ООО «С-Терра СиЭсПи»
124460, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон/Факс: +7 (499) 940 9061
Эл. почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный комплекс С-Терра Клиент. Версия 4.1

Руководство пользователя

РЛКЕ.00009-02 90 04

15.02.2016

Содержание

1. Назначение и функции Продукта

«Программный комплекс С-Терра Клиент. Версия 4.1» функционирует на аппаратных платформах в архитектуре Intel x86/x86-64 под управлением операционных систем Microsoft Windows.

«Программный комплекс С-Терра Клиент. Версия 4.1» (далее Продукт S-Terra Client, Продукт, S-Terra Client, С-Терра Клиент) выполняет роль персонального экрана и VPN клиента.

S-Terra Client может устанавливаться на:

- *персональный компьютер пользователя* – для защиты индивидуального рабочего места пользователя при работе как в локальных, так и в открытых сетях (Интернет)
- *автономный сервер*
- *специализированные устройства в составе платежных систем: банкоматы, расчетные терминалы, кассовые аппараты (POS-терминалы) и датчики автоматизированных систем управления технологическими процессами.*

S-Terra Client предназначен для защиты от несанкционированного доступа, сетевых атак, создания защищенных VPN соединений между устройством, на котором он установлен, и другими взаимодействующими с ним доверенными VPN-шлюзами и VPN-клиентами.

Продукт S-Terra Client выполняет следующие функции:

- защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP
- пакетную и контекстную фильтрацию любого исходящего и входящего трафика на хост с использованием информации в полях заголовков сетевого, транспортного и прикладного уровней;
- фильтрацию с учетом входного и выходного сетевого интерфейса;
- фильтрацию запросов на установление виртуальных соединений;
- фильтрацию по любым значимым полям IP-заголовка и полям данных сетевого пакета;
- фильтрацию с учетом даты и времени;
- аутентификацию пользователя и аутентификацию узла сети;
- идентификацию и аутентификацию администратора при доступе с целью администрирования;
- событийное протоколирование;
- реализацию заданной дисциплины взаимодействия (аутентификацию и/или защиту трафика) для каждого защищенного соединения, доступ в заданном защищенном режиме только для зарегистрированных, в том числе и для мобильных партнеров по взаимодействию;
- регулируемую стойкость защиты трафика.

S-Terra Client осуществляет защиту трафика протоколов семейства TCP/IP в рамках международных стандартов IKE/IPsec:

- Security Architecture for the Internet Protocol – RFC2401
- IP Authentication Header (AH) – RFC2402
- IP Encapsulating Security Payload (ESP) – RFC2406
- Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408
- The Internet Key Exchange (IKE) – RFC2409
- The Internet IP Security Domain of Interpretation for ISAKMP (DOI) – RFC2407.

Продукт S-Terra Client использует в качестве внешней криптографической библиотеки средство криптографической защиты информации (СКЗИ) "КриптоПро CSP 3.6/3.6R2/3.6R4/3.9", разработанное компанией "Крипто-Про".

СКЗИ "КриптоПро CSP" реализует российские криптографические алгоритмы:

- ГОСТ 28147-89 – шифрование/расшифрование данных,
- ГОСТ Р 34.11-94 – алгоритм хэширования,
- ГОСТ Р 34.10-2001 – формирование и проверка электронно-цифровой подписи (ЭЦП),
- VKO ГОСТ Р 34.10-2001 [RFC 4357] – выработка общего сессионного ключа,
- а также генерацию случайных чисел.

Продукт S-Terra Client работает не только с криптоалгоритмами ГОСТ, но и с международными алгоритмами.

Продукт S-Terra Client в режиме КС1 обеспечивают защиту конфиденциальной информации от внешнего нарушителя.

Продукты S-Terra Client в режиме КС2 и сертифицированное средство доверенной загрузки обеспечивают защиту конфиденциальной информации от внутреннего нарушителя.

S-Terra Client является продуктом для корпоративного использования в том смысле, что политику безопасности и настройки режимов этого Продукта осуществляет администратор безопасности предприятия, но он может дать разрешение на дальнейшее управление продуктом конечному пользователю.

Возможно централизованно-удаленное управление настройками S-Terra Client с использованием продукта «С-Терра КП. Версия 4.1». С его помощью можно обновить сертификаты, ключи, политику безопасности, лицензии и др.

В Продукте S-Terra Client по умолчанию для всех интерфейсов задается одинаковая политика безопасности. Для задания разной политики безопасности на интерфейсах используйте структуру NetworkInterface или программный продукт «С-Терра КП. Версия 4.1».

2. Требования на базовые платформы и совместимость

Продукт S-Terra Client работает под управлением следующих ОС:

- MS Windows XP SP3 Russian Edition,
- MS Windows Vista SP2 Russian Edition 32-bit,
- MS Windows 7 Russian Edition (32-bit, 64-bit),
- MS Windows 8 Russian Edition (32-bit, 64-bit),
- MS Windows 8.1 Russian Edition (32-bit, 64-bit),
- MS Windows Server 2003 Edition 32-bit,
- MS Windows Server 2008 Edition (32-bit, 64-bit),
- MS Windows Server 2008R2 Edition 64-bit,
- MS Windows Server 2012 Edition 64-bit.

Программный комплекс С-Терра Клиент (исполнения класса защиты КС1) может функционировать в виртуальной среде (VMWare).

Продукт, работающий под управлением ОС Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008, совместим с криптографическими библиотеками, разработанными компанией "Крипто-Про":

- "КриптоПро CSP 3.6" (версия 3.6.5402),
- "КриптоПро CSP 3.6R2" (версия 3.6.6497),
- "КриптоПро CSP 3.6R4",
- "КриптоПро CSP 3.9".

Продукт, работающий под управлением ОС Windows 7, Windows 8, Windows Server 2008R2, совместим с криптографической библиотекой, разработанной компанией "Крипто-Про":

- "КриптоПро CSP 3.6R2" (версия 3.6.6497),
- "КриптоПро CSP 3.6R4",
- "КриптоПро CSP 3.9".

Продукт, работающий под управлением ОС MS Windows Server 2012, совместим с криптографической библиотекой, разработанной компанией "Крипто-Про":

- "КриптоПро CSP 3.6R4",
- "КриптоПро CSP 3.9".

Продукт, работающий под управлением ОС MS Windows 8.1, совместим с криптографической библиотекой, разработанной компанией "Крипто-Про":

- "КриптоПро CSP 3.9".

Продукт S-Terra Client 4.1 совместим со следующими продуктами компании «С-Терра СиЭсПи»:

CSP VPN Gate – версии 3.1, 3.11,
S-Terra Gate – версии 4.1,
CSP VPN Server – версии 3.1, 3.11,
С-Терра КП – версии 3.11, 4.1.

В части реализации протоколов IPsec/IKE и их расширений Продукт совместим с Cisco IOS v.12.4 и v.15.x.x.

Продукт совместим с eToken PRO32k, eToken PRO64k, eToken NG-FLASH, eToken NG-OTP, eToken PRO (Java) производства компании Aladdin, а также eToken 5100 производства SafeNet Incorporation.

3. Атрибуты аутентификации

Для аутентификации взаимодействующих сторон протоколу IKE необходима некоторая аутентификационная информация.

Такой аутентификационной информацией может быть:

- предопределенный (разделяемый) ключ (Preshared Key),
- сертификат открытого ключа стандарта X.509.

Предопределеный ключ

Предопределенный ключ – произвольная последовательность байтов, которая может быть записана в файл. Самый простой способ создать предопределенный ключ – записать в файл любую произвольную последовательность символов.

Сертификат открытого ключа

При подготовке ***локального сертификата*** пользователя возможны несколько сценариев, описанных ниже. Более подробное описание приведено в «Приложении А», в разделе «Получение сертификата пользователя».

Режим защиты КС1

Первый сценарий

Все действия по созданию ключевой пары, формированию запроса и созданию сертификата пользователя выполняются администратором СА. При этом контейнер с секретным ключом записывается на внешний ключевой носитель, например, eToken, поддерживаемый СКЗИ «КриптоПро CSP». Администратор безопасности получает Корневой сертификат Удостоверяющего Центра (Trusted CA Certificate), сертификат пользователя, импортированные в файлы, а также контейнер на внешнем носителе.

Второй сценарий

Все действия по созданию ключевой пары и формированию запроса на сертификат пользователя выполняются на компьютере пользователя (на котором в дальнейшем и будет установлен Продукт S-Terra Client) либо администратором безопасности, либо пользователем. При этом контейнер с секретным ключом размещается на компьютере пользователя в локальном хранилище, например, в Реестре. Подробно эти действия описаны в «Приложении А» в разделе «Создание ключевой пары и формирование запроса на сертификат пользователя».

Режим защиты КС2

Для режима защиты КС2 ПК от НСД создание ключевой пары и запроса на сертификат пользователя должны выполняться на компьютере с установленным ССДЗ («Соболь» или «Аккорд») (это может быть либо компьютер пользователя, либо администратора). В этом случае при создании ключевой пары будет использоваться не биологический ДСЧ, а аппаратный. Контейнер с секретным ключом должен размещаться на внешнем ключевом носителе, например, eToken.

Добавление аппаратного ДСЧ в «КриптоПро CSP» и создание ключевой пары и запроса на сертификат описано в «Приложении А».

Особенности генерации ключевой пары для режима защиты КС2, если для ССДЗ не поддерживается функциональность ДСЧ описаны в соответствующем разделе в «Приложении А».

Работа с eToken

При инициализации eToken не устанавливайте флажок «При первом входе необходимо изменить пароль»

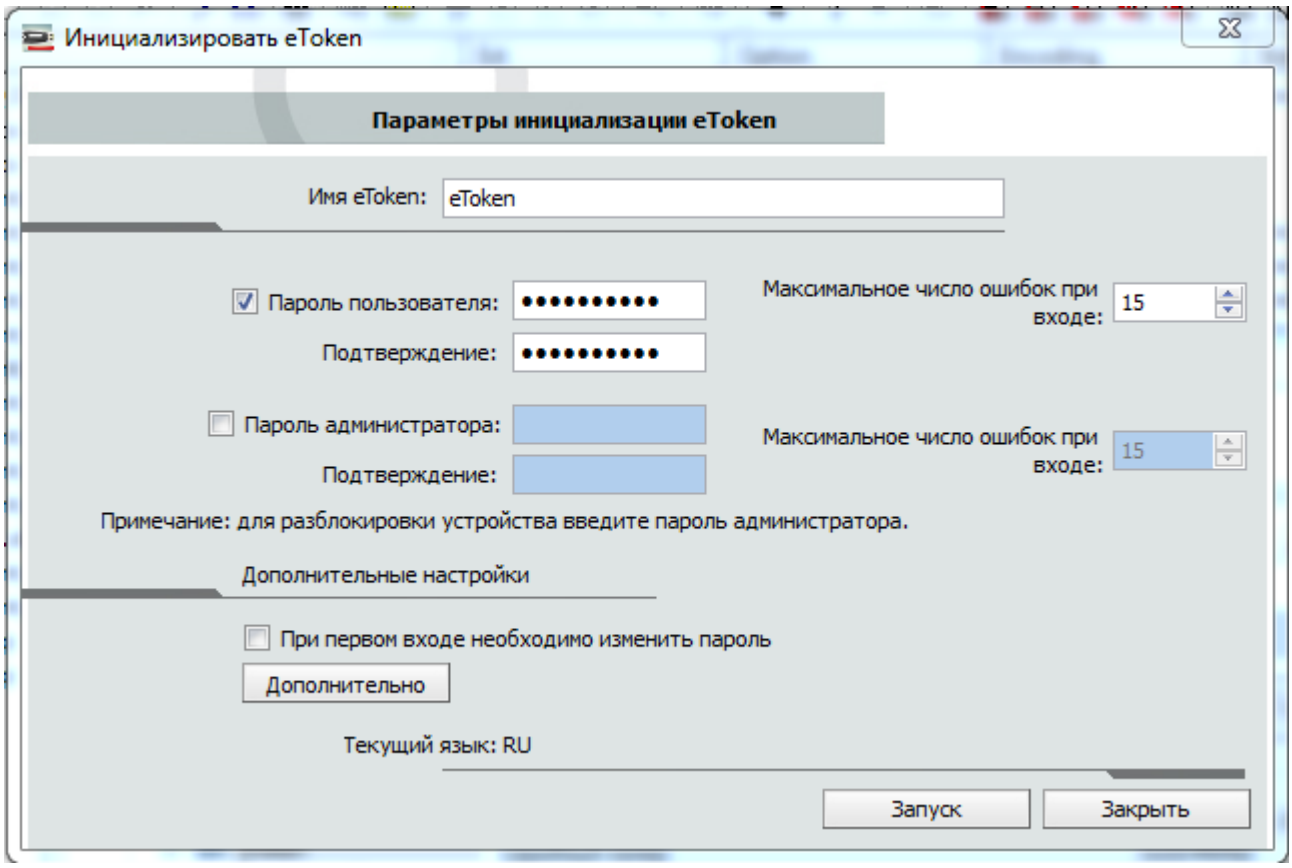


Рисунок 1

4. Процесс подготовки персонального инсталляционного пакета пользователя

Персональный инсталляционный пакет пользователя готовит администратор безопасности и поэтому эта информация для пользователя носит ознакомительный характер.

Продукт S-Terra Client предназначен для виртуальных корпоративных сетей. Полагаем, что в таких сетях пользователь не имеет права на изменение политики безопасности корпоративной сети. Поэтому, Продукт S-Terra Client разработан таким образом, что администратор безопасности корпоративной сети формирует персонализованный инсталляционный пакет для каждого пользователя, при этом настройки для пользователя согласуются с его должностными обязанностями.

Действия администратора при подготовке персонализованного инсталляционного пакета пользователя могут различаться в зависимости от используемого метода аутентификации сторон и местонахождения контейнера с секретным ключом..

При использовании ***предопределенного ключа*** для аутентификации сторон администратору предоставляется возможность считать созданный ключ либо из файла, либо ввести его с клавиатуры, задать локальную политику безопасности для данного пользователя, персональные настройки, и создать инсталляционный файл S-Terra Client, который и будет передан пользователю.

При использовании ***сертификатов открытого ключа*** для аутентификации сторон возможны два сценария подготовки инсталляционного пакета, которые отличаются тем имеет ли администратор на своем рабочем месте доступ к контейнеру с секретным ключом сертификата пользователя.

Первый сценарий

Шаг 1: Администратор безопасности получает от администратора CA Корневой сертификат Удостоверяющего Центра (Trusted CA Certificate) и сертификат пользователя, импортированные в файлы, и также контейнер на внешнем носителе.

Поэтому в данном сценарии возможно на компьютере администратора провести проверку соответствия сертификата пользователя и секретного ключа в контейнере при создании инсталляционного файла.

Шаг 2: Администратор безопасности на своем рабочем месте с помощью GUI задает локальную политику безопасности для данного пользователя, путь к локальному и CA сертификату, имя контейнера с секретным ключом – где он будет размещен на компьютере пользователя, локальные настройки, создает инсталляционный файл S-Terra Client.

Шаг 3: Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из:

- инсталляционного файла S-Terra Client
- контейнера с секретным ключом на внешнем ключевом носителе
- утилиты `integr_mgr`
- файла с контрольной суммой инсталляционного файла S-Terra Client.

Контейнер и файл с контрольной суммой должны быть переданы пользователю по заслуживающему доверия каналу связи. Инсталляционный файл S-Terra Client содержит базовый инсталляционный файл, локальную политику безопасности, сертификат пользователя и CA сертификат, персональные настройки.

Если администратор подготовил пользовательский токен, то пользователю передается подготовленный инсталляционный пакет, состоящий из:

- инсталляционного файла S-Terra Client
- пользовательского токена с записанным на нем CA сертификатом, локальным сертификатом, контейнером с секретным ключом и локальной политикой безопасности
- утилиты `integr_mgr` для вычисления контрольной суммы
- файла с контрольной суммой инсталляционного файла S-Terra Client.

Пользовательский токен и файл с контрольной суммой должны быть переданы пользователю по заслуживающему доверия каналу связи.

Второй сценарий

Шаг 1: На компьютере пользователя создается ключевая пара и запрос на сертификат пользователя, который отсылается в Удостоверяющий Центр. Контейнер с секретным ключом размещается на компьютере пользователя в локальном хранилище. Администратор безопасности получает из CA Корневой сертификат Удостоверяющего Центра (Trusted CA Certificate) и сертификат пользователя, импортированные в файлы.

В результате администратор безопасности на своем рабочем месте не имеет доступа к контейнеру, поэтому в данном сценарии невозможно на компьютере администратора провести проверку соответствия сертификата пользователя и секретного ключа в контейнере при создании инсталляционного файла.

Шаг 2: Администратор безопасности на своем рабочем месте с помощью GUI задает локальную политику безопасности для данного пользователя, путь к локальному и CA сертификату, имя контейнера на компьютере пользователя, локальные настройки, и создает инсталляционный файл S-Terra Client.

Шаг 3: Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из:

- инсталляционного файла S-Terra Client
- утилиты `integr_mgr` для вычисления контрольной суммы
- файла с контрольной суммой инсталляционного файла S-Terra Client.

Файл с контрольной суммой должен быть передан пользователю по заслуживающему доверия каналу связи. Инсталляционный файл S-Terra Client содержит базовый инсталляционный файл, локальную политику безопасности, CA сертификат, локальный сертификат, ссылку местоположения контейнера на компьютере пользователя и персональные настройки.

5. Подготовка к инсталляции S-Terra Client

Перед установкой Продукта S-Terra Client на компьютере пользователя выполните следующие действия:

1. Установите на компьютер пользователя сертифицированное средство доверенной загрузки, если уровень защиты ПК «S-Terra Client» от НСД равен КС2.
2. Установите программный Продукт СКЗИ «КриптоПро CSP», если он еще не установлен. При выполнении процедуры инсталляции выберите:

   вид установки – *Выборочная*
   компоненты, которые необходимо установить – *Криптопровайдер уровня ядра ОС*.
3. В «КриптоПро CSP» настройте Биологический ДСЧ для уровня защиты КС1 либо для уровня защиты КС2 аппаратный ДСЧ (в случае использования сертифицированных средств доверенной загрузки «Соболь» или «Аккорд») или `КриптоПро Исходный материал` (если для ССДЗ не поддерживается функциональность ДСЧ).
4. Если пользователь будет работать с eToken, установите набор драйверов и утилит *"eToken PKI Client 5.1 SP1 для Microsoft Windows"*, который можно взять с web-страницы http://www.aladdin-rd.ru/support/download/177/, для работы с eToken PRO, eToken NG-OTP, eToken NG-FLASH, eToken PRO 72K(Java).
5. Далее необходимо создать или подключить ключевой считыватель для размещения временного контейнера с начальным значением ДСЧ, создаваемого во время инсталляции S-Terra Client:

   а) Если для пользователя создан **пользовательский токен**, на котором записан СА сертификат, локальный сертификат, политика безопасности для пользователя и контейнер с секретным ключом, то:

   - подключать **пользовательский токен** к компьютеру пользователя на время инсталляции S-Terra Client <u>не следует</u>
   - инсталлируйте ключевой считыватель Реестр. Такая инсталляция описана в «Приложении А» в разделе «Инсталляция ключевого считывателя Реестр в КриптоПро CSP».

   б) Если для аутентификации сторон будут использованы предопределенные ключи, то инсталлируйте ключевой считыватель Реестр. Такая инсталляция описана в «Приложении А» в разделе «Инсталляция ключевого считывателя Реестр в «КриптоПро CSP».
   в) Если контейнер с секретным ключом сертификата пользователя размещен в Реестре, то в Реестр будет записан и временный контейнер.
   г) Если контейнер с секретным ключом сертификата пользователя размещен на другом внешнем ключевом носителе, на него будет записан и временный контейнер:

   - подключите считыватель этого носителя, как описано в «Приложении А» в разделе «Подключение внешних ключевых считывателей» (eToken до установки драйверов подключать не следует)
   - инсталлируйте считыватель и ключевой носитель, как описано в «Приложении А» в разделе «Инсталляция внешнего считывателя и ключевого носителя в КриптоПро CSP».

   д) Если контейнер с секретным ключом пользователя находится на дискете, то дискета должна быть вставлена в дисковод.
6. На время инсталляции отключите все антивирусные программы.
7. Проверьте (если это необходимо) целостность инсталляционного файла при помощи утилиты `integr_mgr`, которая передается пользователю в составе инсталляционного пакета. Инсталляционный файл и файл с контрольной суммой этого файла должны находиться в одной папке (имя файла с контрольной суммой совпадает с именем инсталляционного файла, но имеет расширение hash):

```
integr_mgr check -f filePath
```

`filePath` имя инсталляционного файла, включая полный путь к нему, для которого будет вычисляться контрольная сумма.

При запуске утилиты вычисляется контрольная сумма заданного файла (`filePath`) и сравнивается полученное значение с контрольным значением в файле `filePath.hash`.

6. Инсталляция S-Terra Client

Установка Продукта осуществляется запуском инсталляционного файла, подготовленного и переданного администратором безопасности пользователю.

Инсталляция должна выполняться пользователем, имеющим права администратора.

После запуска файла инсталляция осуществляется в одном из 3 режимов, который был выбран администратором при подготовке инсталляционного файла:

- **режим basic** – основной режим, неинтерактивная установка с запросом на инсталляцию, вариант по умолчанию
- **режим normal** – интерактивная установка
- **режим silent** – неинтерактивная установка без запросов.

Если при подготовке инсталляционного файла администратор включил копирование контейнера с секретным ключом с одного ключевого носителя на другой, например, в Реестр, то копирование будет выполнено в процессе установки S-Terra Client. Подробное описание копирования размещено в разделе "Копирование контейнера при инсталляции".

Все протоколируемые события при инсталляции S-Terra Client будут записываться в файл, если администратор задал его при создании инсталляционного файла.

При возникновении ошибок во время инсталляции или работы Продукта устраните их и попытайтесь повторно провести инсталляцию Продукта. При появлении сбоев во время работы Продукта – перезагрузите компьютер, но если перезагрузка не устраняет проблему – обратитесь в службу поддержки по адресу mailto:support@s-terra.com.

При инсталляции S-Terra Client происходит отключение стандартного сервиса, связанного с IPsec и IKE и перевод его в состояние Manual. В Windows XP/Windows Server 2003 – это Служба IPSEC, внутреннее название которой PolicyAgent. В ОС Windows Vista и более поздних версиях – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности» (внутреннее название – IKEEXT).

В ОС Windows Vista и более поздних версиях производится настройка штатного FireWall сервиса (Брандмауэр Windows). При установке S-Terra Client в Windows FireWall добавляется новое правило:

- правило для входящих подключений
- имя – CSP VPN Service – UDP allowed (predefined)
- правило включено
- действие – разрешить подключение
- протокол – UDP (все порты)
- программа – полный путь к установленному файлу vpnsvc.exe
- службы – применятьтолько к службам
- профили – все профили
- остальные параметры – по умолчанию.

Эти настройки можно посмотреть следующим образом: `Панель управления – Администрирование – Брандмауэр Windows в режиме повышенной безопасности – Правила для входящих подключений`.

6.1 Режим basic

При установке S-Terra Client выдается окно (Рисунок 2). Необходимо разрешить доступ к компьютеру – выберите предложение *Разрешить*.

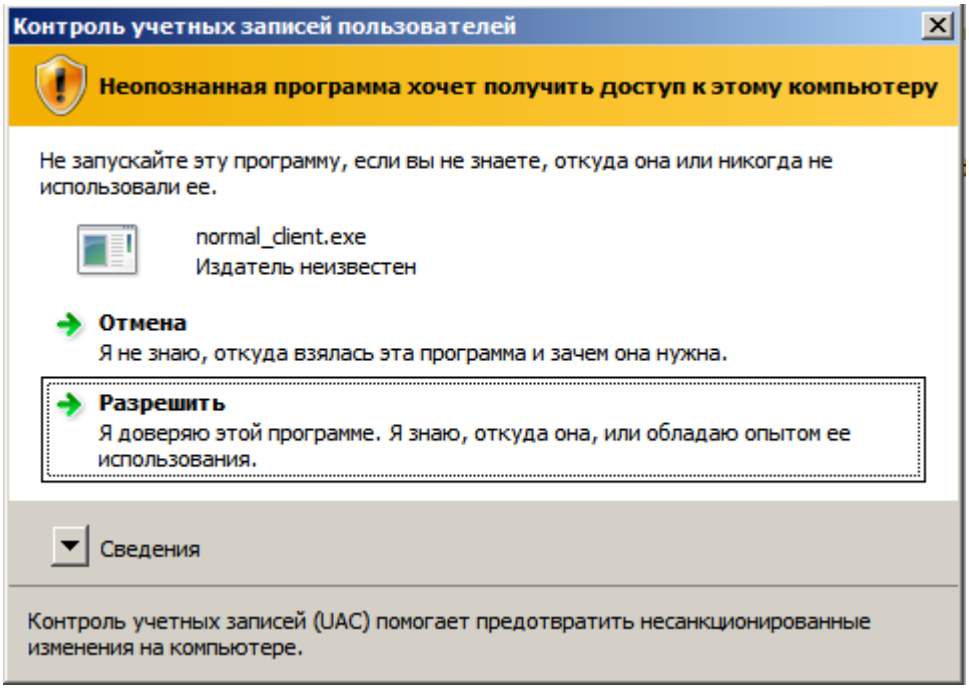


Рисунок 2

Затем выдается запрос на инсталляцию S-Terra Client (в ОС Windows XP это окно появляется первым):

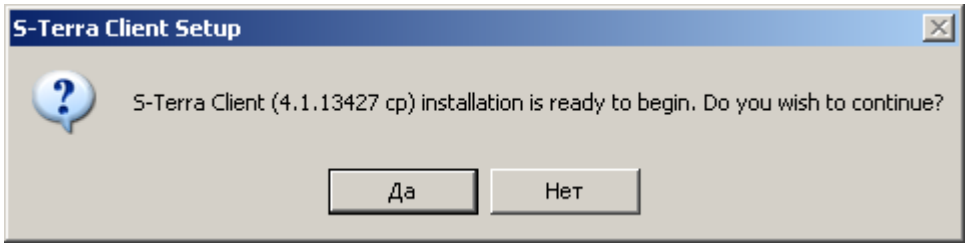


Рисунок 3

После нажатия кнопки *Да* происходит распаковка файлов (Рисунок 4):

Рисунок 4

Устанавливается продукт Microsoft Visual C++ 2008 Redistributable Package. При этом показывается окно вида (Рисунок 5):

Рисунок 5

Далее открывается стартовое окно визарда с приглашением к инсталляции и сразу следует предупреждение о необходимости отключения всех антивирусных программ на время инсталляции S-Terra Client (Рисунок 6).

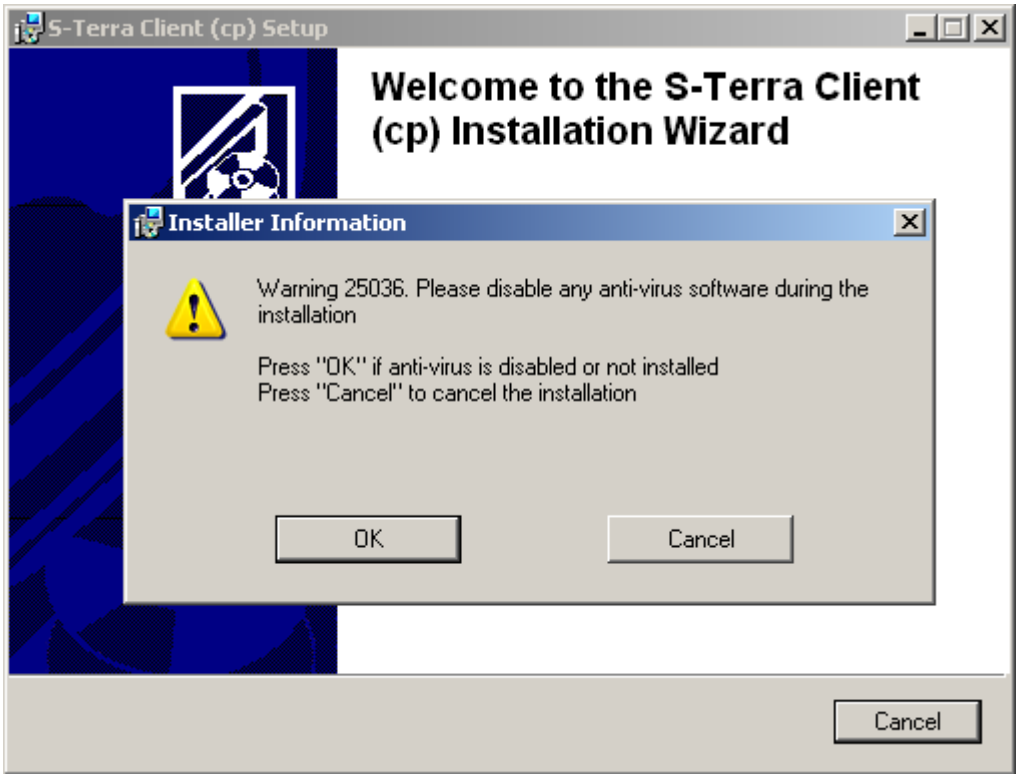


Рисунок 6

При нажатии кнопки *ОК* инсталляция будет продолжена и появится окно с индикатором процесса инсталляции:

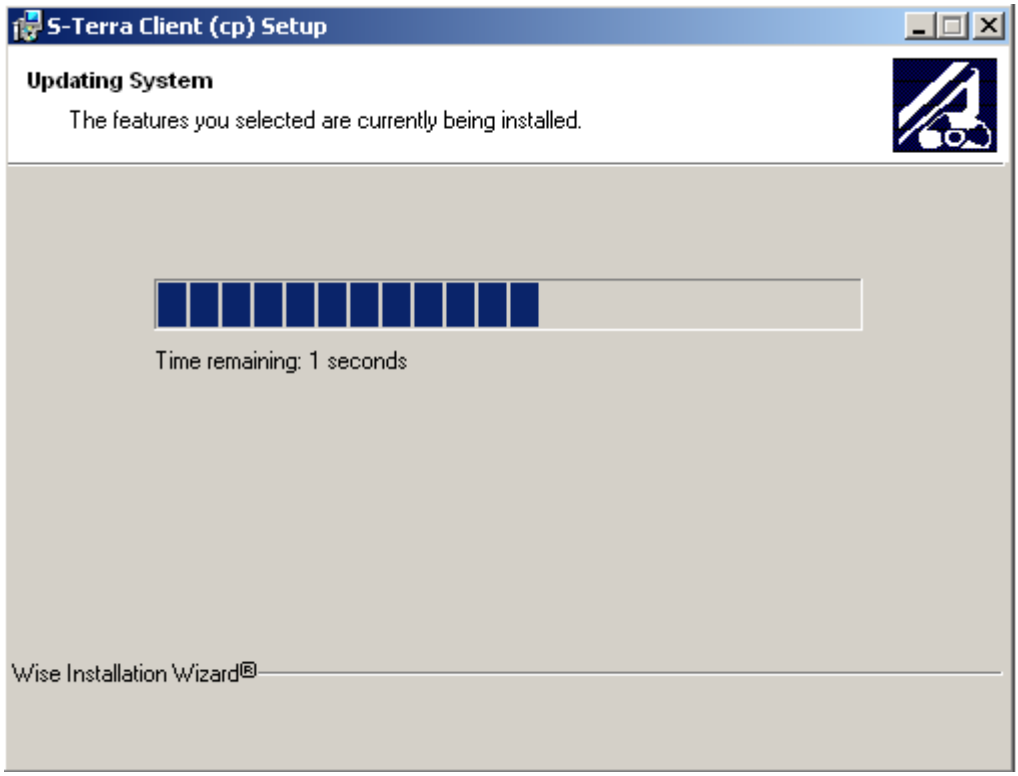


Рисунок 7

Создается контейнер, в который будет записано начальное значение ДСЧ. Если ключевой считыватель Реестр уже инсталлирован, то в него и будет записан контейнер. Если Реестр не инсталлирован, то появится окно с предложением выбрать ключевой носитель:

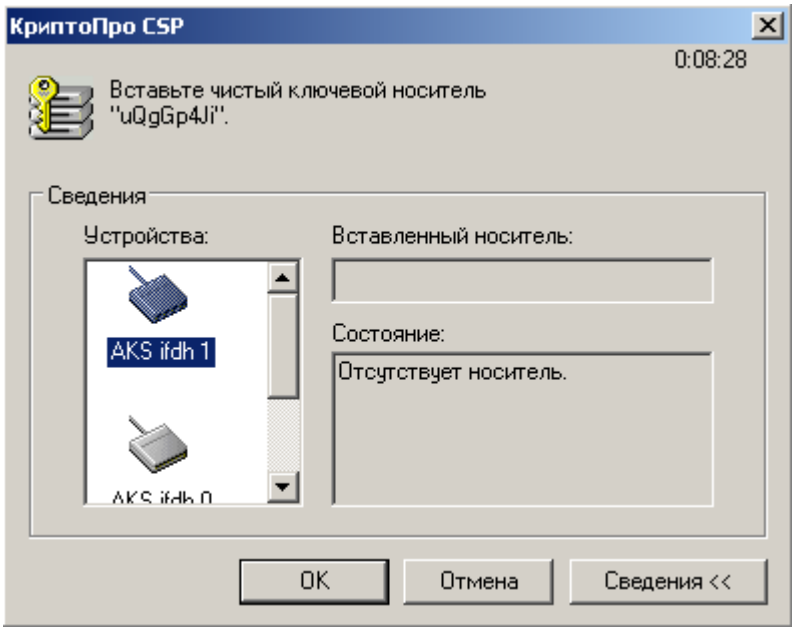


Рисунок 8

Предлагается «биологическая» инициализация ДСЧ – понажимайте клавиши или перемещайте указатель мыши. Если используется режим защиты КС2, то это окно не появится.

