути к файлу или каталогу, которому назначаются права доступа и правила аудита
-s	**<пользователь или группа>:<тип правила>(<виды доступа>)**	Установка новых прав доступа для ресурса взамен имеющихся. При этом наследование прав доступа и правил аудита отключается. Текущие правила аудита полностью сохраняются. Права доступа задаются блоком из 3 параметров. Можно указывать несколько таких блоков, отделяя один от другого символом ";". Параметр <пользователь или группа> — идентификатор безопасности учетной записи (SID) либо полное имя пользователя или группы. Параметр <тип правила> — можно указать только одно значение: "+" разрешение или "-" запрет. Параметр <виды доступа> — перечень разрешаемых или запрещаемых операций. Набор значений: • R – чтение; • W – запись; • X – исполнение; • D – удаление; • P – управление правами доступа
-sa	**<пользователь или группа>:<тип аудита>(<виды доступа>)**	Установка новых правил аудита для ресурса взамен имеющихся. При этом наследование правил аудита и прав доступа отключается. Текущие права доступа полностью сохраняются. Правила аудита задаются блоком из 3 параметров. Можно указывать несколько таких блоков, отделяя один от другого символом ";". Параметр <пользователь или группа> — SID либо полное имя пользователя или группы. Параметр <тип аудита> — можно указать одно или оба значения: "+" успех, "-" отказ (или "+-"). Параметр <виды доступа> — перечень операций, подлежащих аудиту. Набор значений аналогичен приведенному выше для команды **-s**

Команды	Параметры	Описание
-g	**<пользователь или группа>:(<виды доступа>)**	Добавление разрешений к действующим правам доступа. При этом наследование прав доступа и правил аудита отключается. Текущие правила аудита полностью сохраняются. Разрешения задаются блоком из 2 параметров. Можно указывать несколько таких блоков, отделяя один от другого символом ";". Параметр <пользователь или группа> — SID либо полное имя пользователя или группы. Параметр <виды доступа> — перечень разрешаемых операций. Набор значений аналогичен приведенному выше для команды -**s**
-d	**<пользователь или группа>:(<виды доступа>)**	Добавление запретов к действующим правам доступа. При этом наследование прав доступа и правил аудита отключается. Текущие правила аудита полностью сохраняются. Запреты задаются блоком из 2 параметров. Можно указывать несколько таких блоков, отделяя один от другого символом ";". Параметр <пользователь или группа> — SID либо полное имя пользователя или группы. Параметр <виды доступа> — перечень запрещаемых операций. Набор значений аналогичен приведенному выше для команды -**s**
-a	**<пользователь или группа>:<тип аудита>(<виды доступа>)**	Добавление правил аудита к действующим правилам. При этом наследование правил аудита и прав доступа отключается. Текущие права доступа полностью сохраняются. Правила аудита задаются блоком из 3 параметров. Можно указывать несколько таких блоков, отделяя один от другого символом ";". Параметр <пользователь или группа> — SID либо полное имя пользователя или группы. Параметр <тип аудита> — можно указать одно или оба значения: "+" успех, "-" отказ (или "+-"). Параметр <виды доступа> — перечень операций, подлежащих аудиту. Набор значений аналогичен приведенному выше для команды -**s**
-c	-	Включение для заданного ресурса режима наследования прав доступа и правил аудита от вышестоящего каталога. Текущие прав доступа и правила аудита удаляются
-r	**<тип рекурсии>**	Выполнение команд и для дочерних объектов каталога. Параметр <тип рекурсии> может принимать значения: • F – обработка указанного каталога и файлов в нем; • S – обработка указанного каталога и подкаталогов без содержащихся в них файлов; • SF – обработка указанного каталога, подкаталогов и всех файлов в них

Примеры команд:

Установка новых прав доступа и правил аудита:

```
SetSecAttrib.exe C:\folder\file.txt -s S-1-1-0:-(WD);
BUILTIN\Администраторы:+(RWXDP)
```

Выполняется установка новых прав доступа для файла file.txt взамен имеющихся и отключение режима наследования (если он был включен). Пользователю с SID S-1-1-0 запрещаются операции "запись" и "удаление". Группе Администраторы разрешаются все операции. Правила аудита не меняются.

```
SetSecAttrib.exe C:\folder –sa DOMAIN\Ivanov:+-(RWX)
```