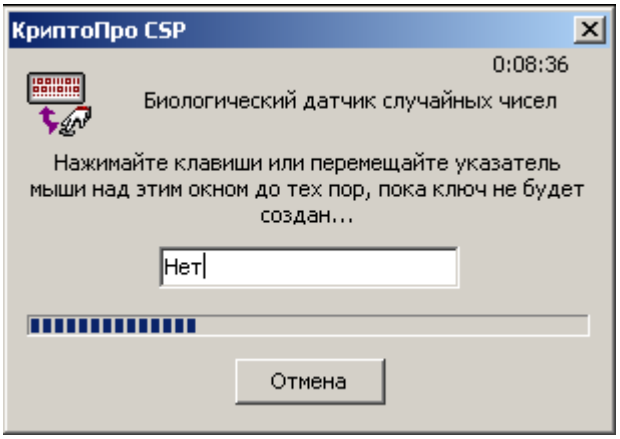


Рисунок 9

При инсталляции, при установке драйверов появляется окно (Рисунок 10). Выберите предложение – *Все равно установить этот драйвер*.

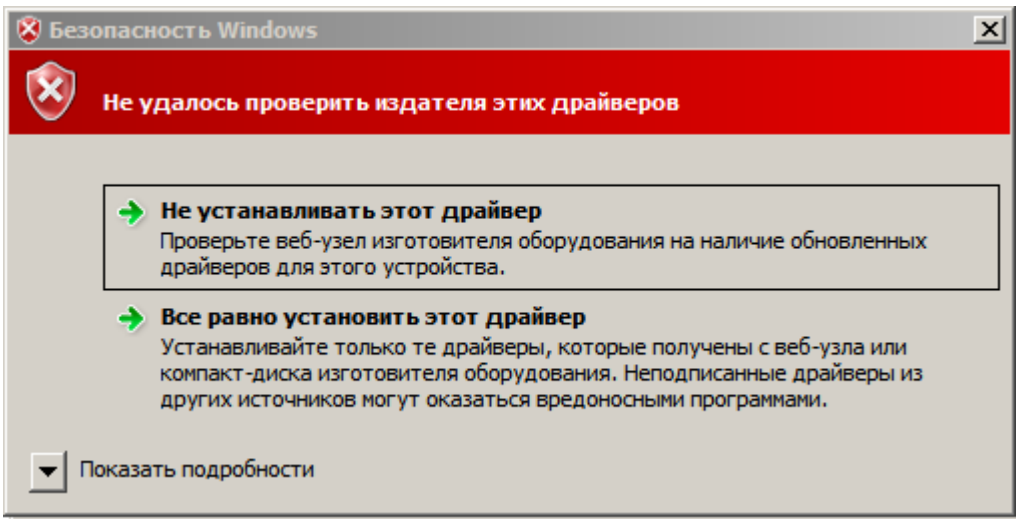
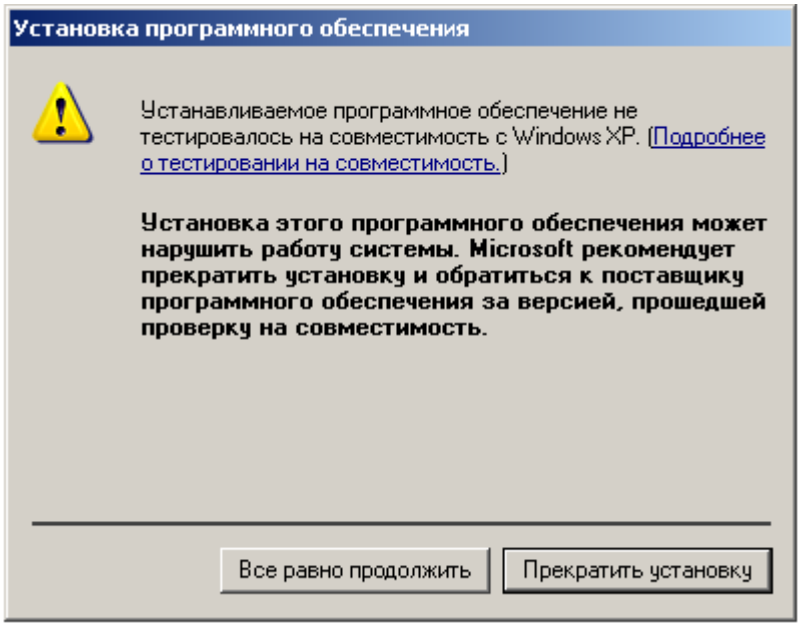


Рисунок 10

При инсталляции в ОС Windows XP и установленной реакции системы Windows на установку неподписанных драйверов в положение *Предупреждать* (`Пуск – Настройка – Панель управления – Система – Свойства системы – Оборудование – Подписывание драйверов – Предупреждать`), возможно появление окон (Рисунок 11), запрашивающих подтверждение установки программного обеспечения. Таких окон может появиться несколько. Для продолжения процесса инсталляции нажмите кнопку *Все равно продолжить* в каждом из этих окон:



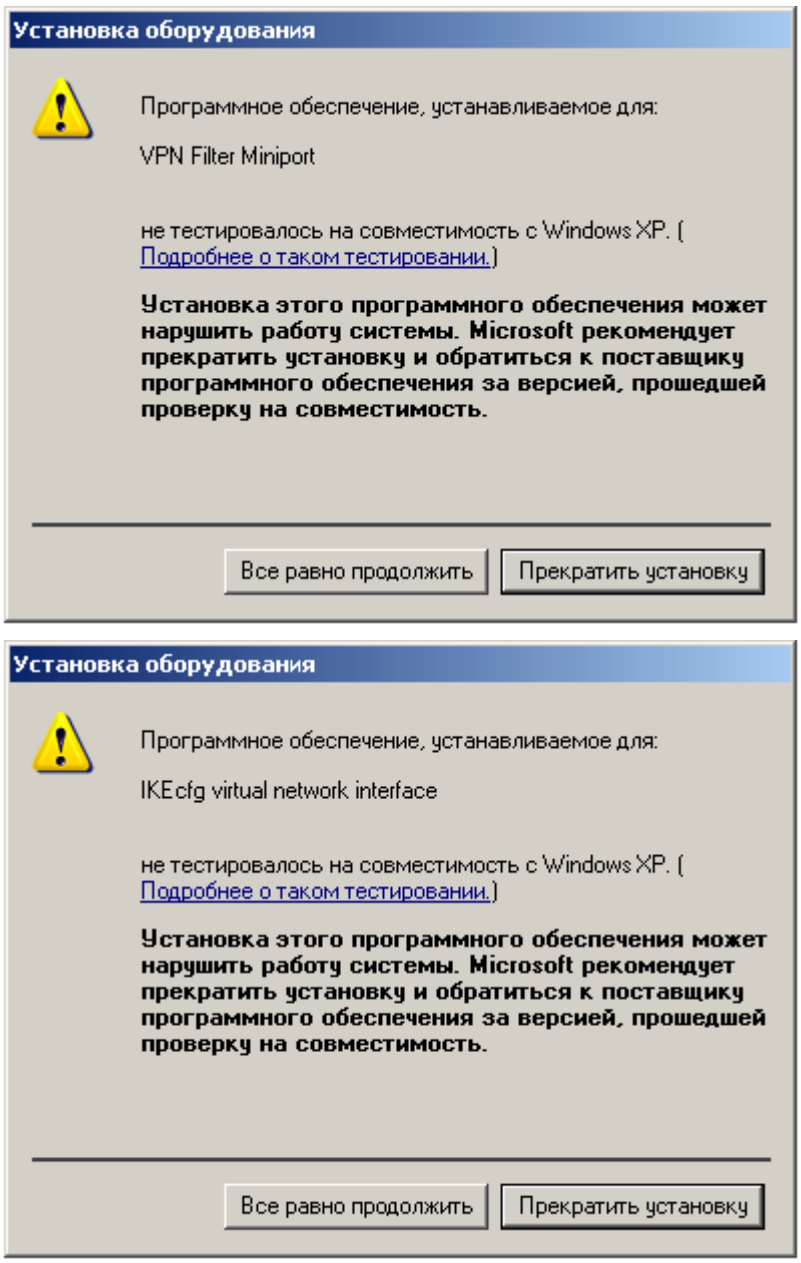


Рисунок 11

Для отключения возможности появления таких окон, установите реакцию системы Windows на установку неподписанных драйверов в положение *Пропускать* (`Пуск – Настройка – Панель управления - Система – Свойства системы- Оборудование – Подписывание драйверов – Пропускать`).

По окончании установки S-Terra Client в ОС Windows XP появляется окно (Рисунок 12) с предупреждением о необходимости перезагрузки операционной системы. После нажатия кнопки *Yes* происходит перезагрузка операционной системы, а нажатие кнопки *No* закрывает окно без перезагрузки. Для ОС Windows Vista и более поздних версий перезагрузка не требуется, но не исключено, что инсталлятор может запросить перезагрузку, если она будет необходима.

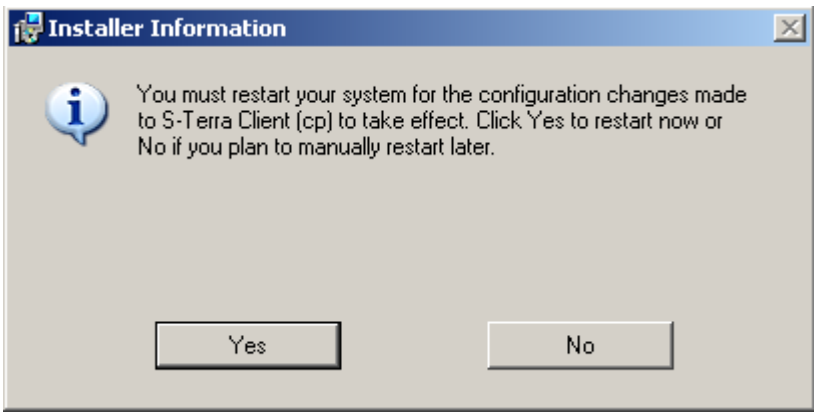


Рисунок 12

Note

Недопустимо удалять из ОС пакет Microsoft Visual C++ 2008 Redistributable Package, отсутствие которого может привести к неработоспособности Продукта S-Terra Client.

6.2 Режим normal

В ОС Windows Vista и более поздних версиях при установке S-Terra Client выдается окно (Рисунок 2) с запросом на доступ к компьютеру. Выберите предложение *Разрешить*.

Затем выдается запрос на инсталляцию S-Terra Client (в ОС Windows XP это окно появляется первым) (Рисунок 13):

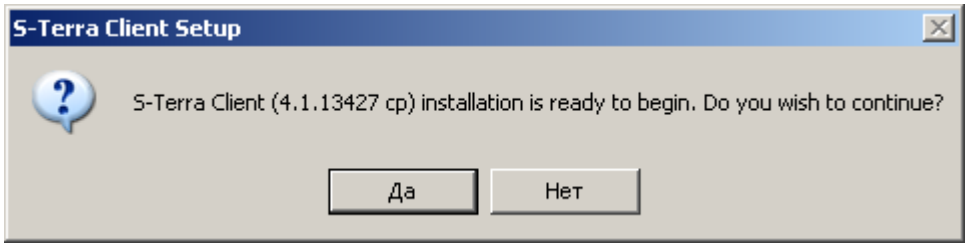


Рисунок 13

После нажатия кнопки *Да* происходит распаковка файлов (Рисунок 14).

Рисунок 14

Устанавливается продукт Microsoft Visual C++ 2008 Redistributable Package. При этом показывается окно вида (Рисунок 15):

Рисунок 15

Этот режим является диалоговым режимом. Далее открывается стартовое окно визарда с приглашением к инсталляции и сразу следует предупреждение о необходимости отключения всех антивирусных программ на время инсталляции S-Terra Client (Рисунок 16).

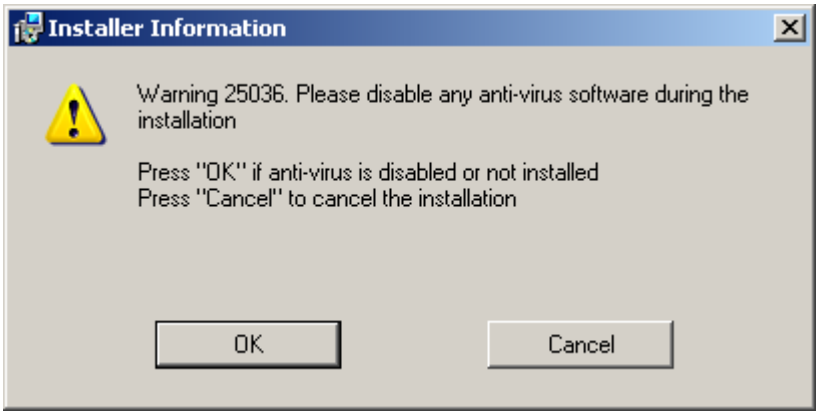


Рисунок 16

При нажатии кнопки *OK* инсталляция продолжается, в окне визарда меняются кнопки управления, нажмите кнопку *Next* (Рисунок 17).

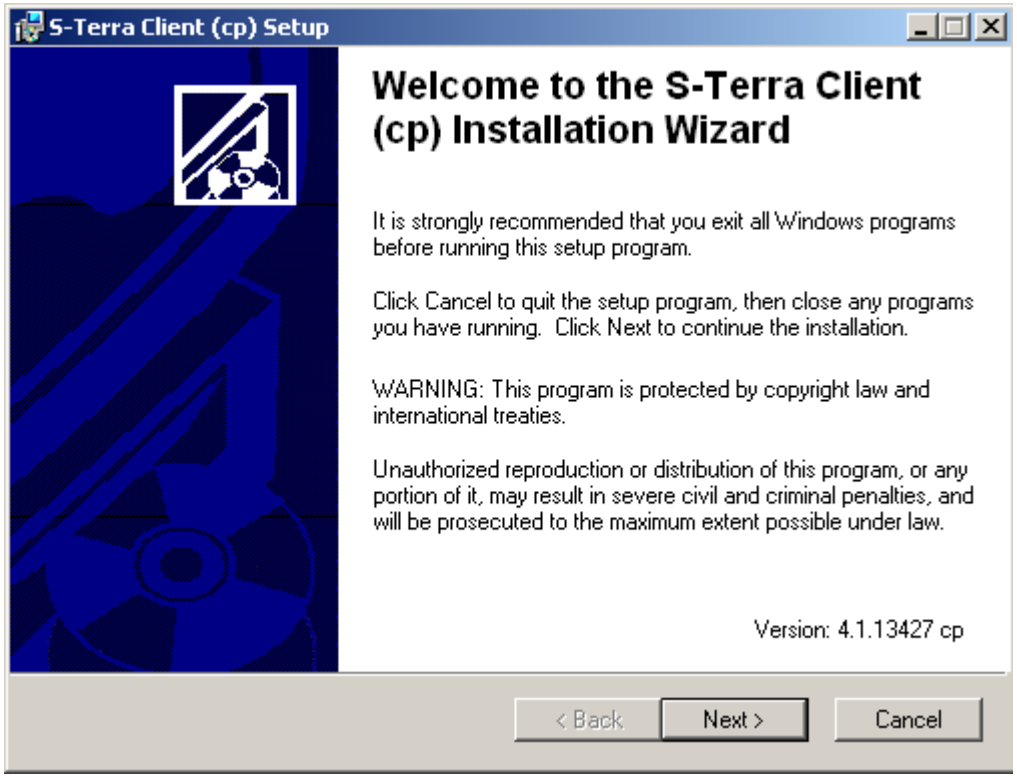


Рисунок 17

Далее открывается окно с текстом Лицензионного Соглашения. После установки переключателя в положение *"I accept the license agreement"* будет доступна кнопка *Next*:

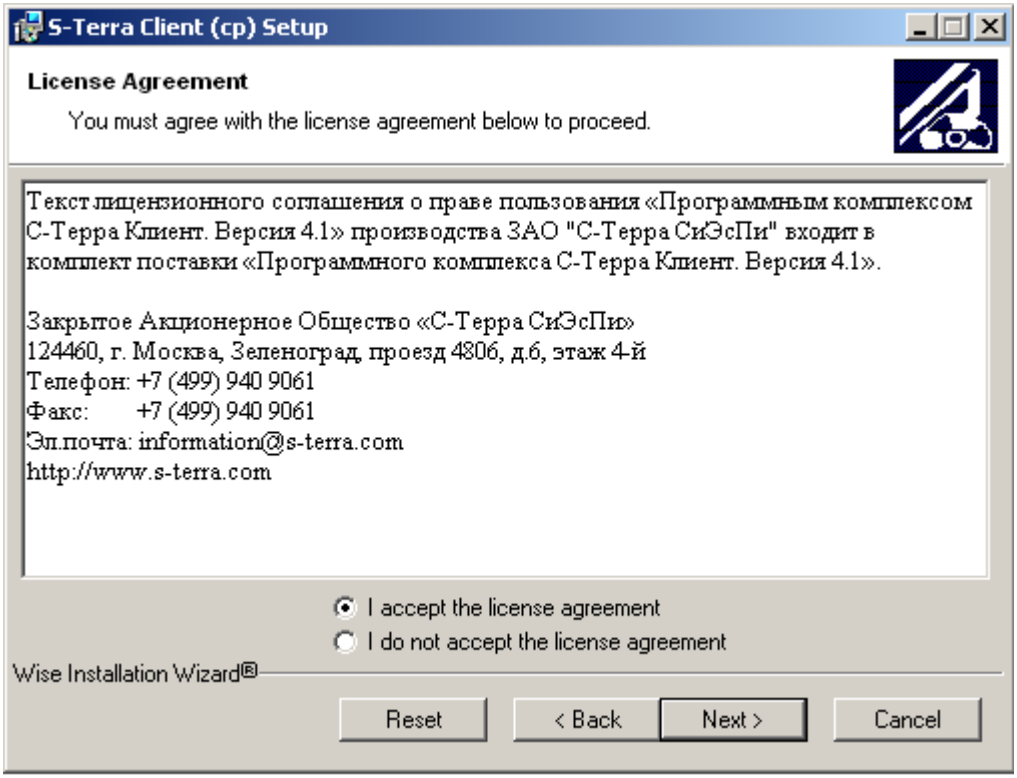


Рисунок 18

Для указания папки, в которую будет установлен Продукт, нажмите кнопку *Browse* и сделайте выбор:

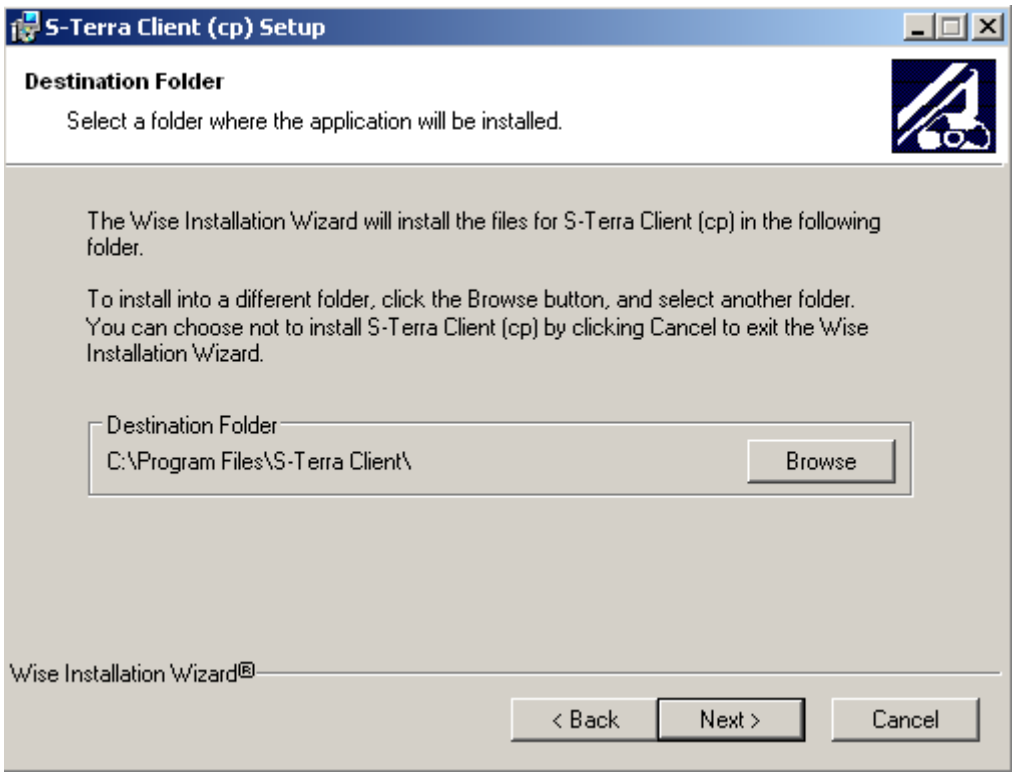


Рисунок 19

Если при создании инсталляционного файла регистрационные данные Лицензии на Продукт S-Terra Client не были включены в инсталляционный файл, то появится окно для ввода данных Лицензии на Продукт:

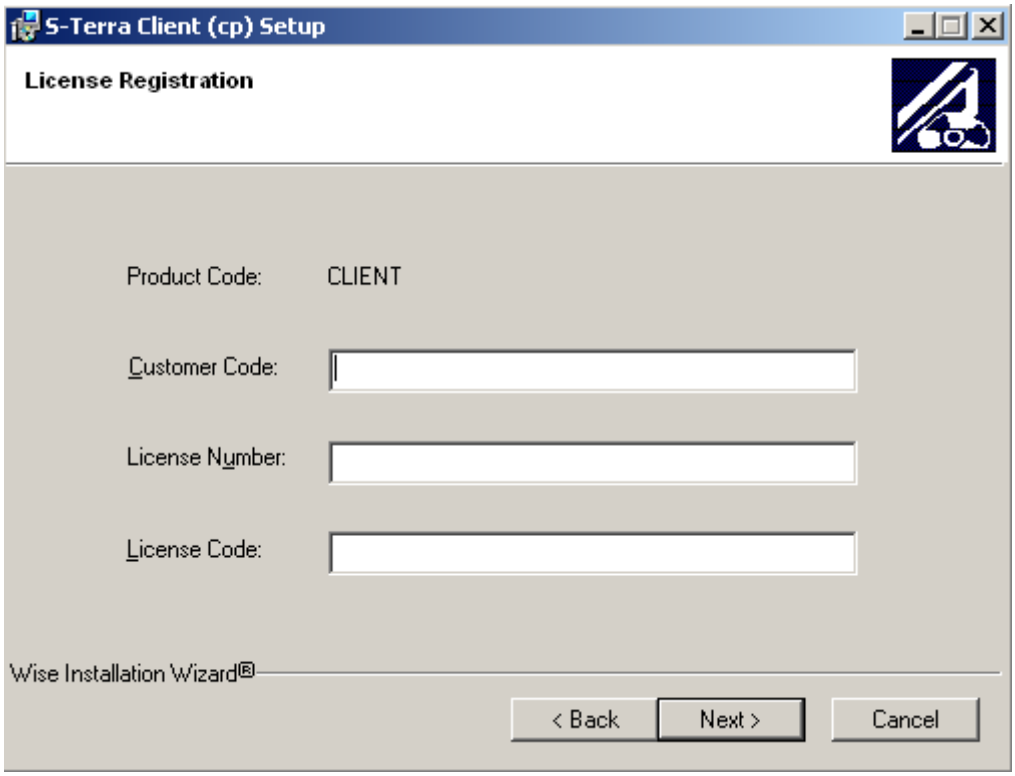


Рисунок 20

Стандартное окно визарда сообщает о готовности к инсталляции. Для начала инсталляции нажмите *Next*:

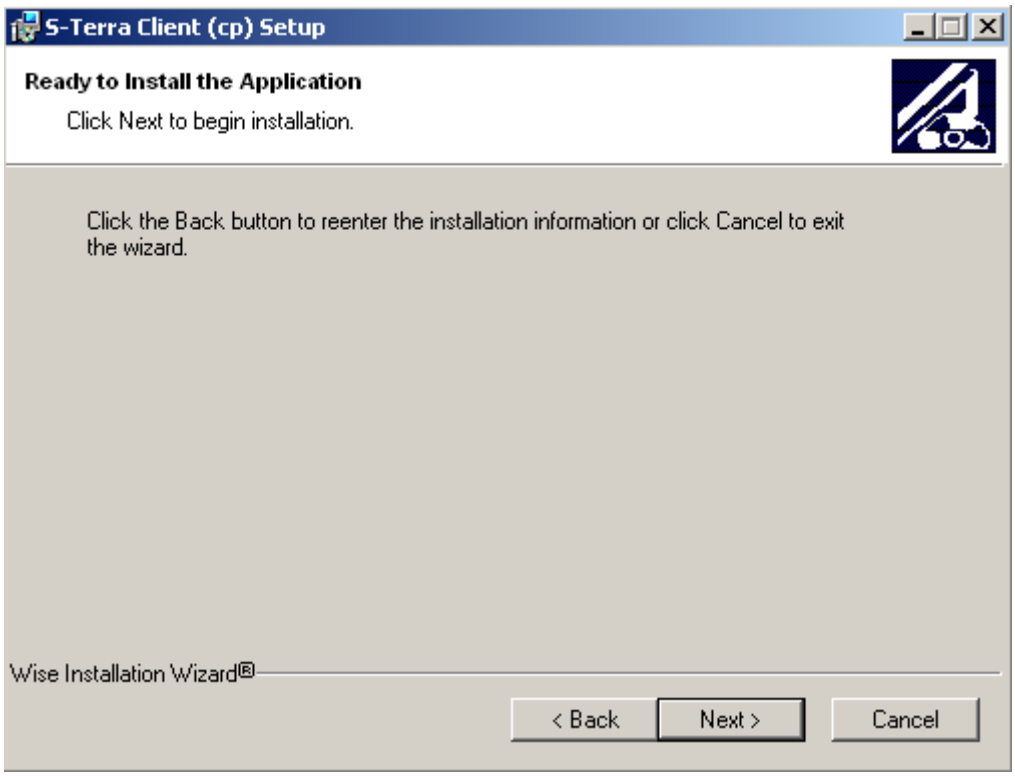


Рисунок 21

Далее появляется окно с индикатором процесса инсталляции:

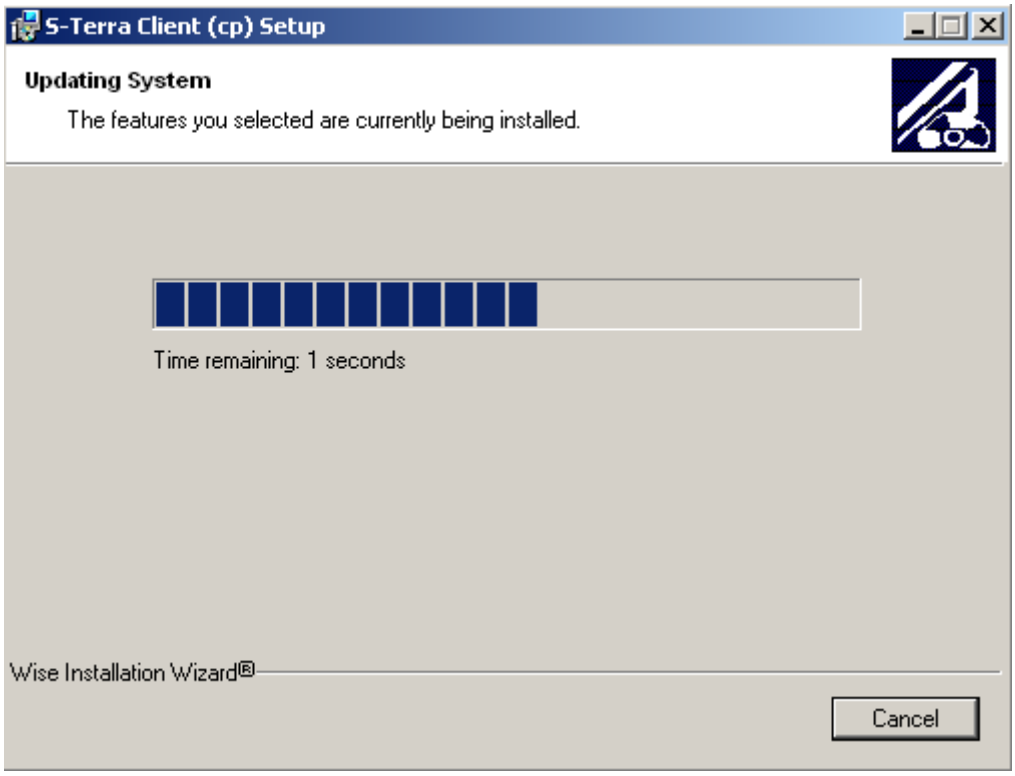


Рисунок 22

Создается контейнер, в который будет записано начальное значение ДСЧ. Если ключевой считыватель Реестр уже инсталлирован, то в него и будет записан контейнер. Если Реестр не инсталлирован, то появится окно с предложением выбрать ключевой носитель (Рисунок 23):

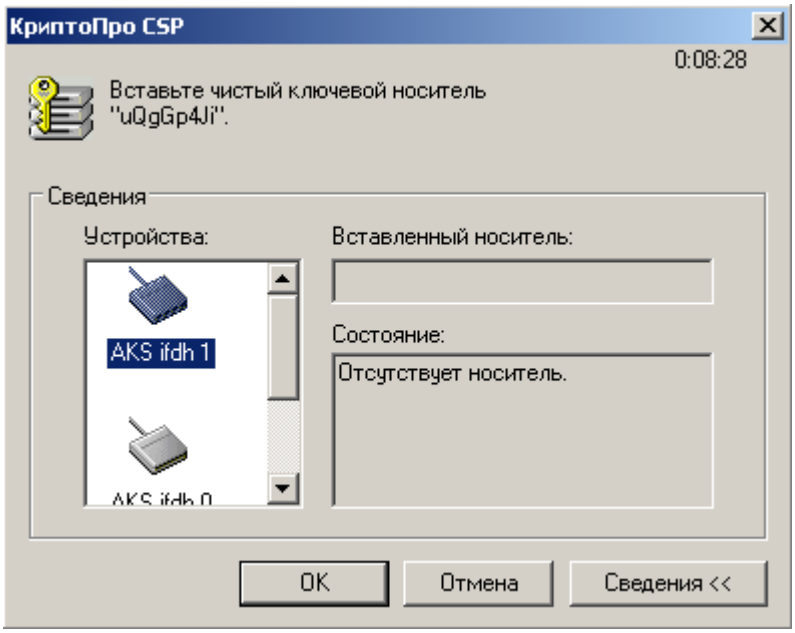


Рисунок 23

Предлагается «биологическая» инициализация ДСЧ – понажимайте клавиши или перемещайте указатель мыши (Рисунок 24). Если используется режим защиты КС2, то это окно не появится.

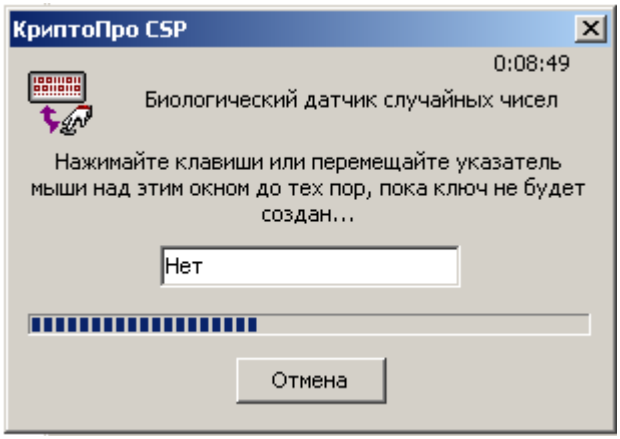


Рисунок 24

Дальнейшее поведение инсталлятора зависит от ОС и установленной пользователем опции Подписывание драйверов, описанной в разделе "Режим basic".

После завершения процедуры инсталляции нажмите *Finish*:

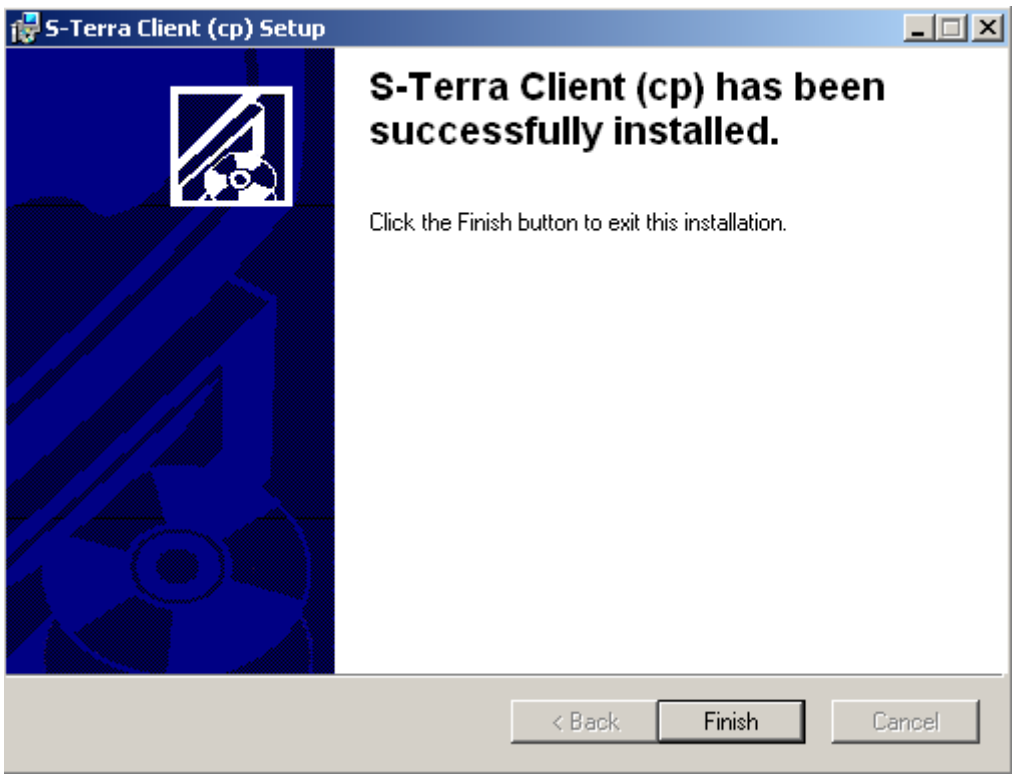


Рисунок 25

По окончании установки S-Terra Client в ОС Windows XP появляется окно (Рисунок 26) с предупреждением о необходимости перезагрузки операционной системы. После нажатия кнопки *Yes* происходит перезагрузка операционной системы, а нажатие кнопки *No* закрывает окно без перезагрузки. Для ОС Windows Vista и более поздних версий перезагрузка не требуется, но не исключено, что инсталлятор может запросить перезагрузку, если она будет необходима.

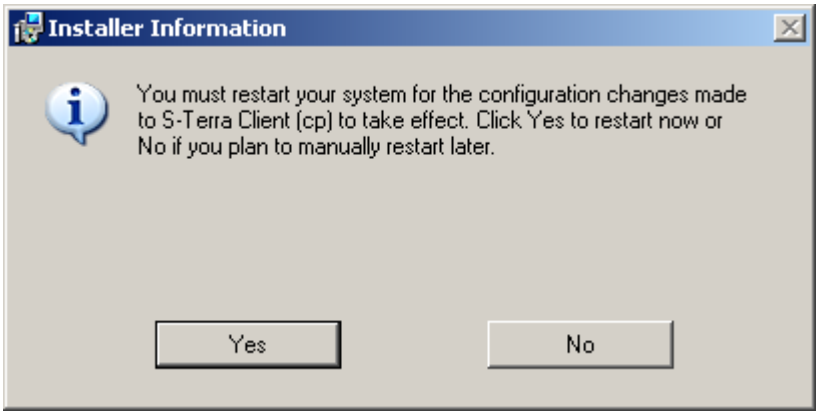


Рисунок 26

Note

Недопустимо удалять из ОС пакет Microsoft Visual C++ 2008 Redistributable Package, отсутствие которого может привести к неработоспособности Продукта S-Terra Client.

6.3 Режим silent

В режиме silent происходит установка S-Terra Client без запросов, но могут появляться либо системные диалоговые окна, либо некоторые интерактивные компоненты, относящиеся к криптоподсистеме.

В ОС Windows Vista и более поздних версиях при установке S-Terra Client выдается окно (Рисунок 2) с запросом на доступ к компьютеру. Выберите предложение *Разрешить*.

Далее выполняется распаковка файлов (Рисунок 27).

Рисунок 27

Устанавливается продукт Microsoft Visual C++ 2008 Redistributable Package (Рисунок 28).

Рисунок 28

Создается контейнер, в который будет записано начальное значение ДСЧ. Если ключевой считыватель Реестр уже инсталлирован, то в него и будет записан контейнер. Если Реестр не инсталлирован, появится окно с предложением выбрать ключевой носитель (Рисунок 29):

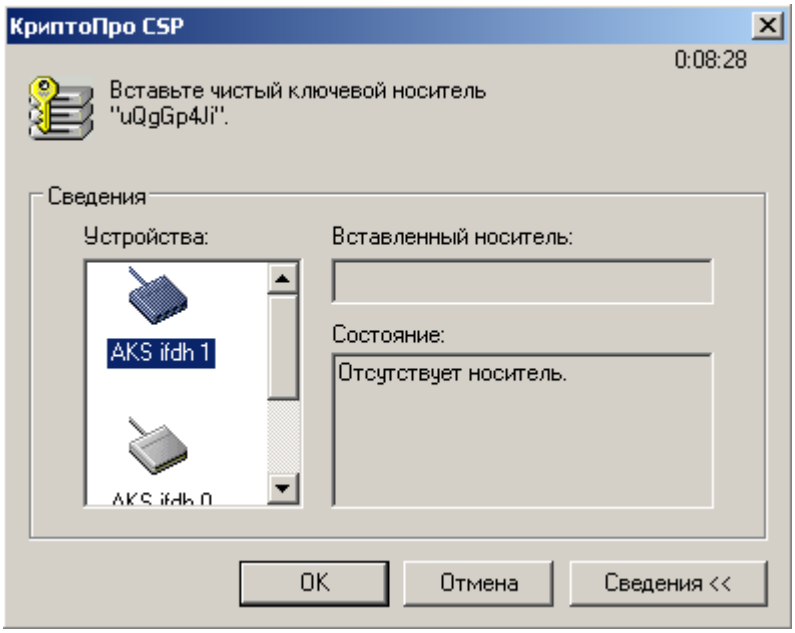


Рисунок 29

Предлагается «биологическая» инициализация ДСЧ – понажимайте клавиши или перемещайте указатель мыши. Если используется режим защиты КС2, то это окно не появится.

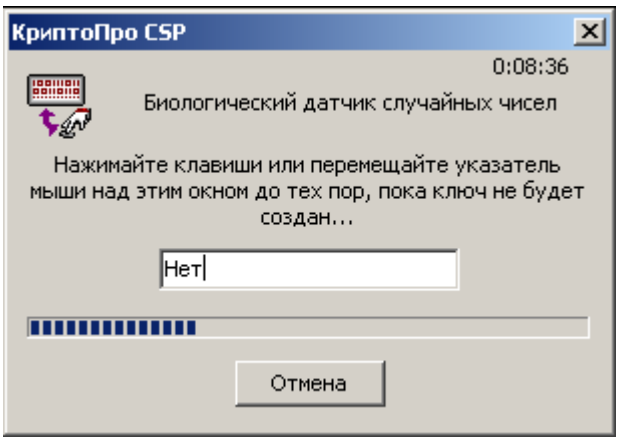


Рисунок 30

Дальнейшее поведение инсталлятора зависит от ОС и установленной пользователем опции `Подписывание драйверов`, описанной в разделе "Режим basic".

По окончании установки S-Terra Client в ОС Windows XP происходит перезагрузка операционной системы без предупреждений. Для ОС Windows Vista и более поздних версий перезагрузка не требуется, но не исключено, что инсталлятор может запустить перезагрузку, если она будет необходима.

В случае возникновения ошибок и прерывания инсталляции никакие сообщения на экран не выводятся. Эти сообщения можно посмотреть программой ОС Windows «Просмотр событий» или, если при подготовке инсталляционного пакета администратором была указана опция протоколирования событий при инсталляции в файл, то сообщения можно посмотреть в заданном файле.

Примечание: если при инсталляции будет обнаружена база локальных настроек, оставшаяся от предыдущей установки продукта, то по умолчанию происходит обновление базы локальных настроек кроме тех, которые отсутствуют при новой инсталляции. В некоторых ситуациях это может привести к неработоспособности или некорректной работе продукта (в этом случае рекомендовалось при подготовке инсталляционного файла использовать дополнительный параметр для WinInstaller AGENT_DB_REMOVE=1).

Недопустимо удалять из ОС пакет Microsoft Visual C++ 2008 Redistributable Package, отсутствие которого может привести к неработоспособности Продукта S-Terra Client.

6.4 Копирование контейнера при инсталляции

Если при подготовке инсталляционного файла с использованием сертификатов было задано копирование контейнера, то такое копирование осуществляется при инсталляции S-Terra Client. В случае, если копирование происходит в контейнер с именем, который уже существует, то выдается окно следующего вида:

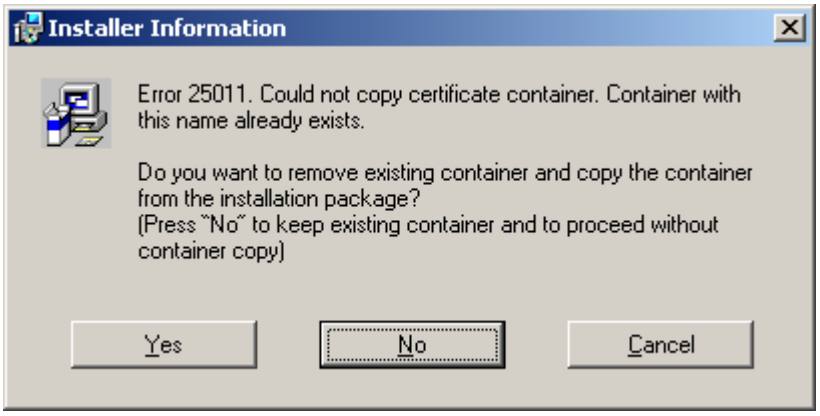


Рисунок 31

Если нажать *Yes*, то существующий контейнер будет удален и процедура копирования будет продолжена. Если нажать *No*, существующий контейнер останется, а процедура копирования будет отменена. Если нажать *Cancel*, то инсталляция клиента будет прервана.

Опишем последовательность действий при копировании контейнера с внешнего ключевого носителя, например, дискеты, в Реестр так, как она выглядит для пользователя.

В первом окне (Рисунок 32) предлагается установить внешний ключевой носитель в устройство считывания, с которого будет выполняться копирование контейнера, например, дискету. Это окно не появляется, если ключевой носитель уже установлен (например, дискета вставлена в дисковод):

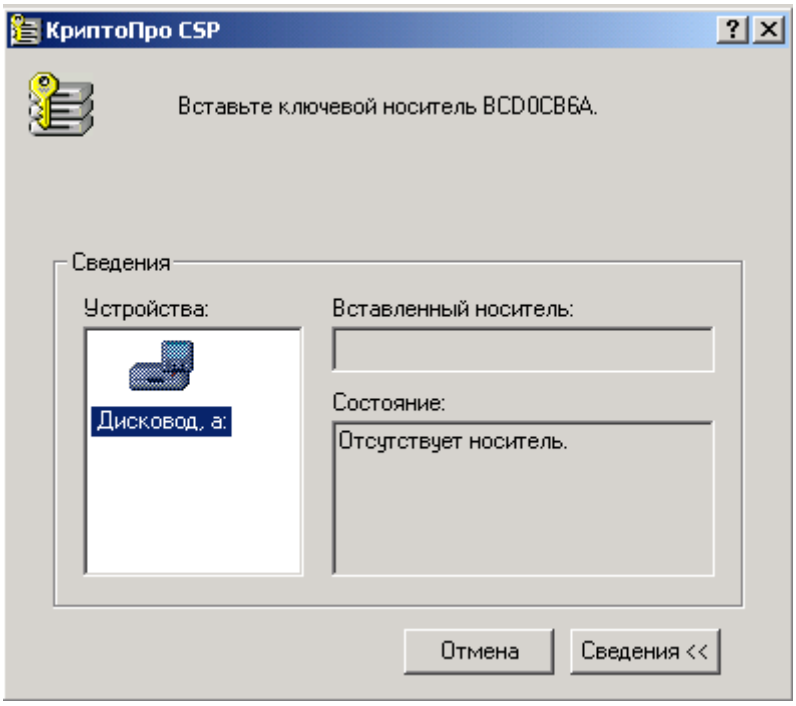


Рисунок 32

Далее отображается работа утилиты копирования (Рисунок 33):

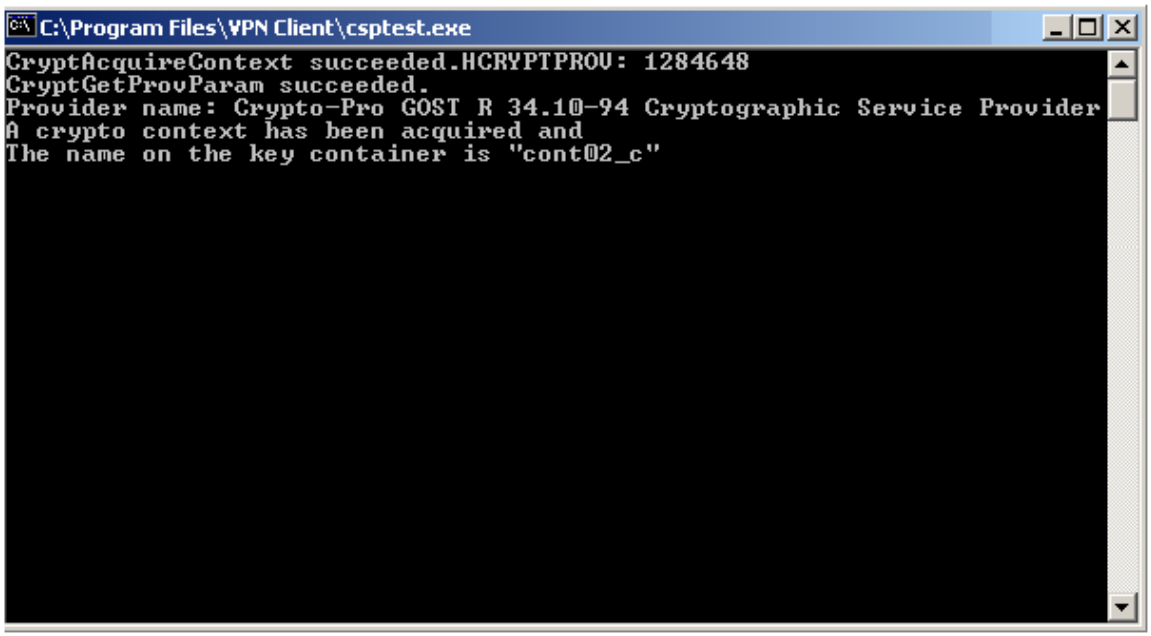


Рисунок 33

Если исходный контейнер защищен паролем, а при подготовке инсталляционного файла он не был задан, то появляется окно для ввода пароля (Рисунок 34):

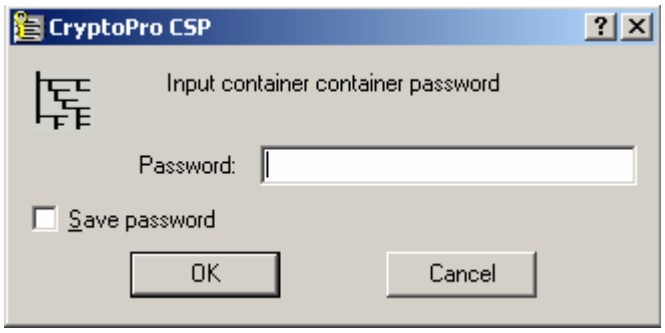


Рисунок 34

В окне с запросом пароля для нового контейнера надо ввести пароль, который обязательно должен совпадать с указанным паролем при подготовке инсталляционного файла. Если используется пустой пароль – достаточно нажать *OK* (Рисунок 35):

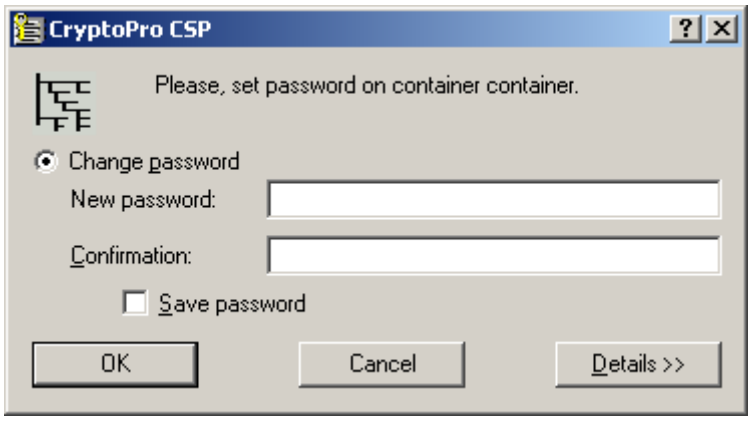


Рисунок 35

Если при копировании контейнера возникли ошибки, то в текстовом окне появляется сообщение об ошибке и предложение нажать на *Enter* (Рисунок 36):

```
C:\Program Files\VPN Client>yset -container container -copy container -passwd 1
CryptAcquireContext succeeded.HCRYPTPROV: 1285384
CryptGetProvParam succeeded.
Provider name: Crypto-Pro GOST R 34.10-94 Cryptographic Service Provider
A crypto context has been acquired and
The name on the key container is "container"

A signature key is available. HCRYPTKEY: 1291048

An exchange key exists. HCRYPTKEY: 1296912
An error occurred in running the program.
./ctkey.c:1658:Error during CryptAcquireContext.

Error number 8009000f (-2146893809).
Object already exists.
Program terminating.
Press Enter to exit.
```

Рисунок 36

Инсталляция после этого завершится с сообщением об ошибке: "`Copy certificate container failed. Installation aborted.`"

Если копирование прошло без ошибок, текстовое окно просто закрывается. Инсталляция Продукта продолжается.

Примечание: если инсталляции происходит в режиме `silent`, и на компьютере пользователя уже существует контейнер с указанным именем, в который происходит копирование, то инсталляция прерывается без выдачи на экран каких-либо запросов пользователю.

6.5 Сообщения об ошибках при инсталляции

Ниже приведены тексты сообщений об ошибках, которые могут появиться при инсталляции S-Terra Client.

Таблица 1

	Текст сообщения	Примечание
1330	A file that is required cannot be installed because the cabinet file <file> has an invalid digital signature. This may indicate that the cabinet file is corrupt	Перед установкой Продукта должны быть установлены сертификаты от VeriSign, выпущенные не позднее 10.10.10, которые удостоверяют сертификат JSC S-Terra CSP, который в свою очередь подписывает драйвера, MSI и CAB. С сайта microsoft.com получите обновление "Update for Root Certificates" (ключевое слово – KB931125).
25001	License check failed.	Неправильная лицензия
25002	CryptoPro must be installed before the product installation.	Перед установкой Продукта должно быть установлено CryptoPro
25004	Delete existing product settings?	Удалить существующие настройки продукта? (вопрос при деинсталляции)
25005	Old product settings found. Delete existing product settings?	Найдены старые настройки продукта. Удалить существующие настройки продукта?
25006	RNG initialization failed. {Reason: <reason>.} Installation aborted. {RNG container path: <path>}, где <reason> может быть одним из следующих: Random initialization tool returned an error You must have Administrator privileges Random initialization tool not found Random initialization tool can't run: system error Random value initialization failed Container name generation limit exceeded	Не удалось создать RNG контейнер. {Причина: <reason>} Инсталляция прервана. Путь к RNG контейнеру: <path> основные <reason>: Утилита для инициализации ДСЧ вернула ошибку Вы должны иметь администраторские привилегии Утилита для инициализации ДСЧ не найдена Не удалось запустить утилиту для инициализации ДСЧ: системная ошибка Инициализация ДСЧ не произошла Исчерпан лимит генерируемых имен контейнера
25009	Copy certificate container failed. {Reason: <reason>.} Installation aborted. Source container path: <src>. Destination container path: <dst>.	Не удалось скопировать сертификатный контейнер. {Причина: <reason>} Инсталляция прервана. Путь к исходному контейнеру: <src>. Путь к новому контейнеру: <dst>.
25011	Could not copy certificate container. Container with this name already exists. Do you want to remove existing container	Нельзя скопировать сертификатный контейнер, поскольку контейнер с таким

	Текст сообщения	Примечание
	and copy the container from the installation package? (Press “No” to keep existing container and to proceed without container copy)	именем уже есть. Хотите ли вы удалить существующий контейнер и скопировать контейнер из инсталляционного пакета? (Нажмите “No” для того, чтобы сохранить существующий контейнер и продолжить без копирования)
25016	Version {<Version> } of CryptoPro CSP is not supported. CryptoPro CSP version 3.6 must be installed before the product installation	Версия <Version> продукта КриптоПро CSP не поддерживается. Должно быть установлено КриптоПро CSP версии 3.6 до инсталляции продукта. Примечания: <Version> в сообщении может отсутствовать, если ее не удалось определить Для версии 3.6 с build меньше, чем 5402, к <Version> добавляется приписка “(beta)” К <Version> добавляется приписка “(unrecognized)”, если по каким-либо причинам не удалось определить build КриптоПро CSP.
25018	Product "<Product_name version>" was detected. You should uninstall it first before the installation.	Был обнаружен Продукт "<Product_name version>". Вам необходимо сначала деинсталлировать его.
	This product needs Windows 2000 or higher	Для Продукта необходима Windows 2000 или выше
25019	The "<dll_path>" was wrongly marked as the previous GINA DLL. The system GINA DLL will be used instead.	[Windows XP] Файл <dll_path> был ошибочно помечен, как предыдущая GINA DLL. Будет использована системная GINA DLL.
25020	The previous GINA DLL "<dll_path>" was not found. The system GINA DLL will be used instead.	[Windows XP] Предыдущая GINA DLL <dll_path> не найдена. Будет использована системная GINA DLL.
25021	Driver "<driver_name>" installation failed. Product installation aborted.	Не удалось установить драйвер <driver_name>. Инсталляция продукта прервана.
25022	Product "<Product_name version>" was advertised. You should uninstall it first before the installation.	Для продукта <Product_name version> была выполнена операция объявления пользователям (advertisement). Вы должны деинсталлировать его до инсталляции.
25023	There is no CryptoPro CSP driver library installed on the system. You should install it first before the installation. Product installation aborted.	Не установлена драйверная библиотека КриптоПро CSP. Вы должны инсталлиро вать ее до инсталляции продукта. Инсталляция продукта прервана.

	Текст сообщения	Примечание
25025	Failed to add Windows Firewall rule allowing network traffic for S-Terra VPN Service. If you intend to use Windows Firewall or other firewall, you should manually configure it to allow network traffic for S-Terra VPN Service.	Не удалось добавить правило Брандмауэра Windows открывающее сетевой трафик для VPN сервиса. Если Вы собираетесь использовать Брандмауэр Windows или другой firewall, вы должны настроить его вручную, чтобы пропустить сетевой трафик для VPN сервиса. Рекомендации по ручной настройке Брандмауэра Windows даны в разделе «Рекомендации по ручной настройке Брандмауэра Windows».
25026	You must have administrator privileges.	Вам необходимы администраторские привилегии.
25032	Version {<Version> } of CryptoPro CSP is not supported one. It could be incompatible with the product. Do you want to continue the installation?	Версия КриптоПро CSP официально не поддерживается продуктом. Она может быть несовместима с продуктом. Продолжить инсталляцию?
25033	The Visual C++ Redistributable Package is absent or damaged	Visual C++ Redistributable Package отсутствует или поврежден
25034	RNG initialization was canceled. Do you want to retry RNG initialization (press "No" to cancel the installation)?	Инициализация RNG была прервана пользователем. Вы хотите повторить инициализацию RNG (нажмите "No" для прерывания инсталляции)?
25035	Token Software must be installed before the product installation.	Программное обеспечение для поддержки токенов должно быть установлено до установки продукта. Примечание: сообщение появляется только если дополнительный параметр инсталляции TOKEN_LOGIN равен 1.
25036	Please disable any anti-virus software during the installation Press "OK" if anti-virus is disabled or not installed Press "Cancel" to cancel the installation	Пожалуйста, отключите любую антивирусную программу на время инсталляции Нажмите "OK" если антивирус отключен или не установлен Нажмите "Cancel" для отмены инсталляции Примечание: появление данного сообщения может быть отключено, если установить параметр инсталляции DISABLE_ANTIVIRUS_WARNING=1

7. Дополнительные настройки

7.1 Обеспечение работоспособности VPN сервиса

Для обеспечения работоспособности VPN сервиса необходимо:

отключить службу «Брандмауэр Windows/Общий доступ к Интернету (ICS)» для ОС Windows XP и Windows Server 2003 или, для более поздних версий Windows, отключить службу «Общий доступ к подключению к Интернету (ICS)»

либо

в свойствах интерфейса, участвующего в построении защищенного соединения, во вкладке «Доступ» сбросить флажок «Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера».

7.2 Настройка переменных окружения

Имеется возможность настроить некоторые переменные окружения, которые могут повлиять на работу S-Terra Client или дать возможность получить дополнительную информацию в лог-файле.

Чтобы присвоить значение переменным окружения войдите в `Панель Управления -> Система -> Дополнительно(Дополнительные параметры системы) -> Переменные среды`.
В окне `Переменные среды` перейдите в область `Системные переменные` и нажмите кнопку `Создать`.
Введите `Имя переменной` и `Значение переменной`.
Перезагрузите компьютер.

Описание переменных окружения

CSP_SYS_RESPONSE_TIMEOUT	задает максимальное время (в секундах), на которое vpn-демон может "подвиснуть" перед тем как аварийно закончить свою работу. "Подвисание" – состояние, когда ни одна из рабочих нитей не может взяться за выполнение задания. По достижении указанного времени vpn-демон сам аварийно завершает свою работу и создает core-файл. Механизм слежения за зависанием vpn-демона позволяет завершить работу неработоспособного демона и запустить новую сессию, тем самым повысив отказоустойчивость системы. Если CSP_SYS_RESPONSE_TIMEOUT = 0, то механизм слежения за зависанием vpn-демона не включается.

Переменные окружения CSP_LOG_TASK_TIME и CSP_LOG_TASK_QUEUE_PERIOD используются службой поддержки для диагностики различных ситуаций. Обе переменные задают время, по истечении которого в файл лога выдаются сообщения. CSP_LOG_TASK_QUEUE_PERIOD выдает сообщения уровня `info`, CSP_LOG_TASK_TIME выдает сообщения уровня `warning`.