Выполняется установка новых правил аудита для каталога folder взамен имеющихся и отключение режима наследования (если он был включен). Для доменного пользователя DOMAIN\Ivanov будут регистрироваться все успешные и неуспешные попытки выполнения операций "чтение", "запись" и "выполнение". Права доступа не меняются.

```
SetSecAttrib.exe C:\folder\file.txt -s S-1-1-0:+(RWXD)
–sa S-1-1-0:-(RWXD)
```

Пример использования команд установки прав доступа и правил аудита в одной командной строке.

Изменение прав доступа и правил аудита:

```
SetSecAttrib.exe C:\folder –g DOMAIN\Ivanov:(P)
```

Выполняется добавление разрешений к действующим правам доступа для каталога folder и отключение режима наследования (если он был включен). Доменному пользователю DOMAIN\Ivanov теперь разрешается управлять правами доступа для данного каталога. Правила аудита не меняются.

```
SetSecAttrib.exe C:\folder\file.txt -d S-1-1-0:(WD)
```

Выполняется добавление запретов к действующим правам доступа для файла file.txt и отключение режима наследования (если он был включен). Пользователю с SID S-1-1-0 теперь запрещаются операции "запись" и "удаление". Правила аудита не меняются.

```
SetSecAttrib.exe C:\folder -a DOMAIN\Ivanov:+-(X)
```

Выполняется добавление правил аудита к действующим правилам для каталога folder и отключение режима наследования (если он был включен). Для доменного пользователя DOMAIN\Ivanov теперь будут регистрироваться все успешные и неуспешные попытки запуска в каталоге исполняемых файлов. Права доступа не меняются.

Включение наследования:

```
SetSecAttrib.exe C:\folder –c
```

Выполняется включение для каталога folder режима наследования прав доступа и правил аудита от вышестоящего каталога. Текущие права доступа и правила аудита удаляются.

Дополнительные примеры:

```
SetSecAttrib.exe C:\folder –g DOMAIN\Ivanov:(P) –r S
```

Пример использования рекурсии. Для каталога folder и всех его подкаталогов к действующим правам доступа добавляются новые разрешения.

```
SetSecAttrib.exe C:\folder –l 2 –f IS –g S-1-1-0:(RWX)
–r F
```

Пример использования команд управления параметрами полномочного и дискреционного доступа в одной командной строке.

Средства для подсистемы контроля устройств

Утилита SnHwUtil.exe

Утилита SnHwUtil.exe предназначена для работы со списком устройств компьютера и предоставляет следующие возможности:

- утверждение обнаруженных изменений в конфигурации устройств;
- проверка изменений в конфигурации устройств;
- загрузка актуального списка устройств;
- поиск и исправление недействительных записей в списке устройств;
- удаление явно заданных параметров контроля и прав доступа в списке устройств;
- удаление из списка устройств, которые отсутствуют на компьютере;
- экспорт списка устройств в файл.

Данная утилита находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\SnHwUtil\. В зависимости от разрядности ОС — в подкаталогах Win32 и x64.

Внимание! Для доступа к списку устройств требуются права локального администратора.

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
SnHwUtil.exe -<команда>
```

Описание команд представлено в следующей таблице.

Команды	Описание
-?	Получение сведений об использовании утилиты
-c	Утверждение конфигурации оборудования
-q	Проверка конфигурации оборудования
-s	Обновление списка устройств
-v	Поиск и исправление недействительных записей в списке устройств
-r	Удаление явных настроек управления и прав доступа для всех устройств из списка устройств
-d [-g]	Удаление устройств, не существующих на компьютере, из списка устройств
-f [<Имя файла>]	Экспорт локальной политики устройств в файл
-e [<Имя файла>]	Экспорт локальной базы устройств в файл
-p [<Имя файла>]	Экспорт локальной базы принтеров в файл

Прочие вспомогательные средства

Утилита SnetPol.exe

Утилита SnetPol.exe предназначена для экспорта и импорта параметров Secret Net Studio эффективной (результирующей) политики на компьютере. Экспорт/импорт выполняется с использованием файлов-шаблонов групповых политик, формат которых соответствует файлам сведений ОС Windows (*.inf).

Данная утилита находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\SnetPol\. В зависимости от разрядности ОС — в подкаталогах Win32 и x64.

Внимание! Для доступа к параметрам политики требуются права локального администратора.

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
SnetPol.exe -<команда>
```

Описание команд представлено в следующей таблице.