CSP_LOG_TASK_TIME	задает время (в секундах), которое должно быть затрачено на выполнение одной задачи. При превышении заданного времени в файл лога будет

	выдаваться сообщение о большем затраченном времени на выполнение одной задачи: `Event Manager profiler: task time is <n> sec (src=<hex> dst=<hex> idx=<n> proc=<hex>)` Если CSP_LOG_TASK_TIME = 0, то сообщение в файл лога не выводится.
CSP_LOG_TASK_QUEUE_PERIOD	задает период (в секундах), с которым в файл лога будут выдаваться сообщения о времени ожидания задачи в очереди и длине очереди задач. Сообщения выводятся следующего вида: `Event Manager profiler: waiting time of task queue is <n> sec, queue length is <n> tasks` Если CSP_LOG_TASK_QUEUE_PERIOD = 0, то сообщения в файл лога не выводятся.

7.3 Рекомендации по ручной настройке Брандмауэра Windows

Данные рекомендации описывают ручную настройку Брандмауэра Windows для обеспечения работоспособности VPN сервиса.

Обычно действия, описываемые в данном разделе, выполняются автоматически инсталлятором. Но если на момент инсталляции служба Брандмауэра Windows была отключена, никаких действий с Брандмауэром Windows на этапе инсталляции не производится. Это может привести к частичной неработоспособности Продукта после запуска службы Брандмауэра Windows. В данной ситуации пользователь уведомляется предупреждением инсталлятора 25025.

Если вместо Брандмауэра Windows используется другой персональный firewall, в нем следует вручную внести настройки, аналогичные описываемым в этом разделе.

Ниже рассмотрим рекомендуемые настройки Брандмауэра Windows для некоторых ОС Windows.

Ручная настройка Брандмауэр Windows на Windows XP

Войдите в *Панель управления -> Брандмауэр Windows*.

Перейдите во вкладку *Исключения* и нажмите кнопку *Добавить программу..*

В появившемся окне *Добавление программы* в поле *Путь* задайте полный путь к файлу vpnsvc.exe, который располагается в каталоге продукта (по умолчанию – C:\Program Files\S-Terra Client).

Нажмите кнопку *Изменить область...* и убедитесь, что выбрано *Любой компьютер (включая из Интернета)*. По умолчанию выставляется именно такая настройка.

Подтвердите настройку, нажав *OK*.

Ручная настройка Брандмауэр Windows на Windows Vista

Войдите в *Панель управления -> Система и ее обслуживание –> Администрирование -> Брандмауэр Windows в режиме повышенной безопасности*.

Для *Правила для входящих подключений* выберите *Действия –> Новое правило*...

Укажите *Тип правила – Настраиваемые*.

Для раздела *Программа* укажите:

Путь программы (задайте полный путь к файлу vpnsvc.exe, который располагается в каталоге продукта (по умолчанию – C:\Program Files\S-Terra Client).

Службы -> Настроить -> Применять только к службам.

Для раздела *Тип протокола* выберите – *UDP. Все порты*.

Затем в разделе *Область* укажите – *Любой IP-адрес*

В разделе *Действие – Разрешить подключение*.

В разделе *Профиль* – все (*Домен, Личный, Общий*).

В разделе *Имя – S-Terra VPN Service*.

Нажмите – *Готово*.

Ручная настройка Брандмауэр Windows на Windows 7

Войдите в *Панель управления -> Система и безопасность -> Брандмауэр Windows*.

Выберите раздел *Дополнительные параметры*.

Должно появиться окно *Брандмауэр Windows в режиме повышенной безопасности*.

Выберите – *Правила для входящих подключений и Действие – Создать правило...*

Выполните шаги:

Тип правила – Настраиваемые.

Программа:

- *Путь программы*. (задайте, нажав кнопку *Обзор...* полный путь к файлу vpnsvc.exe (располагается в каталоге продукта, по умолчанию – C:\Program Files\S-Terra Client).
- *Службы -> Настроить -> Применять только к службам*.

Тип протокола – UDP. Все порты

Область – Любой IP-адрес

Действие – Разрешить подключение

Профиль – все (*Доменный, Частный, Публичный*).

Имя – S-Terra VPN Service.

Нажмите *Готово*.

8. Регистрация пользователя

Регистрация пользователя в Продукте при использовании пользовательского токена описана в разделе ”Логин в режиме пользовательского токена”.

При подготовке инсталляционного пакета устанавливается интерактивный или неинтерактивный режим логина пользователя в Продукт.

8.1 Интерактивный режим логина в Продукт

ОС Windows XP

В ОС Windows XP после перезагрузки ОС при интерактивном режиме появляется окно логина (Рисунок 37) в Продукт для ввода и изменения пароля пользователя. По умолчанию пароль является пустым.

Рисунок 37

При нажатии на кнопку Change Password откроется окно, в котором можно изменить пароль пользователя (Рисунок 38):

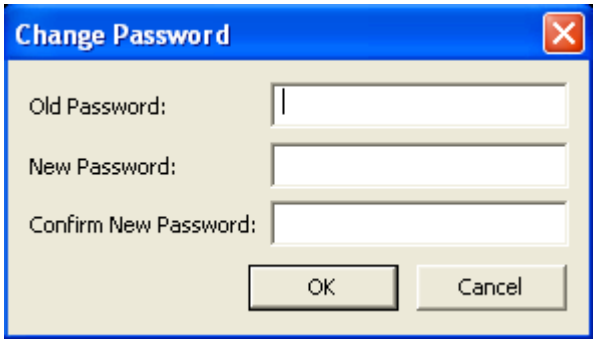


Рисунок 38

Для смены пароля необходимо ввести старый пароль и новый с подтверждением правильности нового пароля. Если старый пароль вводится трижды неправильно, то каждая последующая попытка ввода пароля будет прерываться паузой на полминуты.

Окно логина в Продукт (Рисунок 37) будет выводиться только при запущенном VPN-сервисе. Если к моменту вывода окна ОС Windows еще не запустила VPN-сервис, то Продукт будет ждать 30 секунд (по умолчанию). Если VPN-сервис не будет запущен и через 30 секунд, то появится сообщение с предложением повторить процесс логина (Рисунок 39). Чтобы данное окно не

появлялось – увеличьте время инициализации сервиса (см. раздел. «Время инициализации VPN сервиса»).

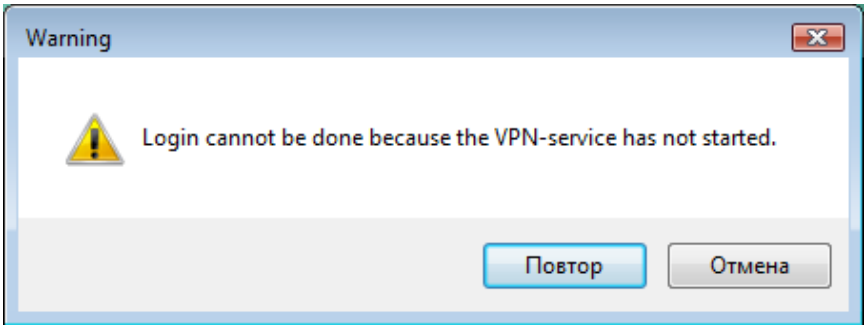


Рисунок 39

Окно логина в ОС Windows XP появляется только после регистрации пользователя в Продукте или отказе от нее.

ОС Windows Vista и более поздние версии ОС

После перезагрузки ОС при интерактивном режиме логина на экран выводятся иконки для выбора пользователя, текущего статуса Продукта S-Terra Client и окно логина в Продукт.

Процессы входа в ОС и логина в Продукт независимы друг от друга. Можно сначала зарегистрироваться в Продукте, а потом войти в ОС или наоборот.

В окне выбора пользователя иконка, отображающая текущий статус Продукта, может быть смещена в нужном направлении, если ее положение неудобно (см. раздел «Изменение положения иконки текущего статуса Продукта»).

Окно логина в Продукт появляется только после инициализации VPN сервиса. Если к моменту вывода окна VPN сервис не будет готов к работе, то Продукт будет ждать 30 секунд (время по умолчанию) (см. раздел «Время инициализации VPN сервиса»). Если VPN сервис не будет готов к работе и через 30 секунд, то появится сообщение с предложением повторить процесс логина (Рисунок 39).

Окно логина в Продукт автоматически появляется в интерактивном режиме, когда необходимо выбрать пользователя для входа в ОС Windows:

- после загрузки системы
- при выходе пользователя из системы
- при смене пользователя.

Успешная регистрация

После успешной регистрации пользователя в Продукт загружается локальная политика безопасности, предписанная данному пользователю и находящаяся в базе Продукта.

После входа пользователя в ОС иконка статуса Продукта будет размещена в панели задач и изменит свой вид (Рисунок 40) (см. главу «Отображение текущего статуса Продукта»).

Рисунок 40

Если отказаться от логина пользователя в Продукт, то потом зарегистрироваться в Продукте можно:

- нажав на иконку статуса Продукта в окне выбора пользователя, и в выпадающем меню выбрать предложение Login (Рисунок 41)
- либо после входа в ОС, нажав на иконку статуса Продукта в панели задач (см. раздел “Login/Logout”).

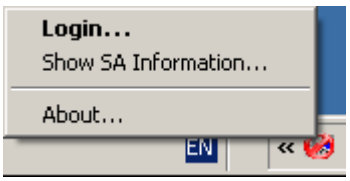


Рисунок 41

Неуспешная регистрация

Специальная политика безопасности **Log-off policy**, задаваемая администратором при подготовке инсталляционного пакета, служит для безопасности работы пользователя, при которой клиент не может создавать защищенных соединений, и загружается автоматически в следующих случаях:

- до тех пор, пока пользователь не ввел свой пароль
- при вводе неверного пароля три раза
- при отказе от регистрации (login), если нажать кнопку Cancel
- при выходе пользователя из системы
- при смене пользователя
- при отключении пользовательского токена.

Политика **Log-off policy** работает по одному из двух правил:

- правило `PassDHCP` – пропускать пакеты только по протоколу DHCP. Трафик DHCP пропускается для настройки TCP/IP стека по протоколу DHCP
- правило `Default Driver Policy (DDP)` – политика драйвера по умолчанию, может принимать значения:
  - правило `Passall` – пропускать все пакеты. Значение по умолчанию.
  - правило `PassDHCP` – пропускать пакеты только по протоколу DHCP. Трафик DHCP пропускается для настройки TCP/IP стека по протоколу DHCP.
  - правило `Dropall` – не пропускать трафик.

Политика **Default Driver Policy (DDP)**, задаваемая администратором, загружается в следующих случаях:

- при ошибочной загрузке конфигурации – до старта VPN сервиса
- при остановке VPN сервиса.

8.2 Неинтерактивный режим логина в Продукт

При неинтерактивном режиме логина в Продукт автоматически производится попытка логина с пустым паролем (в качестве пароля используется пустая строка) и при успешном логине окно с запросом пароля не появляется. При неуспешном логине Продукт ведет себя как при интерактивном логине – будет выдано окно запроса пароля (Рисунок 38).

При установленном Продукте S-Terra Client можно изменить интерактивный режим логина на неинтерактивный. Включение неинтерактивного режима осуществляется присвоением значения, отличного от 0, переменной в реестре NonInteractiveLogin:

```
HKEY_LOCL_MACHINE\SOFTWARE\VPN Agent\NonInteractiveLogin.
```

При работе продукта под управлением ОС Windows 7 x64 для переключения в неинтерактивный режим следующим переменным надо присвоить значение 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VPN Agent\NonInteractiveLogin
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VPN Agent\NonInteractiveLogin
```

При значении 0 – будет включен интерактивный режим (значение по умолчанию).

8.3 Время инициализации VPN сервиса

Можно задать время инициализации VPN сервиса в реестре при помощи переменной `MaxServiceStartTimeout`:

```
HKEY_LOCL_MACHINE\SOFTWARE\VPN Agent\MaxServiceStartTimeout
```

Эта переменная задает время в секундах ожидания запуска VPN сервиса. Если эта переменная не задана, то принимается значение по умолчанию, равное 30 секундам. Максимальное значение, которое можно задать – 600 секунд. При задании большего значения – устанавливается значение в 600 секунд.

При старте vpn-сервиса выполняется стартовый контроль целостности установленного Продукта S-Terra Client, описанный в разделе «Стартовый и регламентный контроль целостности продукта».

8.4 Переключение в режим пользовательского токена

Установленный Продукт S-Terra Client, не подготовленный для работы с пользовательским токеном, можно переключить в этот режим работы посредством присвоения значения, отличного от 0, переменной `TokenLogin` в реестре:

для ОС Windows 32-bit:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VPN Agent
```

для ОС Windows 64-bit:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VPN Agent.
```

После внесенных изменений перезагрузите ОС Windows.

Вернуть Продукт в обычный режим работы – переменной `TokenLogin` присвоить значение 0.

8.5 Логин в режиме пользовательского токена

При использовании пользовательского токена устанавливается только интерактивный режим логина в Продукт, для этого:

- подключите пользовательский токен к компьютеру
- перезагрузите ОС
- введите PIN-код к токену в появившемся окне логина в Продукт (Рисунок 42).

.

Рисунок 42

В ОС Windows XP после регистрации пользователя в Продукте или отказе от нее появится окно логина в ОС.

В ОС Windows Vista и более поздних версиях ОС процессы входа в ОС и логина в Продукт независимы друг от друга. Можно сначала зарегистрироваться в Продукте, а потом войти в ОС или наоборот.

При успешном вводе PIN-кода с токена загружается локальная политика безопасности, заданная для данного пользователя, а в панели задач появляется иконка Продукта рядом с иконкой токена (Рисунок 43) (см. раздел “Отображение текущего статуса Продукта”).

Рисунок 43

При каждом отключении токена от компьютера, Продукт детектирует момент отключения и в панели задач появляется другая иконка (Рисунок 44), которая говорит о том, что пользователь не зарегистрирован в Продукте. Политика безопасности отгружается и загружается специальная политика `Log-off policy`, при которой невозможно создавать защищенные соединения.

Рисунок 44

Любая попытка зарегистрироваться в Продукте при отключенном пользовательском токене заканчивается неудачей. Например, при нажатии правой кнопки мыши на иконке Продукта появляется меню следующего вида (Рисунок 45).

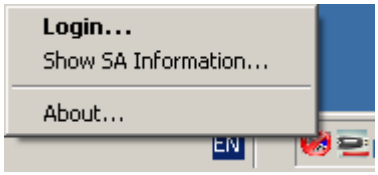


Рисунок 45

Выбор предложения Login при отключенном токене приводит к появлению окна логина с просьбой вставить (выбрать) пользовательский токен и ввести PIN-код (Рисунок 46).

Рисунок 46

8.6 Неинтерактивный режим логина в ОС

При интерактивном/неинтерактивном режиме логина в S-Terra Client для автоматического входа пользователя в ОС Windows (не появляется окно Log On to Windows) необходимо выполнить дополнительные настройки. Конкретную информацию о настройках для определенной ОС Windows можно получить на сайте Microsoft.

8.7 Замечание

Время загрузки ОС Windows XP с продуктом S-Terra Client зависит от нескольких факторов, в том числе:

- аппаратной платформы (CPU, объема памяти, диска)
- количества и качества установленного программного обеспечения
- степени фрагментации жесткого диска
- количества накопленного «информационного мусора» в реестре.

Установленный на компьютер S-Terra Client позволяет создавать защищенное соединение до логина пользователя в ОС Windows XP, но для этого пользователь должен пройти дополнительную аутентификацию (окно регистрации в продукт) перед логином в ОС.

Сервис аутентификации дожидается запуска всех пользовательских сервисов и запуска S-Terra Client. Для давно эксплуатирующейся системы, где установлено много приложений, время загрузки сервисов значительно возрастает. На компьютерах с небольшим объемом памяти процесс загрузки сервисов еще увеличивается, поскольку системе не хватает памяти, и она начинает выгружать только что загруженные приложения в swap файл на диск.

Ожидание появления дополнительного окна аутентификации может расцениваться пользователем как запуск конкретного приложения S-Terra Client, а не запуск всех приложений ОС. Пользователю кажется, что загрузка ОС становится значительно дольше, хотя объективные замеры с секундомером доказывают обратное.

Чтобы избежать описанной выше ситуации рекомендуется выполнить некоторые действия:

- удалить неиспользуемые приложения, запускающиеся в процессе загрузки Windows
- выполнить чистку и дефрагментацию реестра
- выполнить дефрагментацию жесткого диска.

9. Стартовый и регламентный контроль целостности Продукта

Программная часть Продукта

При старте сервиса vpnsvc автоматически запускается утилита `cspvpn_verify` для проверки целостности программной части (неизменяемых файлов) установленного Продукта, перечисленных в файле `.hashes`.

При успешной проверке никакого сообщения на экран не выдается, а в файл `cspvpn_verify_err.log`, расположенный в каталоге Продукта, передается сообщение: `Verification SUCCESS: <n> files verified`.

При обнаружении ошибки работа утилиты прерывается и выдается сообщение об ошибке в файл `cspvpn_verify_err.log`.

Файл `.hashes` расположен в каталоге Продукта (по умолчанию – `Program Files\S-Terra Client`) и содержит строки вида (между контрольной суммой и именем файла один пробел):

```
<hash> <encoded_file_path>
```

где

`<hash>` – эталонное значение контрольной суммы для данного файла

`<encoded_file_path>` – полный путь к проверяемому файлу.

Регламентный контроль целостности S-Terra Client осуществляется во время работы Продукта запуском вручную утилиты `cspvpn_verify` из каталога установленного Продукта.

При успешной проверке и при обнаружении ошибки реакция будет такой же как и при стартовом контроле.

Возможные сообщения об ошибках

Таблица 2

	Сообщение об ошибке	Описание проблемы	Код возврата	Продолжение работы утилиты
1	Integrity verification tool not found	Отсутствует продукт, используемый непосредственно для подсчета контрольных сумм.	1	
2	Integrity verification list “<file_.hashes_full_path >” not found	Отсутствует файл .hashes.	2	
3	Integrity verification list “<file_.hashes_full_path >” is corrupted	Проблемы с чтением файла .hashes (например, ошибочный синтаксис файла).	3	

4	Integrity verification tool call failed on file “<product_file_full_path> ”	Запуск cpverify по каким-либо причинам не произошел (какая-то системная ошибка; например, нехватка ресурсов, проблемы с правами доступа и т.п.) или вернул неожиданный код возврата (прерывание по сигналу, необработанный exception и т.п.).	4	Улитита продолжает работать
5	File “<product_file_full_path> ” is corrupted	Один или больше файлов продукта повреждены (контрольная сумма не соответствует эталонной; также возможны и другие ситуации – например, отсутствующий файл – cpverify их не различает).	5	Улитита продолжает работать

где

`<file_.hashes_full_path>` – полный путь к файлу `.hashes`

`<product_file_full_path>` – полный путь к файлу Продукта, на котором произошла ошибка.

При обнаружении ошибки по окончании работы утилиты выдается сообщение: `Verification FAILED`. Затем проверяется сервис vpnsvc и если он работает, то выполняется его аварийное прерывание.

Если обнаруживается несколько разнородных ошибок, то код возврата утилиты формируется по первому сообщению об ошибке.

При устранении ошибки перезапустите сервис vpnsvc:

```
net start vpnsvc.
```

Информационная часть Продукта

Регламентная проверка целостности информационной части Продукта осуществляется при помощи утилиты `integr_mgr check`, описанной в разделе «Специализированные команды».

10. Отображение текущего статуса Продукта

Текущий статус Продукта отображает иконка, расположенная в панели задач.

Если пользователь не аутентифицировался, то иконка имеет вид:

Рисунок 47

Пользователь аутентифицировался, но Продукт не имеет ни одного защищенного соединения – иконка принимает вид:

Рисунок 48

Когда появляется хотя бы одно защищенное соединение, но трафик по этим соединениям отсутствует, то на иконке изменяется цвет "соединения" с серого на зеленый:

Рисунок 49

Если Продукт имеет хотя бы одно защищенное соединение и обрабатывает трафик по этим соединениям, то на иконке изменяется цвет "монитора" с синего на бирюзовый:

Рисунок 50

При наведении курсора мыши на иконку всплывает информация о количестве "живых" SA (существующих на момент наведения курсора мыши на иконку) и количестве байт обработанного трафика по всем существовавшим и существующим SA с момента загрузки операционной системы.

Рисунок 51

10.1 Изменение положения иконки текущего статуса Продукта

Положение иконки, отображающей текущий статус Продукта в окне выбора пользователя, если оно неудобно, можно изменить с помощью переменной в реестре:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\{7026F7B9-3C2E-4b80-A62E-69645BFF1190}\Position`

Значением переменной `Position` является строка формата:

`<int_x>,<int_y>`

где

`int_x` – целое число, задающее смещение иконки по горизонтальной оси, которое может принимать значения:

- 0 – положение иконки задается автоматически с учетом разных параметров
- положит.знач. – положение иконки отсчитывается относительно левой стороны экрана
- отрицат.знач. – положение иконки отсчитывается относительно правой стороны экрана

`int_y` – целое число, задающее смещение иконки по вертикальной оси, которое может принимать значения:

- 0 – положение иконки задается автоматически с учетом разных параметров
- положит.знач. – положение иконки отсчитывается относительно верхней стороны экрана
- отрицат.знач. – положение иконки отсчитывается относительно нижней стороны экрана.

10.2 Login/Logout

При нажатии на иконку правой кнопкой мыши открывается меню следующего вида:

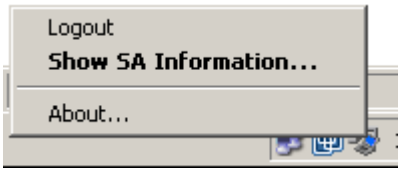


Рисунок 52

В зависимости от состояния системы (аутентифицировался пользователь или нет) будет показано предложение `Login` или `Logout`.

При выборе предложения `Login` появится окно ввода пароля (Рисунок 38) для аутентификации пользователя и изменения пароля.

При выборе предложения `Logout` выполнится следующее:

- будут уничтожены все существующие SA с данным клиентом
- загрузится специальная политика Log-off policy
- предложение `Logout` изменится на `Login`.

10.3 SA Information

При выборе предложения `Show SA Information` – появится окно монитора созданных SA:

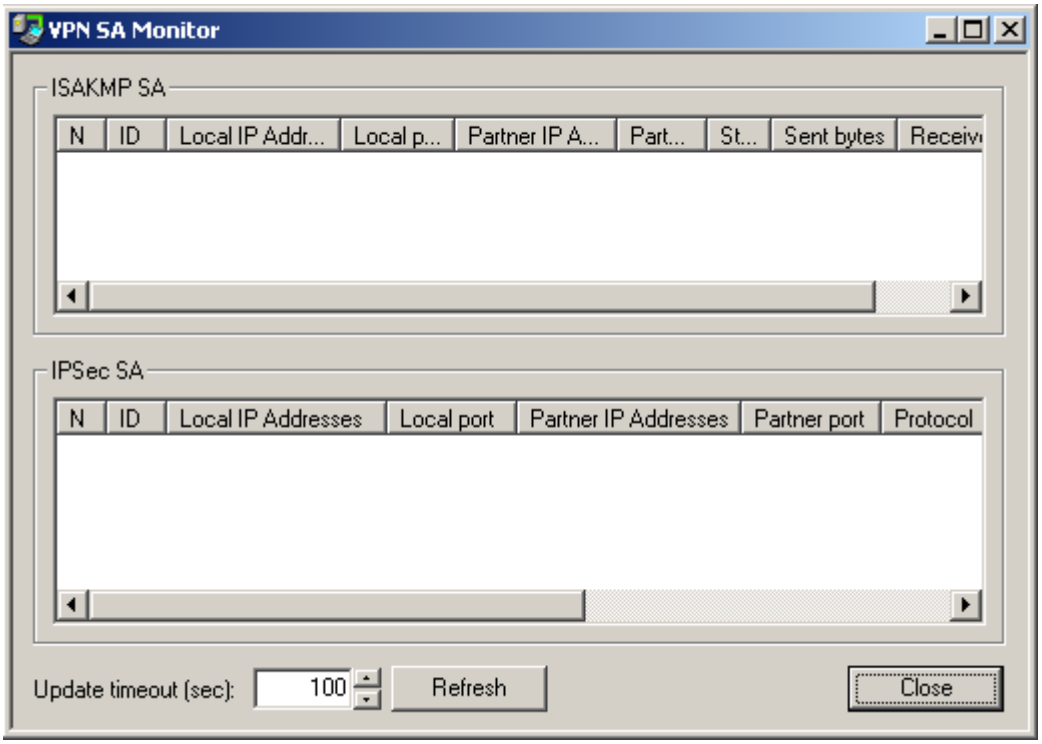


Рисунок 53

где:

ISAKMP SA – список ISAKMP SA. Выводятся следующие поля:

- `N` – порядковый номер в таблице
- `ID` – уникальный номер SA
- `Local IP Addresses` – локальные адреса
- `Local port` – локальный IKE порт
- `Partner IP Addresses` – партнерские адреса
- `Partner port` – партнерский IKE порт
- `State` – состояние SA:
  - `incomplete` – недостроенный
  - `ready` – рабочий
  - `configuration` – изменяемый
  - `deletion` – удаляемый
  - `unknown` – неизвестное состояние (не должно выводится)
- `Sent bytes` – количество отосланных байт
- `Received bytes` – количество полученных байт

IPSec SA – список IPsec SA с полями:

- `N` – порядковый номер в таблице
- `ID` – уникальный номер SA

- `Local IP Addresses` – локальные адреса
- `Local port` – локальные порты
- `Partner IP Addresses` – партнерские адреса
- `Partner port` – партнерские порты
- `Protocol` – сетевые протоколы
- `Action` – тип действия:
  - `AH`
  - `ESP`
  - `AH+ESP`
- `Type` – тип соединения:
  - `transport` – транспортный режим
  - `tunnel` – туннельный режим
  - `nat-t-transport` – транспортный режим через NAT
  - `nat-t-tunnel` – туннельный режим через NAT
- `Sent bytes` – количество отосланных байт
- `Received bytes` – количество полученных байт

  Update timeout (sec) – время, через которое будут обновляться данные в таблице о созданных SA. Диапазон значений `1..9999`, начальное значение – 2 секунды.

При выборе предложения `About` в меню выводится информация о версии Продукта:

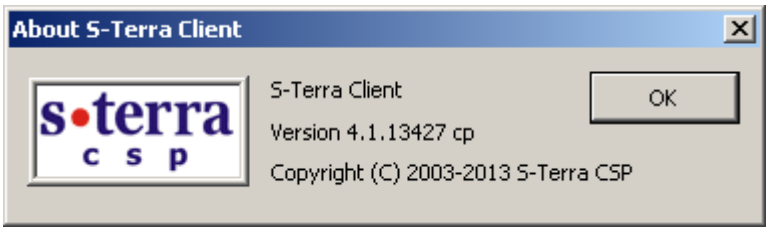


Рисунок 54

11. Деинсталляция S-Terra Client

Деинсталляция S-Terra Client производится стандартными средствами операционной системы – вызовом модуля Add/Remove Programs и выбором из списка строки S-Terra Client.

При деинсталляции S-Terra Client происходит включение стандартного сервиса, связанного с IPsec и IKE. В ОС Windows XP и ОС Windows Server 2003 – это Служба IPSEC, в ОС Windows Vista и более поздних версиях – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности».

При деинсталляции S-Terra Client может появиться окно (Рисунок 55). Необходимо разрешить запуск деинсталлятора.

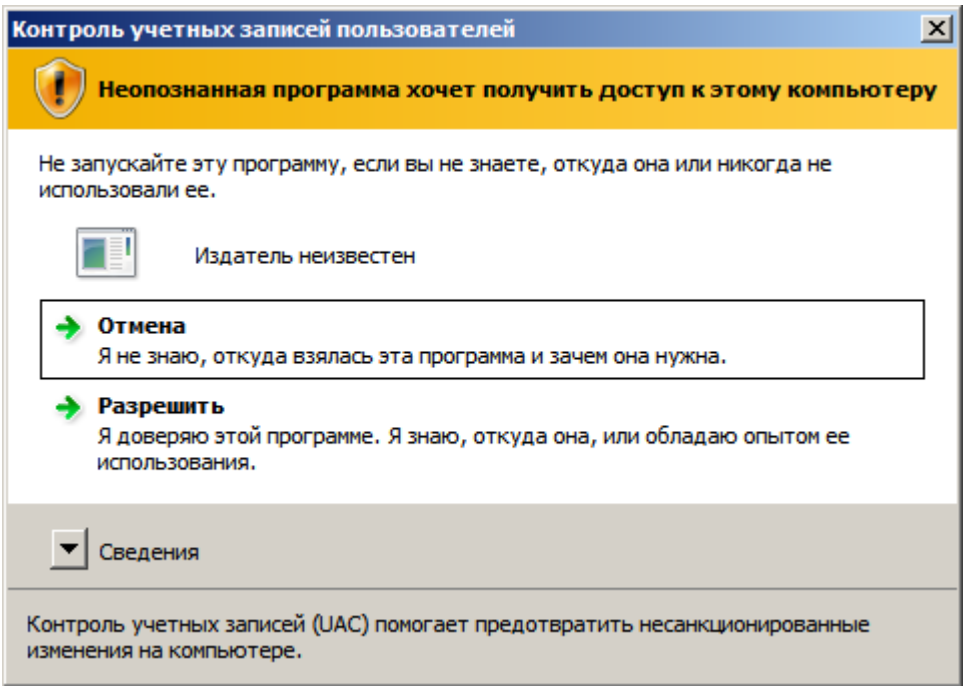


Рисунок 55

Примечание: не рекомендуется деинсталлировать S-Terra Client после выхода из спящего режима или режима гибернации. В этом случае сначала следует перезагрузить компьютер.

12. Восстановление S-Terra Client

Во внештатных ситуациях – сбой в работе Продукта, зависание Продукта и др. перезагрузите LSP конфигурацию командой `lsp_reload` (если это возможно) или перезапустите компьютер. Если функции продукта не восстановились, то переустановите S-Terra Client.

13. Специализированные команды

Программные утилиты, входящие в состав Продукта S-Terra Client:

`cert_mgr show`	для просмотра сертификатов, размещенных в файле или базе Продукта
`cert_mgr check`	для проверки сертификатов в базе Продукта
`cert_mgr create`	для генерации ключевой пары и создания запроса на сертификат
`cert_mgr import`	для регистрации промежуточных CA сертификатов и сертификатов партнеров в базе Продукта
`cert_mgr remove`	для удаления сертификатов из базы Продукта
`client_login`	для аутентификации пользователя при входе в систему
`client_logout`	для завершения сессии пользователя
`cspvpn_verify`	для регламентной проверки целостности установленного Продукта
`dp_mgr show`	для просмотра настроек политики Default Driver Policy
`dp_mgr set`	для настройки параметров Default Driver Policy
`drv_mgr`	показывает список поддерживаемых настроек IPsec-драйвера
`drv_mgr show`	для просмотра настроек IPsec-драйвера
`drv_mgr set`	для изменения настроек IPsec-драйвера
`drv_mgr reload`	для загрузки настроек IPsec-драйвера
`fwconn_show`	для просмотра информации о TCP-соединениях
`if_show`	для просмотра параметров сетевых интерфейсов, как защищаемых, так и не контролируемых Продуктом
`integr_mgr calc`	для вычисления контрольной суммы указанного файла
`integr_mgr check`	для проверки целостности информационной части Продукта
`key_mgr import`	для импорта предопределенных ключей в базу Продукта
`key_mgr remove`	для удаления предопределенных ключей из базы Продукта
`key_mgr show`	для просмотра предопределенных ключей, зарегистрированных в Продукте
`key_mgr list`	для просмотра имен предопределенных ключей, зарегистрированных в Продукте
`klogview`	для просмотра сообщений, выдаваемых системой протоколирования IPsec-драйвера
`lic_mgr show`	для просмотра текущей лицензии на Продукт
`lic_mgr set`	для установки лицензии на Продукт
`log_mgr show`	для просмотра общего уровня протоколирования всех событий, уровня протоколирования групп событий и настроек syslog-клиента
`log_mgr set`	для настроек протоколирования
`lsp_mgr check`	для проверки LSP конфигурации
`lsp_mgr load`	для для загрузки конфигурации из файла в базу Продукта
`lsp_mgr reload`	для перезагрузки LSP конфигурации
`lsp_mgr unload`	для выгрузки LSP конфигурации и загрузки политики DDP
`lsp_mgr show`	для просмотра LSP

`lsp_mgr show-info`	для просмотра информации о LSP
`pwd_change`	для изменения пароля пользователя
`sa_mgr show`	для просмотра информации обо всех IPsec SA и ISAKMP SA
`sa_mgr clear`	для удаления ISAKMP и IPsec соединений
`ver_show`	для получения информации о Продукте.

В операционной системе Microsoft® Windows выполнение этих команд можно производить из командной строки. Для запуска утилиты из командной строки перейдите в папку, в которой находится утилита: `C:\Programs Files\S-Terra Client`.

Запуск утилит с ключом `-h` вызывает помощь.

Все утилиты, обращающиеся к vpnsvc сервису, имеют опцию `-T <timeout>`, устанавливающую максимальное время ожидания ответа от vpnsvc сервиса. Опция глобальная и должна указываться в начале списка опций, с которыми запускается утилита.
Например, команда `sa_mgr -T 0 show` – корректная, а `sa_mgr show -T 0` – нет.
Если опция не указана явно, то утилита ожидает ответа от vpnsvc сервиса в течение времени, установленного по умолчанию для этой утилиты.

Количество одновременно обрабатываемых запросов от утилит vpnsvc сервисом не больше 3. При превышении лимита запросы отвергаются, и утилита выдает диагностику “`DAEMON BUSY NOW`”. Повторить запуск утилиты можно после того, как хотя бы одна из таких утилит завершит работу.

Ограничения на работу с утилитами

Для работы с некоторыми утилитами необходимо выполнение двух условий:

- Пользователь должен иметь права Администратора.
  Начиная с ОС Windows Vista консольное окно “cmd”, из которого выполняются такие утилиты, должно быть запущено с помощью пункта "Запуск от имени администратора" (Run As Administrator).
  Если это условие не выполнено, пользователю будет выдано сообщение:
  `Error: You need Administrator permissions.`
- Пользователь должен иметь право на изменение настроек Продукта.
  Эта возможность локального управления Продуктом задается администратором при подготовке инсталляционного пакета пользователя.
  Если это условие не выполнено, пользователю будет выдано сообщение:
  `Error: Local management is not allowed.`

13.1 cert_mgr show

Команда `cert_mgr show` предназначена для просмотра сертификатов, лежащих в файле или базе Продукта.

Синтаксис

cert_mgr [-T timeout] **show** [-f C_FILE [-p C_FILE_PWD]] [-i OBJ_INDEX1]…[-i OBJ_INDEXN] [-expired_remote]

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-f C_FILE	путь к файлу с сертификатами. Если данная опция не указана, то будут показаны сертификаты из базы Продукта.
-p C_FILE_PWD	пароль к файлу с сертификатами. Необязательный параметр. Используется только для доступа к файлам, защищенным паролем.
-i OBJ_INDEXN	индекс объекта (сертификата) в файле или базе Продукта. Если при написании команды указан путь к файлу, то индекс будет задавать номер искомого сертификата в файле. Если путь к файлу не указан, то индекс будет применяться к базе Продукта. Индекс задается в виде целого десятичного числа. В качестве индекса нельзя указывать 0.
-expired_remote	показать все сертификаты партнеров, срок действия которых истек. Сертификаты, не вступившие в силу, не показываются.

Значение по умолчанию значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра списка сертификатов и CRL, размещенных в файле или базе Продукта. Без указания файла и индекса объекта будет показан весь нумерованный список сертификатов и CRL, лежащих в базе Продукта.

Пример

Пример просмотра сертификатов, лежащих в контейнере, который защищен паролем:

```
C:\Program Files\S-Terra Client>cert_mgr show -f test.p12 -p russia
Certificate/Crl from file test.p12
Found 2 certificates. Found 1 CRL.
1 O=S-Terra,CN=CA Cert
2 O=S-Terra,CN=Technological Cert
3 CRL: C=RU,O=STcert,OU=QA,CN=CAUN0
```

Пример просмотра в базе Продукта сертификатов партнеров, срок действия которых истек.

```
C:\Program Files\S-Terra Client>cert_mgr show -expired_remote
3 Status: remote
  Subject: O=TrustWorks,CN=CA Cert
  Issuer: O=TrustWorks,CN=CA Cert
  Valid from: Fri Dec 31 16:00:00 1999
  Valid to:   Sat Dec 31 16:00:00 2005
  Version: 3
```



```
  Serial number: 01
  Signature algorithm: md5RSAencryption
  Public key: RSA(1024)
  Hash MD5:  1E 8D 9D 61 2E 41 4C A1 CC BB 33 81 EF 52 42 35
  Hash SHA1: E8 4F 2C A6 2E 01 5D 36 DF 07 14 E2 9C 51 B2 F7 8B 44
1F FF
  CRLI[0]: O=TrustWorks,CN=CA Cert
```


13.2 cert_mgr check

Команда `cert_mgr check` предназначена для проверки сертификатов, размещенных в базе Продукта.

Синтаксис

`cert_mgr` `[-T timeout]` **`check`** `[-i OBJ_INDEXN]`

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
`-i OBJ_INDEXN`	индекс сертификата в базе Продукта, который следует проверить. Необязательный параметр.

Значение по умолчанию значение по умолчанию отсутствует

Рекомендации по использованию

Проверяются сертификаты, находящиеся в базе Продукта. Без указания параметра `-i` проверяются все сертификаты из базы Продукта.

Утилита выводит состояние сертификата `"Active"` или `"Inactive"`. В случае, если сертификат имеет состояние `"Inactive"`, выводится краткое описание причины неактивности:

- `Certificate is invalid` – неверный формат сертификата
- `Certificate is expired` – срок использования сертификата истек
- `Certificate is not valid yet` – время использования сертификата не наступило
- `Certificate is revoked` – сертификат отозван
- `Certificate can not be verified` – сертификат не удается проверить:
  - в базе отсутствует сертификат(ы) для построения цепочки сертификатов с корректным конечным CA сертификатом, которому мы доверяем
  - в базе нет необходимого CRL для проверки одного из сертификатов цепочки, подобная ситуация может возникнуть при включении проверки CRLs (загружена DDP или в загруженной конфигурации явно задано CRLHandlingMode = ENABLE)
- `Private key container is not accessible` – нет доступа к контейнеру с секретным ключом
- `Private key is not accessible` – нет доступа к секретному ключу
- `Private key is not consistent certificate` – секретный ключ не подходит к сертификату
- `It is certificate request` – данный объект является сертификатным запросом.

Пример

Проверка сертификатов в базе Продукта:

```
cert_mgr check
1 State: Inactive CN=partner
Certificate is expired.
Valid from: Wed Sep 22 00:17:02 2010
Valid to:   Thu Sep 22 00:27:02 2011
```


13.3 cert_mgr create

Команда `cert_mgr create` предназначена для генерации ключевой пары и создания запроса на локальный сертификат для конечного устройства. На основании этого запроса Certificate Authority создаст соответствующий сертификат.

Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
cert_mgr [-T timeout] create - subj CERT_SUBJ [-RSA|-DSA|-GOST_R3410EL] [-512|-1024]  [-mail MAIL] [-ip IP_ADDR] [-dns DNS] [-kc K_CONTAINER_NAME]
 [-kcp K_CONTAINER_PWD] [-f OUT_FILE_NAME]
```

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
`-subj CERT_SUBJ`	значение поля `Subject Name` сертификата
`-RSA`	идентификатор алгоритма RSA, который будет использован для генерации ключевой пары. Затем секретный ключ будет применен для формирования ЭЦП создаваемого запроса.
`-DSA`	идентификатор алгоритма DSA, который будет использован для генерации ключевой пары. Затем секретный ключ будет применен для формирования ЭЦП создаваемого запроса.
`-GOST_R3410EL`	идентификатор алгоритма ГОСТ Р 34.10-2001, который будет использован для генерации ключевой пары. Затем секретный ключ будет применен для формирования ЭЦП создаваемого запроса.
`-512`	длина открытого ключа – 512 бит (только для алгоритмов RSA и DSA).
`-1024`	длина открытого ключа – 1024 бита (только для алгоритмов RSA и DSA).
`-mail MAIL`	значение поля Mail для альтернативного имени (Alternative Subject Name) владельца сертификата, которое может использоваться в качестве идентификатора владельца.
`-ip IP_ADDR`	значение поля IP Address для альтернативного имени (Alternative Subject Name) владельца сертификата, которое может использоваться в качестве идентификатора владельца.
`-dns DNS`	значение поля DNS для альтернативного имени (Alternative Subject Name) владельца сертификата, которое может использоваться в качестве идентификатора владельца.
`-kc K_CONTAINER_NAME`	имя контейнера с секретным ключом.
`-kcp K_CONTAINER_PWD`	пароль к контейнеру с секретным ключом.
`-f OUT_FILE_NAME`	имя файла, в который будет помещен запрос на сертификат в формате PKCS#10.

Значение по умолчанию

По умолчанию используется алгоритм RSA и ключ длиной 512 бит.

Рекомендации по использованию

Используйте данную команду для создания ключевой пары и запроса на сертификат.

Созданный запрос на сертификат защищается от подмены при помощи ЭЦП, которая формируется с использованием созданного секретного ключа и выбранного алгоритма ЭЦП.

В режиме **КС1**, в момент генерации ключевой пары (при использовании алгоритма ГОСТ Р 34.10-2001), запускается генератор случайных чисел и на консоли появляется просьба понажимать любые клавиши или поперемещать указатель мыши.

Команда `cert_mgr create` позволяет сохранить контейнер с секретным ключом на конечном устройстве в локальном хранилище, избежав ситуации переноса контейнера с одного носителя на другой.

Если при запуске команды не указать опцию `-f` с именем файла для размещения запроса, то сформированный запрос будет выведен на экран в формате `b64`.

Если при запуске команды не указать имя контейнера, то он будет создан с именем \\.\REGISTRY\REGISTRY\\vpnXXXXXXXX.

Одновременно хранится только один сертификатный запрос. При создании следующего запроса и незаконченном первом (по которому не создан сертификат), старый запрос удаляется. При таком удалении неиспользованного запроса будет так же удаляться и контейнер с ним связанный.

В режиме **КС2** при генерации ключевой пары будет использоваться датчик случайных чисел сертифицированного средства доверенной загрузки. Необходимо уточнение поддержки использования аппаратных ДСЧ для разных операционных систем. Особенности генерации ключевой пары для режима защиты КС2, если для ССДЗ не поддерживается функциональность ДСЧ описаны в соответствующем разделе в «Приложении А».

Работа с eToken

Если создания контейнера и запроса на локальный сертификат выполняется на токене, то использование опции `kcp` обязательно. В качестве пароля к контейнеру должен использоваться PIN-код к токену.

Пример

Пример создания запроса на локальный сертификат с использованием алгоритма ГОСТ Р 34.10-2001:

```
cert_mgr create -subj "O=S-Terra,CN=LocalCert" -GOST_R3410EL -dns
local.s-terra.com -f c:\certs\local_cert
```

Пример создания запроса на локальный сертификат и контейнера на токене:

```
cert_mgr.exe create -subj "C=test" -GOST_R3410EL -kc "\\.\AKS ifdh 0\11"
-kcp 1234
```


13.4 cert_mgr import

Команда `cert_mgr import` предназначена для регистрации сертификатов партнеров, промежуточных CA сертификатов и списка отозванных сертификатов в базе Продукта.

Для работы с опциями `-t` и `-l` требуются права Администратора, пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
cert_mgr [-T timeout] import -f C_FILE [-p C_FILE_PWD] [-i OBJ_INDEXN]
[-t |-l | -kc K_CONTAINER_NAME [-kcp K_CONTAUNER_PWD] | [-kf K_FILE [-kfp
K_FILE_PWD]]
```

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
`-f C_FILE`	путь к файлу с сертификатами
`-p C_FILE_PWD`	пароль к файлу с сертификатами. Необязательный параметр. Используется только для доступа к файлам, защищенным паролем.
`-i OBJ_INDEXN`	индекс сертификата в файле. При импорте одного сертификата из файла, содержащего один сертификат, данный параметр можно не указывать, он будет равен 1. Индекс задается в виде целого десятичного числа. В качестве индекса нельзя указывать 0.
`-t`	признак, что данный CA-сертификат должен быть импортирован как TRUSTED.
`-l`	признак, что сертификат должен быть импортирован как локальный (допустимо только для случая, когда сертификат является ответом на запрос, созданный с помощью cert_mgr create; несовместимо с опцией `-kc`).
`-kc K_CONTAINER_NAME`	имя контейнера с секретным ключом регистрируемого сертификата. Не может использоваться, если ранее введена опция `-t` или `-l`.
`-kcp K_CONTAINER_PWD`	пароль к контейнеру с секретным ключом регистрируемого сертификата. Необязательный параметр. Используется тогда, когда контейнер с секретным ключом защищен паролем. Если контейнер находится на токене, то в качестве пароля к контейнеру должен использоваться PIN-код к токену.
`-kf K_FILE`	путь к файлу с секретным ключом регистрируемого сертификата. Необязательный параметр. Не может использоваться, если ранее введена опция `-t` или `-l`. (Устаревший параметр, в данной версии Продукта применять не рекомендуется.)
`-kfp K_FILE_PWD`	пароль к файлу с секретным ключом регистрируемого сертификата. Необязательный параметр. Используется, если файл с секретным ключом защищен паролем. (Устаревший параметр, в данной версии Продукта применять не рекомендуется.)

Значение по умолчанию значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для импорта сертификатов партнеров и промежуточных CA сертификатов в базу Продукта (сертификат партнера может быть получен и по протоколу IKE). При импорте нескольких объектов из одного файла используйте последовательное описание параметров импортируемых объектов.

Для успешной регистрации промежуточного CA сертификата в Продукте, в сертификате поле Basic Constraints («Основные ограничения») обязательно должен иметь значение TRUE. В противном случае, такой CA сертификат зарегистрирован не будет с выдачей сообщения об ошибке.

Пример

Регистрация локального сертификата в базе Продукта, контейнер с секретным ключом размещен на дискете или в реестре:

```
cert_mgr import -f c:\certs\partner01.cer
```


13.5 cert_mgr remove

Команда `cert_mgr remove` предназначена для удаления сертификатов из базы Продукта.

Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

`cert_mgr` `[-T timeout]` **`remove`** {-i OBJ_INDEX_01|`-expired_remote`}..[-i OBJ_INDEX_N]

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
`-i OBJ_INDEX_N`	индекс объекта (сертификата) в контейнере или базе Продукта
`-expired_remote`	сертификаты партнеров, срок действия которых истек (сертификаты, не вступившие в силу, не удаляются).

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для удаления сертификатов из базы Продукта.

Удалять можно как один, так и несколько сертификатов.

Для удаления нескольких сертификатов следует последовательно указать номера (индексы) удаляемых сертификатов, под которыми они хранятся в базе Продукта.

Для того чтобы ознакомиться с сертификатами, хранящимися в базе и выяснить номера (индексы) под какими они хранятся в базе Продукта, используйте команду `cert_mgr show`.

Удаление из базы Продукта списка CRL невозможно. Если в тексте команды будет указан номер (индекс) CRL, то будет выведено сообщение об ошибке.

Пример

Ниже приведен пример удаления сертификатов из базы Продукта. При написании команды были указаны индексы объектов 1, 2 и 3. Индексы 1 и 2 соответствовали сертификатам, а под индексом 3 в базе хранился CRL. На попытку удаления CRL программа выдала сообщение об ошибке:

```
cert_mgr remove -i 1 -i 2 -i 3
1 OK O=S-Terra,CN=Technological Cert
2 OK O=S-Terra,CN=CA Cert
User error: CRL can not be removed from base
Other operations are cancelled due to error
```


13.6 client_login

Команда `client_login` запускается автоматически при логине пользователя в систему и представляет собой GUI-приложение (Рисунок 37), в котором нужно ввести пароль для аутентификации пользователя.

Эта команда запускается и при выборе предложения Login в меню (Рисунок 52), которое появляеся на иконке в панели задач при работающем сервисе после того, как было выбрано предложение Logout.

Может быть использована и для изменения пароля пользователя.

Синтаксис

`client_login`

13.7 client_logout

Команда client_logout предназначена для завершения сессии пользователя. При этом производится загрузка политики Log-off Policy.

Эта команда запускается при выборе предложения Logout в меню (Рисунок 52), которое появляеся на иконке в панели задач при работающем сервисе после того, как было выбрано предложение Login. Возможен запуск команды вручную.

Синтаксис

`client_logout` `[-T timeout]`

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

Пример

Ниже приведен пример запуска вручную команды `client_logout`:

```
client_logout
    Logout OK
```


13.8 cspvpn_verify

Утилита `cspvpn_verify` используется для регламентной проверки целостности программной части установленного Продукта S-Terra Client во время его работы. Эта же утилита автоматически запускается при каждом старте сервиса vpnsvc.

Синтаксис

```
cspvpn_verify [-n]
```

`-n` запрет на завершение работы сервиса vpnsvc

Рекомендации по использованию

В состав Продукта входит файл `.hashes`, который содержит список всех исполняемых файлов, библиотек и неизменяемых конфигурационных файлов, а также значение контрольной суммы для каждого файла. Этот файл содержит строки вида:

```
<hash> <full_file_path>
```

где

`<hash>` – эталонное значение контрольной суммы для данного файла

`<full_file_path>` – полный путь к проверяемому файлу.

При запуске утилита проверяет целостность именно этого списка файлов.

Используйте утилиту для проверки целостности программной части во время работы Продукта,

Если проверка прошла успешно, то никакого сообщения не выдается.

При обнаружении ошибки работа утилиты прекращается с ненулевым кодом возврата и в файл лога `cspvpn_verify_err.log` передается сообщение об ошибке. Затем, в случае запуска утилиты без ключа `-n`, проверяется работа сервиса vpnsvc. При его наличии – выполняется аварийное прерывание.

Если обнаруживается несколько разнородных ошибок, то код возврата утилиты формируется по первому сообщению об ошибке.

Возможные сообщения об ошибках для данной утилиты приведены в разделе «Стартовый и регламентный контроль целостности продукта».

При устранении ошибки перезапустите сервис vpnsvc:

```
net start vpnsvc.
```

При нарушении целостности работающего Продукта переустановите Продукт, используя инсталляционный файл.

Пример

Ниже приведен пример запуска команды:

```
cspvpn_verify
    Mon Oct 03 15:00:24 2011
    Verification SUCCESS: 71 files verified
```


13.9 dp_mgr show

Команда `dp_mgr show` предназначена для просмотра установленных настроек политики `Default Driver Policy и Log-off policy`.

Default Driver Policy (DDP) – политика безопасности по умолчанию, задается администратором, может принимать следующие значения:

`passall`	пропускать весь трафик.
`passdhcp`	пропускать пакеты только по протоколу DHCP, т.е. будут уничтожаться все пакеты, кроме исходящих UDP-пакетов на порт 67 и входящих UDP-пакетов на порт 68.
`dropall`	не пропускать трафик (для релиза 14101 это значение недоступно).

Политика DDP задается администратором и загружается в следующих случаях:

- при ошибочной загрузке конфигурации – до старта vpnsvc сервиса
- при остановке vpnsvc.

Log-off policy – специальная политика безопасности, которая задается администратором, и служит для безопасности работы пользователя, при которой клиент не может создавать защищенных соединений. Эта политика работает по одному из двух правил:

`passdhcp`	пропускать пакеты только по протоколу DHCP, т.е. будут уничтожаться все пакеты, кроме исходящих UDP-пакетов на порт 67 и входящих UDP-пакетов на порт 68
`ddp`	политика по умолчанию.

Политика Log-off policy загружается автоматически в следующих случаях:

- до тех пор, пока пользователь не ввел свой пароль
- при вводе неверного пароля три раза
- при отказе от регистрации (login), если нажать кнопку Cancel
- при выходе пользователя из системы
- при смене пользователя.

Синтаксис

`dp_mgr` `[-T timeout]` **`show`** `[-ddp | -lop]`

`dp_mgr` `[-T timeout]` **`show`** (синтаксис команды для релиза 14101)

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд.
`-ddp | -lop`	установка одного из параметров позволяет посмотреть либо Default Driver Policy, либо Log-off policy.

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

Данная команда выводит установленные значения DDP и Log-off-policy, например:

```
dp_mgr show
  Default Driver Policy : passall
  Log-off-policy: ddp
```

13.10 dp_mgr set

Команда `dp_mgr show` предназначена для настройки параметров Default Driver Policy (DDP) – политики по умолчанию и Log-off policy (см. команду dp_mgr show). Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

dp_mgr `[-T timeout]` **set** `[-ddp {passall | passdhcp | dropall}] [-lop {ddp | passdhcp}]`

dp_mgr `[-T timeout]` **set** `[-ddp {passall | passdhcp}] [-lop {ddp | passdhcp}]` (синтаксис команды для релиза 14101)

`-T timeout` время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд.

`-ddp {passall | passdhcp | dropall}` устанавливает Default Driver Policy в один из режимов: passall (пропускать весь трафик), passdhcp (пропускать только DHCP пакеты), dropall (не пропускать трафик (для релиза 14101 этот режим недоступен)).

`-lop {ddp | passdhcp}` устанавливает Default Driver Policy или passdhcp (пропускать только DHCP пакеты).

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

Ниже приведен пример выполнения команды dp_mgr set:

```
dp_mgr set -ddp passall
  Default driver policy is wrote to db successfully
```


13.11 drv_mgr

Команда `drv_mgr` показывает имена поддерживаемых настроек, режим доступа к ним, размер в байтах и диапазон допустимых значений.

Синтаксис

`drv_mgr`

Список выводимых настроек:

```
List of properties:
Name                    access type size (in bytes) range [min-max]

pcap_minimal_mtu        read-only       4               [0-0]
fw_tcp_closed_ttl       lsp-managed     4               [1-65535]
fw_tcp_synsent_ttl      lsp-managed     4               [1-65535]
fw_tcp_synrcvd_ttl      lsp-managed     4               [1-65535]
fw_tcp_estab_ttl        lsp-managed     4               [1-65535]
fw_tcp_fin_ttl          lsp-managed     4               [1-65535]
fw_tcp_strictness       lsp-managed     4               [0-6]
fw_tcp_open_max         lsp-managed     4               [0-1000000]
fw_tcp_half_open_max    lsp-managed     4               [0-1000000]
fw_tcp_half_open_low    lsp-managed     4               [0-1000000]
fw_tcp_conn_rate_max    lsp-managed     4               unlimited
fw_tcp_conn_rate_low    lsp-managed     4               unlimited
frag_dont_grow_fragments read-write     1               [0-1]
frag_minimize_size      read-write      1               [0-1]
frag_df_options         read-write      1               [0-3]
ipsec_breq_max          read-write      4               unlimited
ipsec_breq_count        read-only       4               unlimited
ipsec_recursive_policy read-write       1               [0-1]
```

Описание настроек IPsec драйвера приведено в Таблица 3

Таблица 3

Наименование настройки	Тип доступа	Размерность	Рекомендуемые значения	Значение по умолчанию
	Описание			
frag_dont_grow_ fragments	чтение-запись		0-1	0
	Чтобы избежать повторной перефрагментации пакетов промежуточными маршрутизаторами, предусмотрены следующие значения: 1 – размер фрагментов не будет превышать максимальный размер оригинальных фрагментов 0 – пакет фрагментируется без учета размера оригинальных фрагментов			

Наименование настройки	Тип доступа	Размерность	Рекомендуемые значения	Значение по умолчанию
	Описание			
frag_minimize_size	Чтение-запись		0-1	0
	Чтобы избежать повторной перефрагментации пакетов промежуточными маршрутизаторами, предусмотрены следующие значения: 1 – размер фрагментов усредняется, т.е. минимизируется максимальный размер фрагмента при сохранении минимального количества фрагментов 0 – все фрагменты делаются максимального размера, кроме последнего. Пример: MTU – 270, пакет – 276 байтов, заголовок – 20 байт. Если значение 1, то фрагменты 148 и 148 байтов. Если значение 0, то фрагменты 268 и 28 байтов.			
frag_df_options	чтение запись		0-3	0
	Чтобы избежать повторной перефрагментации пакетов промежуточными маршрутизаторами, предусмотрены значения, которые определяют выставлять ли DF-бит на фрагментах: 0 – на фрагментах DF-бит всегда сбрасывается 1 – выставлять DF-бит у фрагментов, если оригинальный пакет был фрагментирован, не инкапсулирован в IPsec, и на фрагментах был выставлен DF-бит. Это значение позволяет восстанавливать DF-бит для открытого трафика. Таким образом хост, отправивший пакет, может проводить MTU discovery для фрагментированных пакетов. 2 – выставлять DF-бит для фрагментированных IPsec-пакетов, если на соответствующем IPsec SA включено MTU discovery. Этот флаг позволяет проводить MTU discovery для фрагментированных пакетов драйверу и избавиться от повторной фрагментации IPsec пакетов: – IPsec-пакет может быть фрагментирован, если в SA установлен режим сброса или копирования DF-бита (DFHandling в LSP). При этом, если установлен режим копирования, в исходном пакете DF-бит должен быть сброшен – сочетание, когда включено MTU discovery и DFHandling = CLEAR имеет смысл только при frag_df_options ≥ 2, т.к. нет смысла проводить MTU discovery, когда DF-бит всегда сброшен. 3 – комбинация 1 и 2.			
ipsec_breq_max	чтение запись		unlimited	1000
	Максимальное количество одновременно выполняющихся запросов на создание SA bundle. В LSP можно задать отдельные ограничения для каждого правила.			
ipsec_breq_count	чтение		unlimited	0
	Текущее количество одновременно выполняющихся запросов на создание SA bundle.			
ipsec_recursive_policy	чтение		0-1	0
	Включение/выключение рекурсивного режима поиска правил IPsec для обработки пакетов. Настраивается в LSP через атрибут AllowNestedIPsec.			

Наименование настройки	Тип доступа	Размерность	Рекомендуемые значения	Значение по умолчанию
	Описание			
pcap_minimal_mtu	чтение			1500
	Минимальное значение MTU для всех сетевых интерфейсов. Значение вычисляется на основании параметров интерфейсов, доступных для драйвера. Таким образом, минимальное значение MTU, используемое IP-драйвером может отличаться.			
fw_tcp_closed_ttl	чтение	секунды	1-65535	5
fw_tcp_synsent_ttl	чтение	секунды	1-65535	30
fw_tcp_synrcvd_ttl	чтение	секунды	1-65535	60
fw_tcp_estab_ttl	чтение	секунды	1-65535	3600
fw_tcp_fin_ttl	чтение	секунды	1-65535	30
	Время жизни записи о соединении. S-Terra Client сначала определяет состояние TCP соединения для каждого из партнеров, которые создают TCP соединение через шлюз безопасности. А в LSP в зависимости от этих состояний задано время жизни записи о соединении.			
fw_tcp_strictness	чтение		0-6	3
	Уровен "жесткости" к различным ситуациям, которые воспринимаются шлюзом как ошибочные			
fw_tcp_open_max	чтение		0-1000000	65536
	Максимальное количество разрешенных TCP-соединений. При превышении данного предела новые TCP-соединения будут отвергаться. Настраивается в LSP.			
fw_tcp_half_open_max	чтение		0-1000000	500
	Максимальное количество одновременно существующих полуоткрытых сеансов TCP, при достижении которого начинается их удаление при появлении нового запроса на соединение. Настраивается в LSP.			
fw_tcp_half_open_low	чтение		0-1000000	400
	Минимальное количество одновременно существующих полуоткрытых сеансов TCP, при достижении которого прекращается их удаление. Настраивается в LSP.			
fw_tcp_conn_rate_max	чтение		unlimited	500
	Максимальная частота появления полуоткрытых сеансов TCP в минуту, по достижении которой начинается их удаление. Настраивается в LSP.			
fw_tcp_conn_rate_low	чтение		unlimited	400
	Минимальная частота появления полуоткрытых сеансов TCP в минуту, по достижении которой прекращается их удаление. Настраивается в LSP.			

13.12 drv_mgr show

Команда `drv_mgr show` предназначена для просмотра установленных значений настроек работы IPsec-драйвера.

Синтаксис

```
drv_mgr show [PROPERTY_NAME1] [PROPERTY_NAME2] ...
```

`PROPERTY_NAMEn` имена настроек, значения которых должны быть показаны. Если ни одно имя не задано – будут показаны значения всех поддерживаемых настроек.

Имена настроек указаны в Таблица 3.

Пример

```
drv_mgr show
pcap_minimal_mtu       1500
fw_tcp_closed_ttl       5
fw_tcp_synsent_ttl      30
fw_tcp_synrcvd_ttl      60
fw_tcp_estab_ttl        3600
fw_tcp_fin_ttl          30
fw_tcp_strictness       3
fw_tcp_open_max         65536
fw_tcp_half_open_max    500
fw_tcp_half_open_low    400
fw_tcp_conn_rate_max    500
fw_tcp_conn_rate_low    400
frag_dont_grow_fragments 0
frag_minimize_size      0
frag_df_options         0
ipsec_breq_max          1000
ipsec_breq_count        0
ipsec_recursive_policy 0
```


13.13 drv_mgr set

Команда `drv_mgr set` предназначена для редактирования настроек работы IPsec-драйвера. С помощью этой команды можно изменять значения только тех настроек, которые имеют атрибуты `read-write`. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
drv_mgr set PROPERTY_NAME1 VALUE1 [PROPERTY_NAME2 VALUE2]
```

`PROPERTY_NAMEn`	имена настроек, значения которых нужно изменить
`VALUEn`	значения соответствующих настроек.