Команды	Описание
-h	Получение сведений об использовании утилиты
-i <имя файла>	Импорт настроек политики из файла-шаблона
-e <имя файла>	Экспорт настроек политики в файл-шаблон и в xml-файлы блоков политики
-x <компонент защиты> <имя файла>	Загрузка из xml-файла настроек политики для указанного компонента защиты в эффективную политику безопасности Secret Net Studio. Для компонентов защиты используются следующие обозначения: AV - антивирус, NIPS – обнаружение и предотвращение вторжений, UDP – обновление компонентов, SOFTPSPT – паспорт ПО

Пример команды:

```
SnetPol.exe –x AV "c:\AV.xml"
```

Выполняется загрузка настроек политики для антивируса из файла AV.xml.

```
SnetPol.exe –i "c:\test.inf"
```

Выполняется импорт настроек политики из файла test.inf.

Файлы trace_on.reg и trace_off.reg

Файлы trace_on.reg и trace_off.reg предназначены для изменения значений параметров системного реестра, определяющих включение и отключение трассировки. Трассировка — сервисная функция для сбора информации о работе Secret Net Studio.

Данные файлы находятся на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\Trace\.

Внимание! При включенной трассировке осуществляется запись служебных данных о функционировании программных модулей. Эти данные необходимы для диагностики возникновения сбойных или ошибочных ситуаций. Сведения о необходимых действиях предоставляются при обращении в отдел технической поддержки компании "Код Безопасности".

Не рекомендуется включать функцию трассировки без особой необходимости. В штатном режиме эксплуатации Secret Net Studio данная функция должна быть отключена, чтобы не создавать лишнюю нагрузку для компьютера.

Внимание! Для внесения изменений в системный реестр требуются права локального администратора.

Чтобы включить или отключить трассировку, запустите редактор реестра и импортируйте содержимое файла trace_on.reg или trace_off.reg соответственно. Или воспользуйтесь одноименными файлами *.cmd из этого же каталога.

Внимание! Для корректного функционирования трассировки необходимо перезагрузить компьютер.

Утилита SnFCUtil.exe

Утилита SnFCUtil.exe предназначена для настройки подсистемы управления доступом к файлам и каталогам.

Данная утилита находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\SnFCUtil\. В зависимости от разрядности ОС — в подкаталогах Win32 и x64.

Утилита содержит одну команду и выполняет действия в режиме командной строки от имени текущего пользователя.

Пример команды:

```
SnFCUtil.exe -base -fix
```

Восстановление сопоставления с логическими томами локальных баз ресурсов.

CitrixConfig

Файл CitrixConfig.cmd предназначен для настройки процесса подготовки базового образа для системы Citrix PvD. Он находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\CitrixConfig\.

Внимание! При включенной самозащите Secret Net Studio выполнить данную операцию невозможно. Перед использованием CitrixConfig.cmd переключите механизм самозащиты в сервисный режим или отключите его.

SnetApi

Данное расширение находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\SnetApi\.

Подробные сведения об использовании этой библиотеки предоставляются при обращении в службу технической поддержки компании-поставщика.

Ngeninstall

Файл ngeninstall.cmd предназначен для проведения статической компиляции программы управления в код целевой платформы с целью ускорения ее запуска. При установке программы управления компиляция выполняется автоматически. Однако при обновлении программы управления откомпилированные файлы могут быть удалены. Это приведет к замедлению старта программы управления. В таком случае рекомендуется повторно откомпилировать программу управления путем вызова файла ngeninstall.cmd.

Запуск файла осуществляется с правами локального администратора компьютера. Файл ngeninstall.cmd находится на установочном компакт-диске Secret Net Studio в каталоге \Tools\SecurityCode\Ngeninstall\.