Рекомендации по использованию

Имена настроек указаны в Таблица 3 описания утилиты `drv_mgr`.

При успешной установке значения настройки будет выведено сообщение:

```
Value of "PROPERTY_NAME" is set to VALUE
```

При неуспешной установке значения настройки выводится сообщение:

```
Value of "PROPERTY_NAME" is not set to VALUE. Error:
ERROR_DESCRIPTION.
```

Значение настройки также записывается в конфигурационный файл `%PROD_DIR%\csp_ipsec_drv.cfg`, чтобы при запуске демона автоматически выставить его в IPsec-драйвере.

Редактировать этот конфигурационный файл без использования команды `drv_mgr set` нельзя.

13.14 drv_mgr reload

Команда `drv_mgr reload` загружает значения всех настроек IPsec-драйвера из конфигурационного файла `%PROD_DIR%\csp_ipsec_drv.cfg`. Эта команда имеет технологическое применение и используется для автоматической загрузки настроек IPsec-драйвера при запуске демона. Команда не предназначена для использования пользователем. Для работы с утилитой требуются права Администратора.

Синтаксис

```
drv_mgr reload
```

Редактировать конфигурационный файл нельзя. Установить новые значения настроек драйвера, записываемые в конфигурационный файл, можно только командой `drv_mgr set`.

При успешном завершении утилита возвращает значение 0.

13.15 fwconn_show

Команда `fwconn_show` предназначена для просмотра информации о TCP-соединениях, отслеживаемых при контекстной фильтрации трафика.

Синтаксис

```
fwconn_show [-detail] [-i conn_1_id]..[-i conn_n_id]
```

`-detail`	выдается подробная информация о соединениях. Для получения подробной информации о конкретном соединении необходимо указать опцию `-detail` перед `-i`.
`-i conn_n_id`	выдается информация по конкретному соединению с указанным идентификатором. Можно перечислить несколько соединений. В качестве идентификатора соединения допустимо указывать одно из двух чисел Connection ID, разделенных "/". Данные идентификаторы соединения также присутствуют в выводе утилиты `klogview` (группы сообщений FW, FR, FWTCP).

Пример

```
fwconn_show
Connection ID         Protected IP:port   Unprotected IP:port   State
0xd3e38180/0xd3e380c0 10.0.16.103:32779 -> 10.0.131.1:21     ESTAB/ESTAB
Number of TCP connections: 1
Number of established TCP connections: 1
```

где

Connection ID (0xd3e38180/0xd3e380c0) – идентификатор соединения (используется в fwconn_show и выводе klogview)

Protected IP:port (10.0.16.103:32779) – IP-адрес и порт, защищаемые firewall (обычно инициатор соединения)

-> – направление открытия соединения

State (ESTAB/ESTAB) – состояние TCP соединения для каждого из партнеров

Number of TCP connections (1) – общее число отслеживаемых TCP-соединений

Number of established TCP connections (1) – общее число отслеживаемых установившихся TCP-соединений.

```
fwconn_show -detail
Connection ID: 0xd3e38300/0xd3e38480
        Reverse connection: yes
        Protected side: 10.0.16.103:32780
                State: CLOSING
                Sequence number: 141965198
                Acknowlegement number: 1585098758
                Window size: 49232
                TTL left / TTL for current state: 27/30
        Unprotected side: 10.0.131.1:20
                State: CLOSING
```



```
                Sequence number: 1585098758
                Acknowlegement number: 141965198
                Window size: 5840
                TTL left / TTL for current state: 27/30
```

Дополнительные параметры, отображаемые при указании флага `-detail`:

Reverse connection (yes) – направление установления соединения – в данном случае соединения от 10.0.131.1:20 к 10.0.16.103:32780

Sequence number (141965198, 1585098758) – TCP sequence number для каждого их партнеров

Acknowlegement number (1585098758, 141965198) – TCP acknowlegement number для каждого из партнеров

Window size (49232, 5840) – размер TCP-окна для каждого из партнеров с учетом TCP window scaling1

TTL left[2] (27, 27) – время, через которое будет уничтожена запись о соединении, если не будет нового корректного пакета

TTL for current state (30, 30) – максимальное время хранения записи о соединении при отсутствии активности.

```
fwconn_show -detail -i 0xffff88003f99a100
```

```
Connection ID: 0xffff88003f99a100/0xffff88003f99a800
 Reverse connection: no
 Protected side: 5.5.5.5:35382
       State: CLOSING
       Sequence number: 3253957880
       Acknowlegement number: 2429155619
       Window size: 92
       TTL left / TTL for current state: 536/600
 Unprotected side: 6.6.6.6:21
       State: CLOSING
       Sequence number: 2429155619
       Acknowlegement number: 3253957880
       Window size: 91
       TTL left / TTL for current state: 536/600
```

[1] Возможна ситуация, когда firewall начинает отслеживать уже открытое соединение, не получая первых пакетов. В этом случае window scaling не учитывается.

[2] Запись о соединении уничтожается, если для любого из партнеров TTL Left достигает 0.

13.16 if_show

Команда `if_show` предназначена для просмотра логических, физических имен и других параметров сетевых интерфейсов, защищаемых Продуктом.

Синтаксис

`if_show [-all]`

`-all` на экран выдаются все логические имена интерфейсов.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра параметров всех сетевых интерфейсов.

Фильтрация по каждому логическому интерфейсу происходит независимо, так что один и тот же физический интерфейс может быть выдан в нескольких списках, соответствующих разным логическим именам.

Примечание 1:

В выводе команды параметр `State` показывает общее состояние интерфейса. Параметр `State` отображает состояние «головного» интерфейса, и считается, что состояние логических интерфейсов совпадает с состоянием «головного» интерфейса.

Пример

```
if_show
Logical network interface "default":
        Physical name template: "*"

        Physical name: eth{C4E2ACC3-F277-44D8-A0C1-F397DEF58D1B}
        State:         UP
        Index:         2
        MTU:           1500
        MAC addr:      00:0C:29:43:E2:42
        IP addr:       10.0.34.15 mask 255.255.255.0 brd 10.0.34.255
```


13.17 integr_mgr calc

Утилита `integr_mgr calc` используется для вычисления контрольной суммы указанного файла.

Синтаксис

```
integr_mgr calc -f filePath [-q]
```

`-f filePath`	имя файла (включая полный путь к нему), для которого будет вычисляться контрольная сумма
`-q`	запрет вывода текстовых результатов работы утилиты. Итоговый результат работы утилиты при использовании этой опции возможно узнать только из кода ошибки, возвращаемого утилитой. Допустимо указание ключа `-q` либо сразу после названия команды, либо в конце командной строки

Рекомендации по использованию

При вычислении контрольной суммы указанного файла будет создан файл с именем `filePath.hash`, содержащий значение контрольной суммы, которая в дальнейшем может применяться для контроля целостности файла.

Пример

Вычисляется контрольная сумма для файла `x509conv.ini`. В результате в том же каталоге, где расположен файл `x509conv.ini`, должен появиться файл `x509conv.ini.hash`:

```
integr_mgr calc -f x509conv.ini
  SUCCESS:  Operation was finished successfully
```


13.18 integr_mgr check

Утилита `integr_mgr check` применяется для проверки целостности отдельного файла или списка файлов. Утилиту можно использовать для проверки целостности файлов информационной части Продукта (изменяемых файлов в процессе настройки администратором).

.

Синтаксис

```
integr_mgr check -f filePath [-q]
integr_mgr check -l filePathList [-q]
```

`-f filePath`	имя проверяемого файла, включая полный путь к нему
`-l filePathList`	имя текстового файла со списком проверяемых файлов. Каждая строка данного файла – имя проверяемого файла с полным путем к нему
`-q`	запрет вывода текстовых результатов работы утилиты. Итоговый результат работы утилиты при использовании этой опции возможно узнать только из кода ошибки, возвращаемого утилитой. Допустимо указание ключа `-q` либо сразу после названия команды, либо в конце командной строки.

Рекомендации по использованию

В информационную часть Продукта входят каталог базы данных `db` и конфигурационные файлы, такие как:

```
agent.ini
s_logset.ini
syslog.ini
x509conv.ini
```

Все эти файлы лежат в каталоге Продукта, например, `C:\Program Files\S-Terra Client`. Значение контрольной суммы для каждого из этих файлов записано в файл с тем же именем, но с расширением `hash`, например, `s_logset.ini.hash`.

При запуске утилиты для одного файла вычисляется контрольная сумма заданного файла (`filePath)` и сравнивается полученное значение с контрольным значением в файле `filePath.hash` того же каталога.

При изменении данных файлов при помощи программных средств, предлагаемых Продуктом, пересчет контрольных сумм производится автоматически.

При изменении данных файлов вручную, без использования программных средств Продукта, необходимо пересчитать контрольную сумму измененного файла, запустив утилиту integr_mgr calc.

При проверке списка файлов работа утилиты не прерывается по первому несовпадению контрольной суммы, а также при любых других ошибках контроля целостности – ошибки доступа к файлу, отсутствие предварительно вычисленной контрольной суммы и прочих аналогичных ошибках. При каждой наступившей ошибке (если не указана опция `-q)` об этом выдаётся сообщение: имя обрабатываемого файла, код ошибки, расшифровка распространённых ошибок и проверка продолжается.
Опцию `-q` удобно использовать, если есть необходимость в вызове данной утилиты из какого-либо дополнительного скрипта.

Пример

Проверяется целостность файла `x509conv.ini:`

```
integr_mgr check -f x509conv.ini
SUCCESS:  Operation was finished successfully
```

13.19 key_mgr import

Команда `key_mgr import` предназначена для импорта предопределенных ключей из файловой системы в базу Продукта. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

key_mgr [-T timeout] **import** -n KEY_NAME -f KEY_FILE

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-n KEY_NAME	имя предопределенного ключа
-f KEY_FILE	путь к файлу, содержащему предопределенный ключ.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для регистрации предопределенных ключей в базе Продукта.

Пример

Пример импорта предопределенных ключей из файлов в базу Продукта:

```
key_mgr.exe import -f c:\certs\key1 -n key1 -f key2 -n key2name -f key3 -n
key3name
```

```
OK key1name
OK key2name
OK key3name
```

13.20 key_mgr remove

Команда `key_mgr remove` предназначена для удаления предопределенных ключей из базы Продукта. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

key_mgr [-T timeout] **remove** -n KEY_NAME

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-n KEY_NAME	имя предопределенного ключа.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для удаления предопределенных ключей из базы Продукта.

Пример

Ниже приведен пример удаления предопределенного ключа:

```
key_mgr remove -n key1name
  OK key1name
```

13.21 key_mgr show

Команда `key_mgr show` предназначена для получения информации о предопределенных ключей, зарегистрированных в Продукте.

Синтаксис

`key_mgr` `[-T timeout]` **`show`**

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра списка предопределенных ключей в базе Продукта.

При выполнении этой команды будут выводиться следующие данные:

- количество предопределенных ключей
- для каждого ключа:
  - имя ключа
  - тело ключа в печатном виде. Если тело ключа содержит непечатные символы, то при выводе в печатном виде они заменяются на `'.'` (символ точка).
  - тело ключа в hex-представлении.

Пример:

`key_mgr show`

```
Found #1 keys.
----Key----
Name   :        key1
Content         testkey1..
```

13.22 key_mgr list

Команда `key_mgr list` предназначена для просмотра списка предопределенных ключей, зарегистрированных в Продукте.

Синтаксис

`key_mgr` `[-T timeout]` **`list`**

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра списка предопределенных ключей в базе Продукта.

При выполнении этой команды будут выводиться следующие данные:

- количество предопределенных ключей
- для каждого ключа:
  - имя ключа

Пример:

`key_mgr list`

```
Found #3 keys.
--[Key]--------------
Name         :  key1
--[Key]--------------
Name         :  key2name
--[Key]--------------
Name         :  key3name
```

13.23 klogview

Утилита `klogview` предназначена для просмотра сообщений, выдаваемых системой протоколирования IPsec-драйвера.

Синтаксис

```
klogview [-ltTg] [-p ts_precision][-m event_mask] [-f event_mask]
```

`-l`	ожидать сообщения из ядра и выводить их по мере поступления. Эта опция принимается по умолчанию, если не задана опция `-m`.
`-t`	печатать дату и время вывода сообщения
`-T`	печатать относительное время, когда произошло событие. Время выводится в секундах относительно последнего произошедшего события (а не по времени вывода), показанного данным экземпляром утилиты. Например, значение 10.353245 – это 10 секунд и 353245 микросекунд. Максимальная точность – наносекунды, но реальная погрешность зависит от аппаратной платформы и операционной системы. Значение, выдаваемое с первым сообщением, отображает абсолютное значение часов, которое используется для вычисления относительного времени. Абсолютное значение – это либо время со старта системы, либо время относительно какой-то даты, принятой в данной системе за точку отсчета. Возможны отрицательные значения. Время, указанное в событии, относится к началу формирования сообщения, а при параллельном формировании сообщений порядок их отправки не определен
`-g`	печатать перед сообщением в квадратных скобках идентификатор группы событий. Идентификатор группы поясняет, к какому разделу относится данное событие. При выборе фильтра, когда выводится множество сообщений различных разделов, без идентификатора трудно соотнести раздел и сообщение
`-p ts_precision`	количество знаков долей секунд, используемых при печати относительного времени события (`-T`)
`-f event_mask`	задать фильтр событий для данного экземпляра утилиты. Возможные события описаны в таблице
`-m event_mask`	задать фильтр событий по умолчанию. Заданное значение используется, если не указана опция `-f`
`-h`	вывести краткую информацию об использовании утилиты.

В настоящий момент утилита может выводить сообщения, относящиеся к одной или нескольким группам событий. События, по которым выводятся сообщения, сгруппированы двумя способами:

- группировка событий по подсистеме – сообщения, относящиеся к одной подсистеме. Например, PKT – события, относящиеся к подсистеме, реализующей логику обработки пакетов
- группировка событий по маске – позволяет выбирать сообщения более детально. Подсистема может использовать несколько масок событий. Например, PKT включает маски pass и drop.

Группировка событий по маске

Таблица 4

Группа событий	Код	Описание
drop	0x2	Уничтожение пакета. Выводится непосредственно перед уничтожением какого-либо пакета. Сообщение содержит краткий текст, поясняющий причину уничтожения и информацию из IP-заголовка пакета. В некоторых случаях IP-заголовок может быть испорчен к моменту вывода сообщения, тогда в сообщении допускаются нулевые или любые другие случайные адреса.
pass	0x1	Пропуск пакета. Выводится непосредственно перед отсылкой какого-либо пакета. Сообщение содержит краткий текст, поясняющий действия, которые были произведены над пакетом.
sa_minor	0x8	Некоторые внутренние события, происходящие с IPsec - контекстом. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста.
sa_major	0x4	Взаимодействия между IPsec-драйвером и приложением, касающиеся изменения состояния IPsec-контекстов. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста.
sa_trace	0x10	Сообщения выводятся перед попыткой применения к пакету IPsec-контекста.
sa_errors	0x20	Ошибки, связанные с неуспешным применением IPsec-контекста к пакету.
fw_trace	0x80	Результат поиска правил firewall для пакета (если поиск производился). Сообщения, выбираемые fw_trace, включают все сообщения fw_notif.
fw_notif	0x100	Выводятся при применении правила firewall к пакету, если правило помечено в LSP.
fw_obj	0x200	Действия, производимые над правилами firewall (добавление, удаление). Идентификаторами правил являются числа двух типов. В десятичном виде выводятся идентификаторы, загружаемые из vpnsvc. В шестнадцатеричном виде (с префиксом 0x) выводятся идентификаторы динамических правил контекстной фильтрации.
vif_obj	0x400	Изменения конфигурации сетевого интерфейса (vif).
fw_tcpst	0x800	Изменения записи о состоянии TCP соединения (tcp state), ошибки и другие события контекстной фильтрации TCP. Включает все сообщения fw_tcpstat и fw_tcperr. Для идентификации сессий используются два числа (0x....), каждое из которых соответствует записи о состоянии партнера по TCP-соединению. Эти же числа являются идентификаторами соответствующих правил фильтрации в сообщениях групп fw_obj, fw_trace.
fw_tcpstat	0x1000	Вывод статистики после закрытия TCP сессии, если правило помечено в LSP.
fw_tcperr	0x2000	Вывод ошибок, связанных с контекстной фильтрацией TCP-соединения, если правило помечено в LSP.
mtud	0x4000	Действия, связанные с path mtu discovery (отсылка и обработка ICMP сообщений, ошибки). В сообщениях выводятся оригинальные заголовки пакетов, даже если к пакету применялся IPsec. Внешний заголовок можно увидеть в соответствующих сообщениях pass/drop.

Группировка событий по подсистемам

Обозначение подсистемы	*Описание*[3]
LOG	Сервисные сообщения подсистемы протоколирования. Их прием нельзя включить или отключить
SA	Работа с IPsec SA в ядре
IPSEC	Работа протоколов IPsec
PKT	Основная логика обработки пакетов
FW	Фильтрация трафика
FR	Действия над правилами фильтрации трафика
FWTCP	Контекстная фильтрация TCP
MTUD	Работа path mtu discovery
VIF	Действия над описаниями виртуальных сетевых интерфейсов.

Нужный набор событий (event_mask) можно указать перечислением масок событий через запятую (пробелы при перечислении не допускаются). Маска может быть задана численным значением, именем (из таблицы «Группировка событий по маске») или именем подсистемы (из таблицы «Группировка событий по подсистемам»).

Примеры (все перечисленные команды эквивалентны):

```
klogview -f 0x1f
klogview -f 31
klogview -f drop,pass,sa_minor,sa_major,sa_trace
klogview -f PKT,SA,sa_trace
klogview -f drop,1,SA,0x10
```

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра сообщений, выдаваемых системой протоколирования.

[3] Соответствие масок подсистемам можно увидеть в подсказке утилиты klogview.

Сообщения, выводимые утилитой

Сообщения, выводимые утилитой, формируются на основе данных, присылаемых из IPsec-драйвера. Структура большинства сообщений определяется строкой формата[4], получаемой из IPsec-драйвера (см. Примеры сообщений).

Сервисные сообщения, выводимые утилитой:

`*** N messages lost ***`	выводится, если утилита не успевает обрабатывать сообщения и N сообщений поретяны.
`no format string`	в сообщении отсутствует строка формата[5].
`<error: ..`	в выводимом сообщении несоответствие строки формата параметрам сообщения[6].

Приведем список сообщений, которые выводятся системой протоколирования IPsec-драйвера для разных групп событий.

13.23.1 События группы pass и drop

Сообщения для этой группы выводятся непосредственно перед уничтожением или отправкой пакета.

Формат сообщения (в порядке следования):

- входящий или выходящий пакет
- IP-адрес источника
- порт источника
- IP-адрес получателя
- порт получателя
- номер IP-протокола
- длина IP-пакета
- логическое имя интерфейса или код интерфейса, если имя неизвестно
- действие "`passed`" или "`dropped`"
- строка, описывающая причину уничтожения или отправки пакета.

По возможности выводится дополнительная информация, например, имя правила фильтрации и идентификатор SA.

Примеры сообщений группы pass

Пакет обработан по правилу фильтрации с действием `PASS`:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: filtered
```

Пакет был обработан по `IPsec`-правилу:

```
passed in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
decapsulated
passed out packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0:
encapsulated
```

[4] Строка формата по смыслу и стилю похожа на форматную строку в printf.

[5] Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.

[6] Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.

Пакет был отправлен в IP-стек для маршрутизации:

```
passed out packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0:
re-routed
```

Пакет был пропущен в соответствии с конфигурацией драйвера по-умолчанию (пользовательская конфигурация не загружена):

```
passed out packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0:
driver default policy
```

Примеры сообщений группы drop

Сообщения, связанные с некорректными данными заголовков пакета:

IP-заголовок испорчен:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
corrupted IP header
```

TCP/UDP заголовок испорчен:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
corrupted protocol headers
```

Следующее сообщение аналогично "corrupted protocol headers", выводится после сборки (реассемблирования) IP-пакета:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
corrupted protocol headers after reassembly
```

Испорченные заголовки после раскрытия IPsec, это может быть также связано с использованием неверного ключа для расшифровки при отсутствии проверки целостности:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: SA
33: corrupted protocol headers after decapsulation
```

Испорчен ESP или AH заголовок:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
unable to fetch SPI
```

Превышено ограничение по количеству вложений IPsec, раскрываемых на одном хосте (допускается не более 16 вложений):

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0:
too many nested encapsulations
```

Превышено ограничение по количеству вложений IPsec, применяемых на одном хосте (допускается не более 16 вложений), предположительно конфигурация написана таким образом, что пакет зациклился:

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0:
too many nested encapsulations (recursive policy?)
```

Сообщения о подпадании пакета под правило с действием `DROP`:

Пакет уничтожен на этапе фильтрации

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
firewall
```

Пакет уничтожен на этапе проверки IPsec-фильтров.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: IPsec
policy
```

Пакет уничтожен на этапе проверки фильтров, связанных с IPsec-правилом.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0: SA
filter
```

Пакет уничтожен на этапе классификации.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0:
classification
```

Сообщения, связанные с несоответствием входящего пакета локальной конфигурации IPsec. Появление подобных сообщений может быть вызвано двумя причинами:

- несогласованные конфигурации[7] партнеров по IKE/IPsec соединению
- попытка атаки на защищенную сеть.

Пакет был закрыт с помощью IPsec, но подпадает под правило `PASS`:

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
filter 12: IPsec packet is not expected
```

Открытый пакет подпадает под правило фильтрации с IPsec-действием:

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
filter 12: packet must be protected with IPsec
```

При вложенной IPsec-инкапсуляции входящий пакет имеет недостаточное количество слоев IPsec-защиты:

```
dropped in packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0: packet
lacks required IPsec layer
```

Туннельный (внешний) заголовок не соответствует параметрам SA.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
tunnel header doesn't match SA 24
```

Пакет пришел не с того сетевого интерфейса.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: SA 18
is bound to filter which doesn't match current vif
```

Маловероятная ошибка, может произойти в процессе удаления SA в момент обработки пакета.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: SA 3
is not in a bundle
```

При вложенном IPsec пакет порядок применения слоев IPsec некорректный.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: SA 3
is not the first SA in a bundle
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: SPI
0xfa849e11 is not found in SA bundle
После декапсуляции заголовок пакета не соответствует селектору SA.
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: SA
33: decapsulated packet's IP header doesn't match the SA
```

Неизвестный SPI (IPsec SA не найден).

```
dropped in packet 2.3.4.5->3.4.3.3, proto 50, len 140, if eth0: SPI
0xabababab not found in hash
```

SA не привязан к IPsec-фильтру, под который подпадает пакет.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
filter 12: IPsec SA doesn't match
```

Для исходящего пакета, попадающего на IPsec-фильтр, не создан SA bundle, при этом автоматическое создание SA для данного фильтра запрещено (fallback_action = DROP).

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
filter 12: SA bundle not found
```

[7] Рассогласование может произойти "в динамике" - то есть когда один из партнеров находится в процессе конфигурирования, или параметры, которые должны согласовываться автоматически (например, IPsec SA), были рассинхронизированы из-за потерь пакетов или обрыва сетевого соединения.

Ошибки IPsec:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0: SA
33: decapsulation error 5: integrity verification failed
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: SA
33: encapsulation error 4: sequence number wrapped
```

Возможные ошибки представлены ниже.

Таблица 5

Код	Название	Описание проблемы
1	replay packet detected	обнаружен повторный пакет
2	call to crypto subsystem failed	ошибка крипто-подсистемы
3	last sequence number	последний номер пакета
4	sequence number wrapped	переполнение счетчика пакетов
5	integrity verification failed	проверка целостности не прошла
6	corrupted protocol headers	испорченный протокольный заголовок
7	corrupted headers after decapsulation	испорченный протокольный заголовок после декапсуляции
8	memory allocation failed	невозможно выделить память
9	IP ttl expired	счетчик IP ttl истек
10	buffer is too small[8]	буфер слишком мал
11	can't parse IP options	невозможно разобрать опции IP
12	padding check failed	ошибка в заполнителе
13	incorrect SA configuration[9]	неправильная конфигурация SA
14	wrong encapsulation mode for the SA	несоответствующий SA режим инкапсуляции (транспорт или туннель)
15	packet length exceeds 64K-1	длина пакета превышает максимально допустимую
16	TFC packet	TFC пакет
17	traffic limit exceeded	превышение ограничения по трафику
18	wrong tunnel source address	несоответствующий SA адрес источника в туннельном заголовке

[8] Это является внутренней ошибкой, просьба сообщать разработчикам.

9 Тоже внутренняя ошибка, просьба сообщать разработчикам.

Промежуточное состояние при IPsec-rekeying (процесс rekeying (смена ключевого материала) не успел завершиться вовремя):

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: SA
18 is unusable
```

Ограничение на обработку транзитного трафика:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
packet is not local (not a security gateway)
```

Ограничение на обработку транзитного трафика только для IPsec пакета:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
decapsulated packet is not local (not a security gateway)
```

Очередь пакетов, ожидающая создания IPsec SA bundle переполнена (размер очереди задается в LSP, по умолчанию 8):

```
dropped out packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0:
filter 12: reached limit of 8 packets waiting for SA
```

В случае, если произойдет ошибка при построении SA bundle, для ожидающих пакетов будет выдано:

```
dropped out packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0:
filter 12: failed to build SA bundle
```

Превышено общее количество одновременно выполняющихся запросов[10] на создание SA (размер очереди по умолчанию 1000):

```
dropped out packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0:
reached limit of 1000 SA requests
```

Превышено количество одновременно выполняющихся запросов[11] на создание SA по одному фильтру (размер очереди задается в LSP, по умолчанию 8):

```
dropped out packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0:
reached limit of 8 SA requests for filter 12
```

Следующее сообщение говорит о слишком большом количестве пакетов на обработку одним SA (более 40). Скорее всего, это означает неоптимальные настройки Продукта с точки зрения производительности. Просьба обращаться к разработчикам:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: SA
33: queue overflow
```

Пакет после обработки IPsec может превысить максимальную длину IP. То есть к такому пакету IPsec не применим:

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 65530, if eth0:
packet is too large for IPsec, length after encapsulation 65550
```

Внутренние ошибки, о которых просьба сообщать разработчикам:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: ip
data is not 4-byte aligned
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
unknown network interface
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
unknown physical network interface
```

Пришел пакет ICMP destination unreachable/fragmentation needed, который обработан драйвером и далее не пропущен.

```
dropped in packet 2.3.4.5->3.4.3.3, proto 1, len 80, if eth0: ICMP PMTUD
message processed
```

[10] Ограничение касается только запросов, инициатором которых является драйвер.

[11] Ограничение касается только запросов, инициатором которых является драйвер.

Следующие сообщения связаны с тем, что драйвер находится в режиме конфигурирования, и прохождение пакетов заблокировано.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
driver is being configured
```

Следующее означает, что с момента начала обработки пакета, конфигурация драйвера изменилась, и нельзя гарантировать правильность обработки данного пакета.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
packet config id 11 don't match current id 12
```

IPsec-фильтр был уничтожен в процессе обработки пакета.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
IPsec filter 13 is dead
```

Сообщения о нехватке ресурсов.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
filter 12: failed to send SA request: out of memory
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: can't
allocate packet buffer
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
can't prepare SA list: out of memory
```

Исходящие пакеты, отправляемые с виртуального сетевого интерфейса, обязательно должны быть отправлены с использованием туннельного режима IPsec и адрес туннельного заголовка должен отличаться от изначального.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: IP
destination have not been changed for a packet which had come from
IKEcfg virtual interface
```

Исходящие пакеты, отправляемые с виртуального сетевого интерфейса, обязательно должны в качестве адреса источника иметь адрес этого виртуального интерфейса.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: IP
source address is not an address of IKEcfg virtual interface
```

Пакет превышает MTU и не может быть фрагментирован из-за выставленного DF bit.

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: DF
bit set, can't fragment packet, path MTU 1500
```

Ошибка при попытке фрагментировать пакет.

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
can't fragment packet, path MTU 1500
```

13.23.2 События группы fw_trace, fw_notif

Сообщения этой группы позволяют определить, какое правило фильтрации используется для обработки пакета. За время обработки один пакет может проходить по нескольким спискам (например, фильтрация и классификация). Поскольку интенсивность сообщений `fw_trace` может быть очень высокой, `fw_notif` позволяет ограничить их число, получая сообщения только для правил, помеченных в LSP. Параметры пакета выводятся аналогично сообщениям `pass/drop`.

Примеры сообщений:

Найден фильтр, результат фильтрации в конце сообщения. Возможны следующие результаты фильтрации: PASS – пропустить пакет, ASSEMBLE – необходима сборка пакетов из фрагментов, DROP – уничтожить пакет, ERROR – ошибка обработки пакета (испорченный пакет, или нехватка ресурсов для обработки), MATCH – промежуточное состояние при фильтрации (фильтр подобран, но действие еще не определено).

```
filtration result for in packet 10.0.59.1:1680->12.1.1.1:23, proto 6,
len 80, if eth0: chain 10, filter 12, event id some_ftp_filter, status
PASS
```

Отсутствие подходящего фильтра в цепочке.

```
filtration result for in packet 10.0.59.1:1680->12.1.1.1:23, proto 6,
len 80, if eth0: chain 10: no match
```

Переход к другой части цепочки фильтрации (при использовании Filter.Label в LSP).

```
intermediate filtration result for in packet 10.0.59.1:1680-
>12.1.1.1:23, proto 6, len 80, if eth0: chain 10, filter 12, event id
some_ftp_filter, status MATCH, jump to 18
```

Ошибка в структуре цепочки фильтрации, просьба сообщать разработчикам о появлении.

```
filtration result for in packet 10.0.59.1:1680->12.1.1.1:23, proto 6,
len 80, if eth0: chain 10, filter 12: next filter 16 not found
```

13.23.3 События группы sa_minor, sa_major

Сообщения этой группы позволяют контролировать процессы создания, уничтожения и замены IPsec-контекстов. Сообщения о загрузке контекстов содержат детальную информацию о параметрах контекста, включая IP-параметры (адреса, порты), SPI, режимы и др.

Если сообщение содержит IP-параметры (selector), то они выводятся в следующем порядке:

- локальный адрес/диапазон адресов
- локальный порт
- удаленный адрес/диапазон адресов
- удаленный порт
- IP- протокол.

Под локальным адресом понимается адрес источника (source) для исходящих пакетов.

Примеры сообщений группы sa_major

Превышено ограничение SA по трафику:

```
SA 55 expired
```

Пора начинать rekeying SA (пройден барьер по трафику):

```
requesting rekeying for SA 33
```

Сообщения о загрузке новых SA:

```
loaded SA 12: flags 0x1, IPsec flags 0x18, selector 5.4.3.2->2.3.4.5,
tunnel 5.4.3.2->8.9.1.2, type 51, SPI 0xabababba
```

Следующее сообщение говорит о замене IPsec SA без прерывания обработки трафика:

```
loaded replacement for SA 55: SA 69: flags 0x0, IPsec flags, 0x38,
selector 3.4.5.1->2.3.4.0-2.3.4.255 proto 17, tunnel 3.4.5.1->1.3.4.1,
type 50, SPI 0x3b7f44e0
```

Расшифровка type:

```
51 – AH
50 - ESP
```

Расшифровка некоторых[12] битов flags:

```
0x1 – входящий
0x100 - включен path MTU discovery
0x200 - включена повторная маршрутизация (reroute)
```

[12] Остальные значения флагов не предназначены для интерпретации пользователями.

```
0x400 - необходима сборка IP-пакетов из фрагментов перед
инкапсуляцией
```

Расшифровка битов `ipsec flags`:

```
0x1 – туннельный режим
0x2 – сбрасывать DF-bit
0x4 - устанавливать DF-bit
0x8 – включена защита от replay-атак
0x10 – включена проверка целостности
0x20 – включено шифрование
0x40 – испольуется UDP-encapsulation (NAT traversal)
```

Загрузка связки SA (SA bundle):

```
loaded bundle: chain 12, filter 98, flags 0x0, selector 3.4.5.1:98-
>3.4.5.2:99 proto 17, SA list 4 5
```

Расшифровка битов flags:

```
0x1 - пакеты, которые ожидают обработки данным SA bundle, должны
быть уничтожены
```

```
0x2 - источником запроса на создание SA bundle был драйвер
```

Сообщение о загрузке SA bundle, не содержащее списка SA, означает ошибку создания SA bundle приложением (демоном).

Запрос SA bundle (обычно для его обработки требуется IKE-обмен):

```
SA request: filter chain 59, filter 12, selector 5.4.3.2:1->1.2.3.4:5
proto 17, expected SA selector 5.4.3.2->1.2.3.4 proto 17
```

Пакет ожидает SA bundle.

```
waiting for SA: 10.0.59.1:1680->12.1.1.1:23, proto 17, len 90, if eth0
```

SA заблокирован (превышено ограничение по времени/трафику), ожидается завершение процесса rekeying:

```
disabled SA 33
```

Удаление SA:

```
removed SA 33
```

Пришло подтверждение загрузки SA у партнера, SA активируется:

```
application request to enable SA 33 processed
```

Автоматическое обновление SA приостановлено из-за отсутствия трафика, но при первом пакете начнется смена ключей (обновление SA).

```
first packet will trigger rekeying of SA 33
```

Сообщения, возникающие при ошибочном/странном[13] поведении Продукта:

```
can't add bundle: filter id 299 is not found in chain 11
can't add bundle: SA id 33 not found
can't load SA: unable to unpack
can't load replacement for SA 33: SA not found
can't load replacement for SA 33: can't unpack
can't remove SA 33: sa not found
can't disable SA 33: sa not found
can't enable SA 33: sa not found
rekey trigger: can't find SA 33
can't add bundle: non-empty "drop" response
can't add bundle: illegal request size 11
can't add bundle: filter id 2 in chain 2 is not an IPsec filter
can't add bundle: filter chain id 22 is empty
```

[13] Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

```
can't add bundle: filter chain id 22 not found
can't add bundle: filter id 23, chain 18: request 1.2.3.4->4.3.2.1 not
found
can't add bundle: filter 80 is dead
can't add bundle: SA 24 is already in a bundle
```

Примеры сообщений группы sa_minor[14]

```
destroyed SA 12
replacing SA 12 with SA 13
can't enable sa 13: it's already enabled
enabled sa 14, but didn't activate it
enabled sa 15
```

13.23.4 События группы sa_trace

Сообщения группы `sa_trace` позволяют увидеть факт применения IPsec-контекстов к пакету. Для исходящих пакетов – это инкапсуляция, для входящих – декапсуляция. Сообщения содержат идентификатор SA, который выводится при загрузке SA (должны быть включены сообщения группы `sa_major`). Информация о пакете выводится в том же порядке, что и для сообщений группы `pass` и `drop`.

Примеры сообщений:

```
decapsulating with SA 10: 1.2.3.4:5->5.4.3.2:1, proto 6, len 256, if
iprb0
encapsulating with SA 10: 5.4.3.2:1->1.2.3.4:5, proto 6, len 256, if
iprb0
```

13.23.5 События группы sa_errors

Сообщения этой группы выводят дополнительную информацию о специфических ошибках IPsec.

В данный момент есть только одно сообщение – о детектировании replay-атаки. Выводится состояние окна, номер пакета (sequence number).

Пример сообщения:

```
replay packet detected: SA 10 last sequence number 92, window 0x1,
packet sequence number 4.
```

13.23.6 События группы fw_tcpst, fw_tcperr, fw_tcpstat

События группы fw_tcperr

Вывод сообщений данной группы зависит от конфигурации (LSP). Для правила фильтрации, с которым связано событие, должно быть включено протокорирование. Если включена группа `fw_tcpst`, то сообщения выводятся независимо от LSP.

Примеры сообщений:

```
half open session count and creation rate are ok, stopped deleting
connections: count 2 (< 10), 1-minute rate 9 (< 10)
half open sessions limit triggered by 1.1.1.2:23->1.1.1.3:1045, starting
to delete connections: count/max 22/33, 1-minute rate/max 42/42
```

[14] Сообщения данного раздела предназначены для внутреннего использования. Расшифровка пользователям Продукта не предоставляется.

```
sessions limit triggered by 1.1.1.2:23->1.1.1.3:1045, dropping packet:
session count/max 4000/4000
blocked attempt to initiate FTP passive-mode data connection 0x%#5x
(%#1,a:%,2u->%,a:%,2u) from server side
blocked attempt to initiate FTP data connection 0x%#5x (%#1,a:%,2u-
>%,a:%,2u) from client side
blocked FTP PASV response for 0x%#5x (%#1,a:%,2u->%,a:%,2u): user not
authenticated
blocked attempt to use priveleged port %#6d in FTP PASV response for
0x%#5x (%#1,a:%,2u->%,a:%,2u)
blocked FTP PORT command for 0x%#5x (%#1,a:%,2u->%,a:%,2u): user not
authenticated
blocked attempt to use priveleged port %#6d in FTP PORT command for
0x%#5x (%#1,a:%,2u->%,a:%,2u
```

Дополнительные сообщения от stateful firewall:

TCP sequence number не попадает в TCP window (см. описание TCPStrictnessLevel в LSP). Сообщение может быть связано как с намеренным искажением TCP заголовка так и с ограниченными возможностями по отслеживанию соединений в firewall.

```
unexpected TCP sequence number for 0xfafabebe, dropping packet: seq
1040, flags 0x10, expected seq (ack) 4050, win 1024
```

TCP флаги не соответствуют состоянию соединения (см. описание TCPStrictnessLevel в LSP). Сообщение может быть связано как с намеренным искажением TCP заголовка так и с ограниченными возможностями по отслеживанию соединений в firewall.

```
unexpected TCP flags for 0xfafabebe, dropping packet: disallowed state
change ESTAB->SYNSENT/ESTAB->ESTAB, TCP flags 0x2
```

Смена состояния TCP-соединения. ttl – время, через которое запись о соединении удалится при отсутствии активности. Время отслеживается для каждого из партнеров отдельно, но запись будет удалена по истечении любого из таймаутов. Состояния отображаются как старое->новое.

```
session state changed for 0xfafabebe: state ESTAB->ESTAB/SYNRCVD->ESTAB,
ttl 100/100, TCP flags 0x10
```

В соответствии с LSP запрещено открытие TCP-стейтов, для соединений, которые открылись раньше сброса конфигурации firewall (см. описание TCPStrictnessLevel в LSP).

```
not a SYN packet, won't create state for session 10.1.1.1:22-
>10.2.2.2:3532, parent filter 8: TCP flags 0x10
```

Открытие новой записи о TCP соединении.

```
new session 0xbebebebe/0xabababab (1.2.3.4 1.2.3.4:32 32->2.3.4.1
2.3.4.1:33 33): parent filter 18, state SYNSENT/CLOSED, TCP flags 0x2)
```

Невозможно создать новую запись о соединении из-за ограничений на количество установившихся (established) соединений. Неустановившихся соединений для удаления нет.

```
can't delete any old half open session in favor of new session 1.2.3.4
1.2.3.4:32 32->2.3.4.1 2.3.4.1:33 33, dropping packet: half open session
count 0
```

События группы fw_tcpstat

Для правила фильтрации, с которым связано событие, должно быть включено протокорирование. , то сообщения выводятся независимо от LSP.

Пример сообщения:

```
session 0x12345678x/0x12346678 (1.1.1.2:23->1.1.1.3:1045) closed: state
CLOSED/CLOSED, transferred 200/100 bytes, 10/15 packets
```

13.23.7 События группы fw_obj

В данные группы включены сообщения об изменении состава цепочек фильтрации, изменения состояния индивидуальных фильтров. Назначение цепочки фильтрации зависит от того, в каком качестве она подключена к виртуальному интерфейсу. С точки зрения сообщений о состоянии, все цепочки (фильтрация, классификация, IPsec) – одинаковы.

Изменение состояние фильтров и цепочек правил фильтации (аналог FilterChain в LSP). Четные номера цепочек используются для исходящих пакетов. Идентификатор фильтра отображается десятичным числом для фильтров, загружаемых из приложения, шестнадцатеричным числом с префиксом 0x для фильтров, создаваемых динамически внутри драйвера.

Примеры сообщений:

Создание цепочки правил фильтрации:

```
created filter chain 18
```

Удаление цепочки правил фильтрации:

```
destroyed filter chain 18
```

Удаление фильтра из цепочки по инициативе приложения:

```
unloaded filter 12 from chain 18
```

Групповое удаление фильтров из цепочки по инициативе приложения:

```
unloaded 9 filters with parent id 19 from chain 18
```

Включение фильтра или фильтров (в соответствии с графиком, см. LSP, Schedule):

```
enabled filter 4 from chain 9
enabled 9 filters with id 8 from chain 9
```

Выключение фильтра или фильтров (в соответствии с графиком, см. LSP, Schedule):

```
disabled filter 4 from chain 9
disabled 9 filters with id 8 from chain 9
```

Уничтожение фильтра:

```
destroyed filter 19
```

Создание фильтра:

```
created filter 8, chain 4, selector 1.2.3.4 1.2.3.5->9.1.1.1 9.1.1.1
pkttype 4, position at head, action 0x0, nextid 12
```

Селектор (`selector`) фильтра определяет адресную информацию пакетов, к которым будет приминяться действие данного фильтра. Селектор содержит IP-адреса и порты в формате source -> destination, номера IP-протоколов – эти значения всегда выдаются в виде перечисления диапазонов. Так значение 1.2.3.8 1.2.3.11 1.3.3.3 1.3.3.3 – это диапазон 1.2.3.8..1.2.3.11 и единичный адрес 1.3.3.3

`Pkttype` битовая маска из следующих знчачений (описание значений есть в LSP, PacketType): 1 – LOCAL_UNICAST, 2 – LOCAL_BROADCAST, 4 – LOCAL_MISDIRECTED, 8 – TRANSIT

`Nextid` переход к другому фильтру, если произошло совпадение с данным фильтром

`Position` в какое место цепочки фильтр будет вставлен

`action` битовая маска действий, которые связаны с совпадением данного фильтра: 2 – уничтожить пакет, 4 – пакет помечен для получения сообщений группы fw_notif, 32 – фильтр загружен в отключенном состоянии в соответствии с графиком (Schedule).

Остальные значения для внутреннего использования, пользователю описание не предоставляется.

Следующие сообщения отражают изменения объекта frcp (пара цепочек правил фильтрации), который предназначен для фильтрации трафика в обоих направлениях. В состав frcp может входить одна цепочка правил, в случае симметричной фильтрации (например, IPsec) или две. Идентификатор frcp совпадает с идентификатором цепочки фильтров для исходящих пакетов.

Удаление пары цепочек правил фильтрации:

```
destroyed filter chain pair 18
```

Удаление пары цепочкек правил фильтрации из списка доступных (после этого нельзя будет заново подсоединить эту цепочку к виртуальному интерфейсу). Обычно данное действие делается непосредственно перед удалением chain pair.

```
deregistered filter chain pair 18
```

Создание пары цепочкек правил фильтрации.

```
created filter chain pair 8, type 1, visibility 1
```

Значения visibility: 1 – объект доступен для изменения из приложений, 0 – внутренний объект драйвера.
Значения type: 1 – зависимые цепочки (для контекстной фильтрации), 2 – независимые цепочки (простая пакетная фильтрация), 3 – симметричная фильтрация (используется одна цепочка, адресная информация в пакете переворачивается в зависимости от направления)

Сообщения, возникающие при ошибочном/странном[15] поведении продукта:

```
can't load filter: chain 13 is not found
can't load filter: can't create chain 13
can't load filter to chain 13: unable to unpack
can't create filter chain pair 19, type 1, visibility 1: odd id
can't create filter chain pair 8, type 1, visibility 1: out of memory
can't create filter chain pair 4, type 1, visibility 1: can't create
chains
can't deregister filter chain pair 4: not found
can't load filter 18 to chain 13
can't unload filter 18: chain 13 is not found
can't unload filter 18: chain 13 is not initialized
can't unload filter 18 from chain 84: filter is not found
can't disable filter 18: chain 13 is not found
can't disable filter 18: chain 13 is not initialized
can't disable filter 18 from chain 13: filter is already disabled
can't disable filter 18 from chain 13: filter is not found
can't enable filter 18: chain 13 is not found
can't enable filter 18: chain 13 is not initialized
can't enable filter 18 from chain 13: filter is already enabled
can't enable filter 18 from chain 13: filter is not found
can't add filter to chain 13: chain is being destroyed
can't add filter to chain 13 next to filter 8: filter not found
```

13.23.8 События группы vif_obj

В данную группу включены сообщения об изменении состояния виртуальных (vif) и реальных (phy) сетевых интерфейсов.

Примеры сообщений об изменении состояния сетевого интерфейса ОС:

Параметр `flags` отображает следующие состояния:

I – для данного интерфейса имеется информация о конфигурации IP (IP адрес, маска, MTU)

[15] Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

P – интерфейс доступен для перехвата пакетов

V – интерфейс подключен к соответствующему виртуальному интерефейсу.

Изменение статуса интерфейса (частичное отключение, см. flags выше):

```
updated phy "eth0": cleared flags I: PIV>PV
```

Получение IP-информации:

```
updated phy "eth0": id 2, flags PV>PIV, mtu 1500, addresses 1.2.3.4
2.2.3.4, broadcasts 1.2.3.255 2.2.3.255
```

Подключение к виртуальному интерфейсу:

```
updated phy "eth0": flags P>PV, vif 9 "FastEthernet0/1"
```

Появление информации об интерфейсе в перехватчике пакетов:

```
updated phy "eth0": flags I>PI: interface appeared in pcap
```

Создание записи о сетевом интерфейсе:

```
created phy "eth0": phy id 2, flags P
```

Уничтожение записи о сетевом интерфейсе:

```
destroyed phy "eth0"
```

Создание записи о виртуальном интерфейсе по инициативе приложения:

```
created vif 7 "FastEthernet0/1"
```

Подключение цепочки фильтрации:

```
attached filter chain pair 4 to vif 19, chain type 4
```

Расшифровка `type`:

0 – firewall, исходящие пакеты

1 – firewall, входящие

2 – классификация, исходящие

3 – классификация, входящие

4 – IPsec

Включение виртуального интерфейса в общем списке (после этого действия к виртуальному интерфейсу подключаются сетевые интерфейсы ОС):

```
registered vif 11 "FastEthernet0/0": pname "eth0", priority 30
```

`pname` – шаблон имен сетевых интерфейсов ОС

`priority` – приоритет: если для сетевого интерфейса ОС по шаблону `pname` подходит несколько виртуальных, выбирается тот, у которого значение `priority` больше

Уничтожение записи о виртуальном интерфейсе.

```
destroyed vif 7 "FastEthernet0/4"
```

Отключение цепочки фильтрации:

```
detached filter chain pair 2 from vif 9, chain type 8
```

Отключение виртуального интерфейса:

```
deregistering vif 3 "FastEthernet0/1"
```

Сообщения, возникающие при ошибочном/странном[16] поведении продукта:

```
can't attach filter chain pair 2 to vif 3: vif is not found
can't attach filter chain pair 2 to vif 3: chain pair is not found
can't attach filter chain pair 2 to vif 3: unknown chain type 100
```

[16] Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

```
can't attach filter chain pair 2 to vif 3, chain type 1: vif is dead
can't attach filter chain pair 2 to vif 3: chain type 1 is occupied
can't detach filter chain pair type 1 from vif 2: vif is not found
can't detach filter chain pair type 120 from vif 2: unknown chain type
can't detach filter chain pair type 1 from vif 2: chain pair is not
attached
update phy info: can't find phy "eth140"
update phy: can't unpack
can't create vif: unable to unpack
can't deregister vif 9: not found"
```

13.23.9 События группы mtud

ICMP сообщение destination unreachable/fragmentation needed не отослано по причине того, что в SA стоит настройка принудительного выставления DF-бита:

```
not sending ICMP because of DF bit enforced by IPsec SA options for
packet 10.0.59.1:1680->12.1.1.1:23, proto 50, len 140: topmost SA 28
```

MTU с учетом применения IPsec инкапсуляции меньше минимального MTU для IP-пакетов:

```
MTU is too low for packet 10.0.59.1:1680->12.1.1.1:23, proto 50:
calculated MTU 60, topmost SA 49
```

Отослано ICMP сообщение о необходимости снижения MTU трассы:

```
ICMP dest unreachable/fragmentation needed sent for packet
10.0.59.1:1680->12.1.1.1:23, proto 50, len 1520, topmost SA 80: MTU 1430
```

При получении сообщения ICMP не найдено SA, который был использован при обработке проблемного пакета, сообщение проигнорировано:

```
SPI 0xbebebebe not found, discarding ICMP message from 3.2.4.1
```

При получении сообщения ICMP найден SA, который был использован при обработке проблемного пакета, но для этого SA отключена обработка ICMP path mtu discovery, сообщение проигнорировано:

```
MTU discovery is not enabled for SA 32, discarding ICMP message from
3.4.5.6
```

ICMP сообщение обработано, MTU трассы выставлено в соответствии:

```
MTU discovery message from 3.3.3.3 processed, requested value 1400,
setting path MTU to 1400 for SA 89"
```

Запрошенное значение MTU из ICMP сообщения не прошло проверку, сообщение проигнорировано:

```
MTU 10 is out of expected range, discarding ICMP message from 3.5.11.1
```

13.23.10 Сообщение об утере данных

Сообщение о потере данных из-за недостаточной скорости обработки сообщений приложением (например, klogview не успевает их выводить). В случае klogview можно ограничить поток сообщений, выбрав только необходимые группы (параметр -f).

```
*** 1080 messages lost[17]  ***
```

[17] Сообщение имеет id IPSM_LOG_MID_LOST и параметр с индексом 0 типа I32, содержащий количество потерянных сообщений.

13.24 lic_mgr show

Команда `lic_mgr show` предназначена для просмотра текущей Лицензии на продукт S-Terra Client.

Синтаксис

```
lic_mgr show
```

Данная команда не имеет аргументов и ключей.

Значение по умолчанию Значение по умолчанию отсутствует.

13.25 lic_mgr set

Команда `lic_mgr set` предназначена для установки текущей Лицензии. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
lic_mgr set -p PRODUCT_CODE -c CUSTOMER_CODE -n LICENSE_NUMBER -l LICENSE_CODE
```

`-p PRODUCT_CODE`	код Продукта, возможные коды:
	`CLIENTB`
	`CLIENT`

`-c CUSTOMER_CODE`	код заказчика
`-n LICENSE_NUMBER`	номер лицензии
`-l LICENSE_CODE`	код лицензии

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

```
lic_mgr set –p CLIENTB –c test –n 1 –l 5B271A01DF5D143A
Active license:
CustomerCode=test
ProductCode= CLIENTB
LicenseNumber=1
LicenseCode=5B271A01DF5D143A
```


13.26 log_mgr show

Команда `log_mgr show` предназначена для просмотра общего уровня протоколирования, всех событий и настроек syslog-клиента.

Синтаксис

`log_mgr` `[-T timeout]` **`show`** `[-e [msg_group_file.ini]]`

log_mgr `[-T timeout]` **show-syslog**

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд.
`-e msg_group_file.ini`	имя файла `msg_group_file.ini`, в котором указана группа событий и уровень протоколирования для них.
`show-syslog`	вывод настроек syslog-клиента.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Для вывода значения общего уровня протоколирования всех событий используйте команду

```
log_mgr show
```

Для вывода измененного администратором уровня протоколирования какого-либо события используйте команду:

```
log_mgr show -e
```

При отсутствии таких изменений – команда ничего не выводит. Все события, их идентификаторы и уровень лога для каждого из них указанны в файле `s_log.ini` каталога Продукта.

Для вывода настроек syslog-клиента используйте команду:

```
log_mgr show-syslog
```

Пример

`log_mgr show`:

```
Default log level: <6> info
```

`log_mgr show-syslog`

```
syslog parameters: enabled, server_ip=127.0.0.1, facility=local7
```


13.27 log_mgr set

Команда `log_mgr set` предназначена для изменения настройки уровня протоколирования всех событий, не включенных в группы, уровня протоколирования группы событий, настройки syslog-клиента, задания группы событий и др.
Для выполнения опций: `reset-syslog`, `set-syslog`, `set -e`, `save` требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

log_mgr [-T timeout] **set** -l log_level

log_mgr [-T timeout] **set** -e [msg_group_file [-f]]

log_mgr [-T timeout] **save**

log_mgr [-T timeout] **set-syslog** [-y {enable|disable}] [-a syslog_ip] [-f facility]

log_mgr [-T timeout] **reset-syslog**

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-l log_level	уровень протоколирования всех событий, не включенных в группы событий. Имеет одно из возможных значений: emerg – аварийные сообщения alert – тревожные сообщения crit – критические сообщения err – сообщения об ошибках warning – предупреждения notice – извещения info – информационные сообщения debug – отладочные сообщения.
-e msg_group_file	имя файла msg_grpXXX.ini, в котором можно задать группу событий и уровень протоколирования для нее.
-f	(force) указание этой опции разрешает изменять файл с группой событий. По умолчанию опция не задана и изменение файла не допускается.
-y {enable|disable}	включение/выключение протоколирования.
-a syslog_ip	IP-адрес хоста, на который будут отправляться сообщения (syslog-клиент).
-f facility	источник сообщений (начальное значение: local7). Возможные значения: kern, user, mail, daemon, auth, syslog, lpr, news, uucp, cron, authpriv, ftp, ntp, audit, alert, cron2, local0, local1, local2, local3, local4, local5, local6, local7.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Задание общего уровня протоколирования всех событий, которые не включены в группы событий с заданным уровнем, выполняется командой, например:

```
log_mgr set -l warning
```

Продукт поставляется с пятью предустановленными файлами, в которых указаны группы событий и уровень лога для этих событий. Эти файлы созданы для совместимости с продуктом версии 3.1 и 3.11:

- `msg_grpLDAP.ini` – задан уровень лога и идентификаторы событий, связанных с доступом к LDAP-серверу
- `msg_grpSYSTEM.ini` – задан уровень лога и идентификаторы системных событий
- `msg_grpPOLICY.ini` – задан уровень лога и идентификаторы событий, связанных с применением политики безопасности
- `msg_grpCERTS.ini` – задан уровень лога и идентификаторы событий, связанных с сертификатами
- `msg_grpKERNEL.ini` – задан уровень лога и идентификаторы событий, связанных с firewall.

Для задания протоколирования группы событий, указанных в файле с заданным уровнем, обязательно выполните команду (например, для LDAP):

```
log_mgr set -e msg_grpLDAP.ini -f
```

Настройка сохраняется до перезапуска сервиса. После перезапуска сервиса протоколирование этих событий будет происходить с общим уровнем логирования.

Если отредактировать файл `msg_grpLDAP.ini` (или не редактировать) и повторно запустить команду без опции –f, то будет выдано сообщение об ошибке.

Для сохранения изменений в файле с группой событий и уровнем протоколирования, и после перезапуска сервиса, выполните команду:

```
log_mgr save
```

Для отмены всех установленных ранее уровней протоколирования для всех групп событий, выполните команду:

```
log_mgr set -e
```

Настройка сохраняется до перезапуска сервиса.

Создание файла с группами событий

Для создания файла с группой интересующих событий (сообщений), надо знать структуру этого файла и где взять список событий (сообщений). Опишем это далее.

Каждый такой файл должен состоять из секций вида:

```
[LOGLEVEL.<LEVEL>]
<MSG_ID1>
<MSG_ID2>
!........
```

где

`<LEVEL>`	значение уровня лога для всех событий, перечисленных в группе
`<MSG_ID>`	идентификатор события (сообщения)
`!......`	строка, начинающаяся с символа ‘!’, является комментарием. Допустимы пустые строки.

Таких секций в файле может быть несколько. Все события (сообщения) перечислены в файле s_log.ini из состава продукта. Каждое событие в файле имеет два эквивалентных представления – текстовое и в виде индекса (8 шестнадцатеричных цифр), например,

```
[MSG_ID_PRODUCT_START]
INDEX   = 0x03090001
```

Рекомендуется использовать текстовое представление, однако индекс может быть удобнее, если уже имеется файл, в котором сообщение содержит индекс.

Пример такого файла –`msg_groupDEMO1.ini`:

```
[LOGLEVEL.DEBUG]
!     сообщение PRODUCT_START задано его индексом:
03090001
!     сообщение PRODUCT_STOP задано его текстовым представлением:
PRODUCT_STOP
```

Каждое событие имеет свой уровень лога, указанный в файле `s_log.ini`. Если в группу включены события с разными уровнями логирования, то для того, чтобы выполнялось протоколирование по всем этим событиям, проще всего указать для группы уровень лога `debug`.

Если необходимо изменить фиксированный уровень аудита, указанный в файле `C:\Program Files\S-Terra Client\s_log.ini`, для отдельного события, можно создать файл типа `msg_XXX.ini` и задать в нем нужный уровень протоколирования.

Пример

Например, для изменения фиксированного уровня протоколирования сообщения `MSG_ID_AUDIT_SHOW_NEW_LSP с INFO на ERR`, создаем в директории `C:\Program Files\S-Terra Client\ файл msg_LSPSHOW.ini`, содержащий строки:

```
[LOGLEVEL.ERR]
MSG_ID_AUDIT_SHOW_NEW_LSP
```

Далее выполняем команды:

```
log_mgr set -e msg_LSPSHOW.ini
log_mgr save
```

Установка параметров syslog-клиента для сервиса vpnsvc. Установленные настройки Syslog-клиента будут записаны в файл `syslog.ini`.

```
log_mgr set-syslog [-y {enable|disable}] [-a syslog_ip] [-f facility]
```

Например,

```
log_mgr set-syslog -y enable -a 10.0.0.1
```

Неуказанный в команде параметр остается неизменным.

Установка параметров по умолчанию для syslog-клиента:

```
log_mgr reset-syslog
```

при этом действуют следующие настройки:

```
enable
syslog_ip=127.0.0.1
facility=local7
```

При установке уровня протоколирования следует помнить, что самый высокий уровень детализации дает параметр `'debug'`, а самый низкий – параметр `'emerg'`.

Пример

Пример выполнения команды `log_mgr set`:

```
log_mgr set -l warning
```

```
Default log level is set successfully
```

Редактирование файла s_log.ini

Существует группа сообщений, протоколирование которых производит vpnlogsvc. Для таких сообщений описанный выше способ изменения фиксированного уровня протоколирования не работает: внесение изменений происходит непосредственным редактированием файла `s_log.ini`, который располагается в каталоге продукта (по умолчанию – C:\Program Files\S-Terra Client).

Информация, содержащаяся в файле `s_log.ini` имеет вид:

```
[ <MSG_ID mnemonic> ]
<Russian(Русские) UTF-8 comment lines for User's Manual>
SEVERITY  = EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO |
DEBUG
INDEX     = 0x<module index><MSG_ID subindex 0001..ffff>
TMPL      = <message template>
NONBLOCKABLE = TRUE | FALSE
```

где

`<MSG_ID mnemonic>` – текстовое представление идентификатора события, состоящее из заглавных латинских букв и знаков «_» и обязательно содержащее префикс "MSG_ID_"
`<Russian(Русские) UTF-8 comment lines for User's Manual>` – строки, начинающиеся с символов "!!!", содержат описание или комментарии к событию
`SEVERITY` – уровень важности протоколируемых событий.
`INDEX` индекс сообщения, содержащий <module index> = 0001 | 0002 | 0003 | 0010 | 0020 | 0029 | 0032 | 005B | 0065 | 006F | 0072 | 0073 | 007F | 0079 | 0309 | 1000 | 0820..0820 | 0850..085C и <`MSG_ID subindex`> = 0001..ffff
`TMPL` – шаблон сообщения
`NONBLOCKABLE` – опциональный атрибут, установка которого в “TRUE” гарантирует вывод сообщения при любых изменениях уровней важности (LogLevel) протоколируемых событий и изменениях параметров используемого syslog сервера. Т.е., если значение равно “TRUE”, то вывод сообщения не зависит от установленного общего уровня протоколирования. Значение по умолчанию – “`FALSE`”, т.е. вывод сообщения подчиняется общему установленному уровню аудита.

Примечание: Атрибут NONBLOCKABLE имеет значение TRUE лишь для групп событий, имеющих ID с 08530001 до 0853000A (раздел Installer for Unix) и с 00020001 до 00020005 (раздел Log), согласно Таблице 3 документа «Приложение А» (Appendix_A.pdf). При этом, изменение его на FALSE для событий из раздела Installer for Unix невозможно.

Пример отображения информации о протоколируемом событии в файле s_log.ini:

```
[MSG_ID_LOG_SET_PARTICULAR_LOGLEVELS]
!!! Нефильтруемое сообщение об установке частных уровней логирования
некоторым сообщениям.
!!! Выдается при каждом их изменении и в начале сессии VPN Сервиса.
SEVERITY= INFO
INDEX   = 0x00020003
TMPL    = Some particular log levels are set
```

```
NONBLOCKABLE = TRUE
```

Пример редактирования файла s_log.ini:

Например, для изменения уровня протоколирования сообщения, имеющего ID 0029000E, с INFO на DEBUG, необходимо открыть текстовый файл `C:\Program Files\S-Terra Client\s_log.ini` и найти раздел со строкой:

```
INDEX = 0x0029000E
```

В данном разделе нужно изменить значение атрибута SEVERITY на необходимое:

```
SEVERITY = DEBUG
```

Также, если для данного сообщения значение атрибута NONBLOCKABLE равно TRUE, то необходимо выставить его в FALSE:

```
NONBLOCKABLE = FALSE
```

После сохранения файла `s_log.ini` необходимо пересчитать его контрольную сумму, используя утилиту `integr_mgr calc`:

```
integr_mgr calc -f /opt/VPNagent/etc/s_log.ini
```

Перезапустите vpn-демон и log-сервис, последовательно выполнив команды:

```
/etc/init.d/vpngate stop
/etc/init.d/vpnlog stop
/etc/init.d/vpnlog start
/etc/init.d/vpngate start
```

Полный список сообщений, настройка протоколирования которых происходит только путем изменения файла `s_log.ini`, представлен в таблице 1:

Таблица 6

MSG ID	Текстовое представление	Раздел	Уровень
00290001	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_STATS_TRAIL	Firewall	INFO
00290002	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_HCONN_ALERT	Firewall	WARNING
00290003	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_HCONN_ALERT_OFF	Firewall	WARNING
00290004	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PORT_PRIV_PORT	Firewall	WARNING
00290005	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PASV_PRIV_PORT	Firewall	WARNING
00290006	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PORT_NOTAUTH	Firewall	WARNING
00290007	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PASV_NOTAUTH	Firewall	WARNING
00290008	MSG_ID_ON_IPSM_LOG_OTHERS	Firewall	DEBUG
00290009	MSG_ID_KLOGLIB_INIT_NO_MEMORY	Firewall	DEBUG

0029000A	MSG_ID_KLOGLIB_INIT_CANT_ATTACH	Firewall	DEBUG
0029000B	MSG_ID_KLOGLIB_INIT_CANT_SET_FILTER	Firewall	DEBUG
0029000C	MSG_ID_KLOGLIB_INIT_MISSED_ALERT_PACKETS	Firewall	WARNING
0029000D	MSG_ID_KLOGLIB_INIT_MISSED_PACKETS	Firewall	WARNING
0029000E	MSG_ID_KLOGLIB_INIT_PRINT_SUMMARY	Firewall	INFO
03090202	MSG_ID_LOGSRV_SET_SETTINGS_FAIL	<MAIN_APPLICATION>	WARNING
03090203	MSG_ID_LOGSRV_START	<MAIN_APPLICATION>	INFO
03090204	MSG_ID_LOGSRV_STOP	<MAIN_APPLICATION>	INFO

13.28 lsp_mgr check

Команда `lsp_mgr check` предназначена для проверки LSP конфигурации. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

`lsp_mgr` `[-T timeout]` **`check`** `-f LSP_FILE`

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
`-f LSP_FILE`	путь к файлу конфигурации.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте команду `lsp_mgr check` для проверки синтаксиса файла с политикой безопасности.

13.29 lsp_mgr load

Команда `lsp_mgr load` предназначена для загрузки конфигурации из файла в базу Продукта. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

lsp_mgr [-T timeout] **load** -f LSP_FILE [-l LABEL]

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-f LSP_FILE	путь к файлу конфигурации.
-l LABEL	текстовый комментарий к конфигурации (в произвольном формате). По умолчанию в качестве LABEL задается путь до файла с конфигурацией (аргумент опции `-f`).

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Если политика безопасности написана в виде текстового конфигурационного файла, то для загрузки ее в базу Продукта используйте команду lsp_mgr load.

Пример

Пример загрузки LSP конфигурации из файла в базу Продукта:

```
sp_mgr load -f default.txt
  LSP successfully loaded from file default.txt
```


13.30 lsp_mgr reload

Команда `lsp_mgr reload` предназначена для перезагрузки LSP конфигурации.

Синтаксис

`lsp_mgr` `[-T timeout]` **`reload`**

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте команду `lsp_mgr reload` в следующих случаях:

- если произошли какие-то изменения в сертификатах, изменения у партнера, у шлюза безопасности и др.
- для устранения всех установленных соединений с партнерами
- во внештатных ситуациях – зависание Продукта и др.

Пример

Пример загрузки LSP конфигурации из базы Продукта:

```
lsp_mgr reload
  LSP is reloaded successfully
```


13.31 lsp_mgr unload

Команда `lsp_mgr unload` предназначена для выгрузки LSP конфигурации.

Синтаксис

`lsp_mgr` `[-T timeout]` **`unload`**

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для выгрузки активной конфигурации в базу Продукта. При выгрузке конфигурации начинает действовать политика драйвера по умолчанию – DDP. Политика DDP задается администратором при создании инсталляционного файла Продукта S-Terra Client для пользователя.

Пример

Пример выгрузки активной конфигурации в базу Продукта:

```
lsp_mgr unload
  Operation completed successfully
```

13.32 lsp_mgr show

Команда `lsp_mgr show` предназначена для просмотра локальной политики безопасности пользователя (LSP).

Синтаксис

`lsp_mgr` `[-T timeout]` **`show`**

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
`-db`	показать конфигурацию пользователя, хранящуюся в базе локальных настроек продукта.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Если загружена конфигурация пользователя, то по данной команде она будет выведена. Если загружена Default Driver Policy на экран будет выведено сообщение: `Default Driver Policy is loaded` без вывода тела конфигурации.

В штатном режиме работы вывод команды как с указанием опции `-db`, так и без указания данной опции, должен совпадать. Однако он будет отличаться, например, после выполнения команды `lsp_mgr unload`: в этом случае команда `lsp_mgr show -db` по-прежнему выдаст текст конфигурации. При отсутствии конфигурации в базе будет выдано сообщение: `Default Driver Policy is loaded`.

При просмотре конфигурацию можно сохранить в файле, например `current_lsp.txt`, командой:

```
lsp_mgr show > current_lsp.txt
```

Пример

```
lsp_mgr show
GlobalParameters (
 Title = "This LSP was automatically generated by S-Terra Client
AdminTool (cp) at 2011.09.29 14:10:13"
 Version = LSP_4_0
 CRLHandlingMode = BEST_EFFORT
)
LDAPSettings (
 ResponseTimeout = 200
 HoldConnectTimeout = 60
 DropConnectTimeout = 5
)
IdentityEntry auth_identity_01(
)
AuthMethodPreshared auth_method_01(
 SharedIKESecret = "fg"
 LocalID = auth_identity_01
)
```



```
IKEParameters (
 DefaultPort = 500
 SendRetries = 5
 RetryTimeBase = 1
 RetryTimeMax = 30
 SessionTimeMax = 60
……
```

13.33 lsp_mgr show-info

Команда `lsp_mgr show-info` предназначена для просмотра информации о локальной политики безопасности пользователя (LSP).

Выводится следующая информация:

Type – тип локальной политики безопасности – DHCP only | default driver policy | user-defined

Source – источник локальной политики безопасности

Source info – дополнительная информация об источнике локальной политики. Присутствует в выводе команды только в случае, если Type – user-defined.

Синтаксис

lsp_mgr [-T timeout] **show-info**

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-db	показать информацию о конфигурации пользователя, хранящейся в базе локальных настроек продукта.
Значение по умолчанию	Значение по умолчанию отсутствует.

Пример

Ниже приведен пример вывода информации о политике безопасности сразу после установки инсталляционного пакета S-Terra Client:

```
lsp_mgr show-info
  Type: user-defined
  Source: 0
```

Пример вывода информации о политике безопасности в случае загрузки конфигурации в базу продукта из файла, с использованием утилиты lsp_mgr load:

```
lsp_mgr show-info
  Type: user-defined
  Source: command line
  Source info: lsp.txt
```

13.34 pwd_change

Команда `pwd_change` предназначена для изменения пароля пользователя. Эта команда запускается автоматически при нажатии кнопки `Change Password...` в окне логина пользователя (Рисунок 37) и вызовом окна `Change Password` (Рисунок 38) для ввода старого и нового пароля. Эту команду можно запускать и вручную.

Синтаксис

```
pwd_change [old_user_PWD new_user_PWD]
```

`old_user_PWD`	старый пароль
`new_user_PWD`	новый пароль

Если не задать старый и новый пароль, то в интерактивном режиме они будут запрошены. При вводе символов их печать на консоль не производится. Новый пароль будет запрошен дважды во избежание ошибки.

Пример

Ниже приведен пример изменения пароля пользователя:

```
pwd_change "old_pwd" "new_pwd"
  New password is set successfully

pwd_change
  Enter old password:
  Enter new password:
  Re-enter new password:
  New password is set successfully
```


13.35 sa_mgr show

Команда `sa_mgr show` предназначена для просмотра информации обо всех IPsec SA, ISAKMP SA, их состоянии и о количестве IKE обменов.

Синтаксис

sa_mgr [-T timeout] **show** [-isakmp|-ipsec] [-i CONN1_ID] [-i CONNn_ID] [-detail]

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд.
-isakmp	выводится информацию об ISAKMP соединениях.
-ipsec	выводится информацию об IPsec соединениях.
-i CONNn_ID	выводится информация о соединении с указанным идентификатором.
-detail	выводится детальная информация о соединениях.

Команда `sa_mgr show` позволяет просмотреть действующие в данный момент `IPsec SA`.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

sa_mgr show

В данной команде без указания опции `-detail` выводится краткая информация обо всех соединениях, например:

```
ISAKMP sessions: 0 initiated, 0 responded


ISAKMP connections:
Num Conn-id (Remote Addr,Port)-(Local Addr,Port) State Sent Rcvd
1 2 (10.0.10.16,500)-(10.0.10.99,500) active 1560 656
2 3 (10.0.10.18,500)-(10.0.10.99,500) active 1560 656


IPsec connections:
Num Conn-id (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type
Sent Rcvd
1 6 (192.168.15.16,*)-(10.0.10.99,*) * AH+ESP tunn 600 1120
2 8 (192.168.15.18,*)-(10.0.10.99,*) * ESP tunn 1600 3140
```

В выводе присутствует следующая информация:

ISAKMP sessions – количество незавершенных IKE-обменов:

- `ni initiated` – в качестве инициатора
- `nr responded` – в качестве ответчика.

ISAKMP connections – информация обо всех ISAKMP SA и для каждого соединения:

- `Num` – порядковый номер ISAKMP соединения
- `Conn-id` – уникальный идентификатор ISAKMP соединения
- `Remote Addr,Port` – адрес и порт партнера, если порт любой – *

- `Local Addr,Port` – локальный адрес и порт, если порт любой – *
- `State` – состояние SA:
  - `incomplete` – недостроенное соединение
  - `active` – активное соединение
  - `configuration` – для данного SA проводится дополнительная настройка `(IKECFG, XAuth, etc.)`
  - `deleted` – SA не используется, подготовлен к удалению
  - `unknown` – статус соединения неизвестен
- `Sent` – количество переданной информации (в байтах)
- `Rcvd` – количество принятой информации (в байтах)

IPsec connections – информация обо всех IPsec SA и для каждого соединения:

- `Num` – порядковый номер IPsec соединения
- `Conn-id` – уникальный идентификатор IPsec соединения
- `Remote Addr,Port` – адрес и порт партнера, если порт любой – *
- `Local Addr,Port` – локальный адрес и порт, если порт любой – *
- `Protocol` – сетевой протокол, если протокол любой – *
- `Action` – действие – {`AH+ESP|AH|ESP`}
- Type – тип:
  - `tunn` – туннельный режим
  - `trans` – транспортный режим
  - `nat-t-tunn` – туннельный режим через NAT
  - `nat-t-trans` – транспортный режим через NAT
- `Sent` – количество переданной информации (в байтах)
- `Rcvd` – количество принятой информации (в байтах)

`sa_mgr show –ipsec –i 8`

Данная команда выводит информацию о соединении с заданными свойствами.

IPsec connections:

```
Num Conn-id (Remote Addr,Port)-(Local Addr,Port) Protocol Action
Type Sent Rcvd
1 8 (192.168.15.18,*)-(10.0.10.99,*) * ESP tunn 1600 3140
```

`sa_smgr how -detail`

Команда с опцией `detail` выводит полную информацию обо всех соединениях.

```
ISAKMP sessions: 0 initiated, 0 responded


ISAKMP connection id: 2
    cookies: 613E427395946DFE.DE99B25554306A75
    local  peer (addr/port): 10.0.10.99/500
    remote peer (addr/port): 10.0.10.16/500
```

```
    local identity (IPV4_ADDR): 10.0.10.99
    remote identity (IPV4_ADDR): 10.0.10.16
    IKERule name: ike_rule_without_ikecfg
    auth: preshared key
    mode: main

    sa:
     transform: gost2814789cp-cbc gostr341194cp
     Oakley group: 5
     sa limits: key lifetime (qm/k/sec): -/200/28800
     sa timing: remaining key lifetime (qm/k/sec): -/198/26622
     status: active

IPsec connection id: 6
    local  ident (addr/prot/port): 10.0.10.99/0/0
    remote ident (addr/prot/port): 192.168.15.16/0/0

    #pkts sent/rcvd: 32/6777
    #send/recv errors: 2/0

    local crypto endpt.: 10.0.10.99, remote crypto endpt.: 10.0.10.16
    connection status: {initiated locally, }

    remote identity (IPV4_ADDR): 10.0.10.16
    IPsecAction name: IPsec_action_01
    FilteringRule name: filter_rule_00_00
    PFS: none

    inbound esp sa:
     spi: 0x94857A70(2491775600)
      transform: esp-gost2814789cp-cbc esp-gostr341194cp-hmac
      in use settings ={Tunnel, }
      sa limits: key lifetime (k/sec): 4608000/3600
      sa timing: remaining key lifetime (k/sec): 4607998/1426

    inbound ah sa:
     spi: 0x6CD88232(1826128434)
      transform: ah-gostr341194cp-hmac
      in use settings ={Tunnel, }
      sa limiting: key lifetime (k/sec): 4608000/3600
      sa timing: remaining key lifetime (k/sec): 4607999/1426

    outbound esp sa:
     spi: 0xF40CDEE0(4094484192)
      transform: esp-gost2814789cp-cbc esp-gostr341194cp-hmac
```

```
      in use settings ={Tunnel, }
      sa limits: key lifetime (k/sec): 4608000/3600
      sa timing: remaining key lifetime (k/sec): 4607999/1426

    outbound ah sa:
     spi: 0xFBE599CD(4226128333)
      transform: ah-gostr341194cp-hmac
      in use settings ={Tunnel, }
      sa limiting: key lifetime (k/sec): 4608000/3600
      sa timing: remaining key lifetime (k/sec): 4607998/1426
```

В выводе присутствует следующая информация:

ISAKMP sessions – количество незавершенных IKE-обменов:

- `ni initiated` – в качестве инициатора
- `nr responded` – в качестве ответчика.

ISAKMP connection – в выводе будет присутствовать:

- поле `IKECFG address`, если был получен IKECFG адрес:

```
ISAKMP connection id: 1
    cookies: F86F80B571D2240F.A0455C78E9DE66C
    local  peer (addr/port): 10.0.10.193/500
    remote peer (addr/port): 10.0.10.178/500
    IKECFG address: 192.168.15.193
```

- поле `Status` может принимать следующие значения:
  - `incomplete` – недостроенное соединение
  - `active` – активное соединение
  - `configuration` – для данного SA проводится дополнительная настройка `(IKECFG, XAuth, etc.)`
  - `deleted` – SA не используется, подготовлен к удалению
  - `unknown` – статус соединения неизвестен

IPsec connection:

- поле connection `Status` может принимать значения:
  - `initiated locally` – локальный хост выступает инициатором
  - `initiated remotely` – локальный хост выступает ответчиком
  - `rekeyed` – произведено досрочное пересоздание соединения
  - `no rekeying` – досрочное пересоздание соединения в качестве инициатора запрещено
- поле `in use settings` может принимать значения:
  - `Tunnel` – туннельный режим
  - `Transport` – транспортный режим
  - `Tunnel NAT-T` – туннельный режим через NAT
  - `Transport-NAT-T` – транспортный режим через NAT

13.36 sa_mgr clear

Команда `sa_mgr clear` предназначена для удаления ISAKMP и IPsec соединений. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

sa_mgr [-T timeout] **clear** [-isakmp|-ipsec] [-i CONN1_ID] [-i CONNn_ID] [-silent]

sa_mgr [-T timeout] **clear** -all [-silent]

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд.
-isakmp	удаляет ISAKMP соединения.
-ipsec	удаляет IPsec соединения.
-i CONN1_ID	удаляет соединения с указанным идентификатором.
-silent	удаляет соединения без уведомления партнера.
-all	удаляет все IPsec и ISAKMP соединения во всех состояниях, прекращаются все ранее начатые IKE-обмены.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Для выборочного удаления используются опции `-isakmp`, `-ipsec`, `-i`.

При этом ISAKMP соединения не удаляются сразу, а только подготавливаются к удалению (см. Status – deleted) и в течение заданного в политике безопасности времени еще могут быть переиспользованы.

Пример

Удаление ISAKMP соединений с идентификаторами 1 и 4:

```
sa_mgr clear -isakmp -i 1 -i 4
```

```
ISAKMP connection 1 is removed
ISAKMP connection 4 is not found
```

Удаление всех IPsec соединений:

```
sa_mgr clear -ipsec
```

```
IPsec connection 1 is removed
IPsec connection 3 is removed
```

Удаление всех соединений:

```
sa_mgr clear -all
```

```
All connections are removed
или
Not all connections are removed
```

13.37 ver_show

Команда `ver_show` предназначена для просмотра информации об установленном продукте.

Синтаксис

```
ver_show [-a|-i|-n|-r|-w|-d|-l|-p|-h]
```

-a	выводит всю информацию (значение по умолчанию)
-i	выводит информацию об установленной ОС
-n	показывает имя продукта
-r	показывает версию продукта
-w	показывает версию и номер сборки продукта
-d	показывает дату сборки продукта
-l	показываеи лицензию продукта
-p	показывает информацию о криптопровайдере
-h	показывает подсказку

Пример

```
ver_show
OS information:       Windows XP Professional (5.1.2600) Service
Pack 3
product name:         S-Terra Client
product release:      4.1
product build number: 4.1.13427
product build date:   2013-01-25 19:44:24
product license:      CLIENT,DEMO,1
crypto provider:      CryptoPro 3.6.6497
```


13.38 Сообщения об ошибках

Ниже приведены тексты сообщений об ошибках, которые могут возникать при работе с программными утилитами.

Если в тексте полученного сообщения присутствует фраза ”Internal error:”, то обращайтесь в службу поддержки по адресу support@s-terra.com.

Утилита cert_mgr

Текст сообщения	Описание проблемы
User Error: no source file specified	Не указан путь к файлу (cert_mgr … -f)
User Error: FILENAME unable to open file	Ошибка при открытии файла
Internal Error: No memory	Нет свободной оперативной памяти
User Error. No password specified to open FILENAME	Не задан пароль доступа к файлу
FILENAME wrong password PASSWORD	Неверный пароль
User Error. No password specified	Не указан пароль (cert_mgr ….-p)
Internal Error. Unable obtain certs from DB	Не удается получить сертификаты из базы продукта
User Error: no number specified\n	Не указан индекс сертификата (cert_mgr –i)
User Error: NUMBER exceeds number of objects	Указанный индекс превышает количество объектов в базе продукта
User Error. No subject	Не задано поле Subject сертификата
User Error: Key KEY1 is not compatible with key KEY2	Несовместимость заданных параметров (ключей)
User Error: Key KEY is useless	Задан лишний параметр
User Error: Key KEY is used twice	Повторное задание параметра (ключа)
User Error: Unable remove. Base is empty	Попытка удаления сертификата из пустой базы продукта
Internal Error:Unable remove object from base	Неудачная попытка удаления объекта из базы продукта
User Error. Missing parameter	Отсутствует параметр
User Error. No file name specified	Не указано имя файла
Internal Error. Storage error.	Ошибка при открытии хранилища
User Error: INDEX exceeds number of objects in NAME	Значение индекса превышает количество объектов в хранилище NAME
User Error: Container name is not specified	Не указано имя контейнера

User Error: CRL can not be removed from base	CRL не может быть удален из базы продукта
User Error: Object index INDEX exceeds number of certificates and CRLs in base	Индекс объекта превышает количество сертификатов и CRL в базе продукта
User Error. Missing index of object to be removed from base. Specify 'i' key and index	Не указан индекс объекта для удаления из базы продукта
User Error. Specify certificate request subject	Ошибка задания поля Subject в запросе на сертификат
Internal Error. Unable to create certificate request ERRCODE	Ошибка при создании запроса на сертификат
Internal Error. Unable to put certificate request into base ERRCODE	Ошибка при сохранении запроса на сертификат
User Error. Missing index of object to be imported from <FILENAME>. Specify i|t key and index	Не указан индекс объекта для регистрации в базе продукта.
User Error. Container 'CONTAINER_NAME' is not exists or access denied	Не удалось получить доступ к контейнеру (убедиться в наличии и доступности контейнера)
User Error. Failed to read private key: ERROR_DESCRIPTION	Не удалось получить секретный ключ (убедиться в доступности ключа в контейнере)
User Error. Cannot connect to the IPsec service: service is not running.	Не удалось соединиться с демоном (убедиться, что демон запущен)
User Error. Unable to set trusted status to certificate CERT_DSC	Не удалось выставить сертификату статус TRUSTED (убедиться, что сертификат CA)
User Error. Key is not consistent to cert CERT_DSC	Секретный ключ не подходит к сертификату или проверка закончилась неудачей (убедиться, что задан верный контейнер)
User Error. Unable to associate key and crt CERT_DSC	Не удалось ассоциировать секретный ключ и сертификат (убедиться, что сертификат не CA)
User Error: Key -l is not compatible with key -t | -kf | -kfp | -kc | -kcp	Задан недопустимый ключ “-kf | -kfp | -kc | -kcp” при импорте сертификата, полученного из ранее созданного запроса на сертификат
User Error: attempt to import a CRL as certificate	Задан недопустимый ключ “-t | -l | -kf | -kfp | -kc | -kcp” при импорте CRL
User Error: Key -t is not compatible with key -l | -kf | -kfp | -kc | -kcp	Задан недопустимый ключ “-l | -kf | -kfp | -kc | -kcp” при импорте Trusted CA сертификата
Crypto error. Unable to create key container	Не удается создать контейнер ключа (проверить правильность имени контейнера)
Crypto error. Unable to create certificate request. Error code: CRYPTO PROVIDER	Не удается создать запрос на создание сертификата

ERROR	
Error: Cannot import Trusted or Local cert in current TokenLogin mode	Невозможен импорт Trusted или Local сертификата в режиме TokenLogin
Error: Cannot Cannot create request in current TokenLogin mode	Невозможен создать запрос на сертификат в режиме TokenLogin
Error: You need the Administrator permissions	Недостаточно прав пользователя

Утилита client_login, client_logout

Текст сообщения	Описание проблемы
User Error %d: VPN demon is not started	Проблема со стартом демона
Internal Error %d: Logout fail	Неудачный logout
VPN demon is not ready. Try again later	Демон недоступен
VPN service has returned error code: <код ошибки>	Ошибка при попытке входа
VPN service does not know how to provide the operation	Демон не понимает запроса на вход. Возникает при изменениях настроек без перезапуска демона
Old password is incorrect	Неверный старый пароль
The password is not changed. File or directory of DB cannot be created, removed or renamed	Ошибка при при внесении изменений в DB
The password is not changed. Error: <код ошибки>	Ошибка при установке пароля

Утилита cspvpn_verify

Текст сообщения	Описание проблемы
Integrity verification tool not found	Отсутствует продукт, используемый непосредственно для подсчета контрольных сумм.
Integrity verification list “file_.hashes_full_path” not found	Отсутствует файл .hashes.
Integrity verification list “file_.hashes_full_path” is corrupted	Проблемы с чтением файла .hashes (например, ошибочный синтаксис файла).
Integrity verification tool call failed on file “product_file_full_path”	Запуск cpverify по каким-либо причинам не произошел (какая-то системная ошибка; например, нехватка ресурсов, проблемы с правами доступа и т.п.) или вернул неожиданный код возврата (прерывание по сигналу, необработанный exception и т.п.).

Текст сообщения	Описание проблемы
File “product_file_full_path” is corrupted	Один или больше файлов продукта повреждены (контрольная сумма не соответствует эталонной; также возможны и другие ситуации, например, отсутствует файл (утилита cpverify эти ситуации не различает)).

Утилита dp_mgr

Текст сообщения	Описание проблемы
User Error: "ddd" is unknown parameter	Введен неизвестный параметр
User Error %d: VPN demon is not started	Проблема со стартом демона
Internal Error %d: Default driver policy is not wrote to db	Ошибка при записи Default Driver Policy в базу продукта
Internal Error %d: Default driver policy is not read from db	Ошибка при чтении Default Driver Policy из базы продукта

Утилита drv_mgr

Текст сообщения	Описание проблемы
User Error: Value for "NAME" is missing	Не задано значение настройки
User Error: Property name “NAME " is unknown	Имя настройки введено не верно
User Error: Required parameters are missing	Не задан обязательный параметр
User Error: command "NAME" is unknown	Введена неизвестная команда
Internal Error: Value of "NAME" cannot be read. Error: DESC	Не удалось получить значение настройки из драйвера
User Error: Value of "NAME" is not set to VALUE. Error: DESC	Не удалось выставить значение настройки в драйвер
User Error: Value of "NAME" is not saved to file.\n	Не удалось сохранить значение настройки в cfg файл (убедиться, что файл доступен на запись)
User Error: Values are not saved to file NAME.Error:DESC.	Не удалось сохранить cfg файл
User Error: File NAME cannot be loaded	Не удалось загрузить значения настроек из cfg файла (убедиться, что файл доступен на чтение).
Error: You need the Administrator permissions	Недостаточно прав пользователя

Утилита if_show

Текст сообщения	Описание проблемы
Internal error. Couldn't initialize local network interface list	Не удается получить информацию о сетевых интерфейсах
Internal error. Couldn't receive local network interface information	Не удается получить информацию об именах логических интерфейсов
User Error. Couldn't load network interface aliases file	Невозможно загрузить файл “ifaliases.cf”, хотя пакет установлен
User Error. Couldn't access PRODUCT driver	Драйвер пакета недоступен,,хотя пакет установлен
Warning: PRODUCT is not located	Предупреждение. Установленный пакет не найден. Не является ошибкой

Утилита integr_mgr

Код ошибки	Текст сообщения	Описание проблемы
0	SUCCESS: Operation was finished successfuly.	Успешное окончание.
9	ERROR: Missing required command or parameters. (Try ' integr_mgr -h' for help)	Недостаточное количество параметров в командной строке.
9	ERROR: Invalid command 'имя_команды'. (Try ' integr_mgr -h' for help)	Введено имя операции, которое утилита распознать не может. Допустимы операции ‘calc’ и ‘check’.
9	ERROR: Missing or invalid target file definition. (Try ' integr_mgr -h' for help)	В командной строке отсутствует имя файла для выполнения операции с единичным файлом..
9	ERROR: Missing target file name. (Try ' integr_mgr -h' for help)	В командной строке отсутствует имя файла со списком объектов для выполнения операции.
9	ERROR: Too long target file name 'имя файла'. (Try ' integr_mgr -h' for help)	Указанное имя файла превышает в длину 500 символов.
9	ERROR: Hash library initialization error.	Внутренняя ошибка инициализации системы вычисления хеша.
50	ERROR:: Missing file '<имя_файла>' or missing access to this file.	Указано имя несуществующего файла либо отсутствуют права на чтение содержимого этого файла. Данная ошибка может возникнуть как при обработке списка, так и при обработке единичного файла.
50	ERROR:: Missing file '<имя_файла_с_расширением_hash>'.	При попытке операции проверки выявлено отсутствие файла с контрольной информацией.

Код ошибки	Текст сообщения	Описание проблемы
54	ERROR: Read file is fault.	Ошибка чтения содержимого проверяемого файла.
54	ERROR: Invalid hash calculation.	Внутренняя ошибка вычисления контрольной информации.
54	ERROR: Invalid contents file '<имя_файла_с_расширением_hash>'.	Файл с контрольной информацией поврежден.
54	ERROR: Corrupted file '<имя_проверяемого_файла>'	Проверяемый файл поврежден.
54	ERROR: Invalid format of list file.	Формат файла списка проверяемых файлов нарушен.
54	ERROR: File '<имя_файла_из_списка>' was corrupted.	Поврежден проверяемый файл из списка.
75	ERROR: Can't create file '<имя_файла_с_расширением_hash>'.	Невозможно создать файл с контрольной информацией.
75	ERROR: Can't write file '<имя_файла_с_расширением_hash>'	Невозможно записать файл с контрольной информацией

Утилиты key_mgr

Текст сообщения	Описание проблемы
Internal Error: No memory to open file FILENAME	Недостаточно памяти, чтобы открыть файл
User Error: Key file no specified	Не указан файл с ключом
User Error: Key name no specified	Не указано имя ключа
Internal Error. Unable to append key into base KEYNAME	Ошибка при попытке импорта ключа в базу Продукта

Утилита lic_mgr

Текст сообщения	Описание проблемы
User Error: <parameter> undefined	Не указан один из параметров
User Error: Wrong license	Неверная лицензия
Internal Error: Can’t write license file	Ошибка при записи лицензии
Error: You need the Administrator permissions	Недостаточно прав пользователя

Утилита log_mgr

Текст сообщения	Описание проблемы
User Error: "ddd" is unknown parameter	Введен неизвестный параметр.
User Error: %d: VPN demon is not started	Проблема со стартом демона
Internal Error %d: Failed to set default log level	Ошибка при установке уровня протоколирования
Internal Error %d: Failed to get default log level	Ошибка при получении уровня протоколирования
User Error: Parameter is missing	Пропущен параметр команды
User Error: Too many parameters	Слишком много параметров команды
Internal Error: Failed to set log levels for msg group	Ошибка установки группы log levels
Internal Error: Failed to load the msg group file	Ошибка загрузки файла группы
Internal Error: Failed to get the msg group	Ошибка получения группы log levels
Internal Error: Failed to save log levels	Ошибка сохранения log levels

Утилиты lsp_mgr

Текст сообщения	Описание проблемы
User Error.FILENAME unable to open file	Ошибка при попытке открыть файл (убедиться в доступности файла).
Internal Error: Unable to set LSP as active	Не удалось загрузить LSP из файла в базу продукта
Internal Error: No memory to open file FILENAME	Недостаточно памяти для открытия файла
Internal Error: unrecognized error	Внутренняя ошибка
Internal Error: Unable to reload lsp from base	Не удалось перезагрузить LSP из базы продукта
Error: Cannot change LSP in current TokenLogin mode	В режиме TokenLogin изменение LSP запрещено

Утилиты sa_mgr

Текст сообщения	Описание проблемы
Internal Error: SAs' clearing failed. Error: %s.	Не удалось удалить ISAKMP или IPsec соединения.

Internal Error: ISAKMP info not available. Error: %s	Не удается получить информацию об ISAKMP
Internal Error Connections info not available. Error: %s	Не удается получить информацию о соединениях
Timeout expired. Please ensure that all chosen SAs are cleared.	Закончилось время ожидания завершения удаления соединений. Убедитесь, что все выбранные соединения удалены.

Утилита pwd_change

Текст сообщения	Описание проблемы
User Error %d: VPN demon is not started	Проблема со стартом демона
User Error %d: Old password is wrong	Неверный старый пароль
User Error %d: New password is not set	Ошибка при установке пароля

