ЗАО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, проезд 4806, д.6
Телефон: +7 (499) 940-9001
Факс: +7 (499) 940-9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный продукт
VPN Updater
Версия 1.2

Руководство администратора

27.06.2011

Содержание

Продукт VPN Updater 4
Назначение продукта 4
Возможности продукта 5
Характеристика продукта 6
Сценарии обновления 8
Сценарий первого обновления 8
Сценарий последующих обновлений 8
Установка и настройка Сервера обновления 9
Инсталляция Сервера обновления 9
Настройка Сервера обновления 16
Ввод лицензии 17
Создание CA сертификата 18
Создание рабочего сертификата 19
Задание адресов Сервера обновления 19
Обновление CSP VPN Server/CSP VPN Client 21
Создание клиента на Сервере обновления 21
Создание дистрибутивов Клиента обновления и CSP VPN Server/CSP VPN Client 28
Инсталляция Клиента обновления и CSP VPN Server/CSP VPN Client 31
Создание обновлений. Пример успешного обновления клиента 34
Информация о клиенте на Сервере обновления 39
Пример неудачного обновления клиента 44
Обновление CSP VPN Gate 49
Создание клиента на Сервере обновления 49
Создание дистрибутивов Клиента обновления и CSP VPN Gate 52
Инсталляция Клиента обновления и CSP VPN Gate 54
Создание обновлений для CSP VPN Gate 57
Обновление сертификата 58
Настройка ДСЧ на клиенте с CSP VPN Server/CSP VPN Client 58
Настройка ДСЧ на клиенте с CSP VPN Gate 59
Создание обновления с параметрами ключевой пары и запроса на сертификат 59
Создание на клиенте ключевой пары и запроса на сертификат 61
Создание сертификата 63

Создание обновления с новым сертификатом 64
Групповые операции на Сервере обновления 70
Создание шаблона проекта 71
Использование шаблона проекта 73
Действия пользователя при обновлении 74
Описание меню Сервера обновления 76
Меню File 76
Меню Groups 76
Меню Clients 77
Меню Tools 80
Меню Help 86
Настройки Сервера обновления 87
Настройки Клиента обновления 92
Создание обновлений с помощью командной строки 95

Продукт VPN Updater

Назначение продукта

Продукт VPN Updater версии 1.2 предназначен для централизованного удаленного управления и обновления всей линии продуктов, производимых компанией «С-Терра СиЭсПи», а именно, Программных комплексов «Сервер безопасности CSP VPN Server. Версия 3.1», «Клиент безопасности CSP VPN Client. Версия 3.1», «Шлюз безопасности CSP VPN Gate. Версия 3.1», установленных на конечных устройствах, банкоматах, платежных терминалах и др.

Далее продукты CSP VPN Server/CSP VPN Client/CSP VPN Gate будем именовать CSP VPN Agent.

Продукт VPN Updater состоит из двух частей:

- ***Сервер обновления*** – серверная часть продукта, устанавливается на выделенный компьютер и предназначена для управления процессом обновления продуктов CSP VPN Agent, инсталлированных на управляемых vpn-устройствах;
- ***Клиент обновления*** – клиентская часть продукта, устанавливается на управляемое vpn-устройство с инсталлированным продуктом CSP VPN Agent и предназначена для его обновления.

Общая схема использования продукта VPN Updater

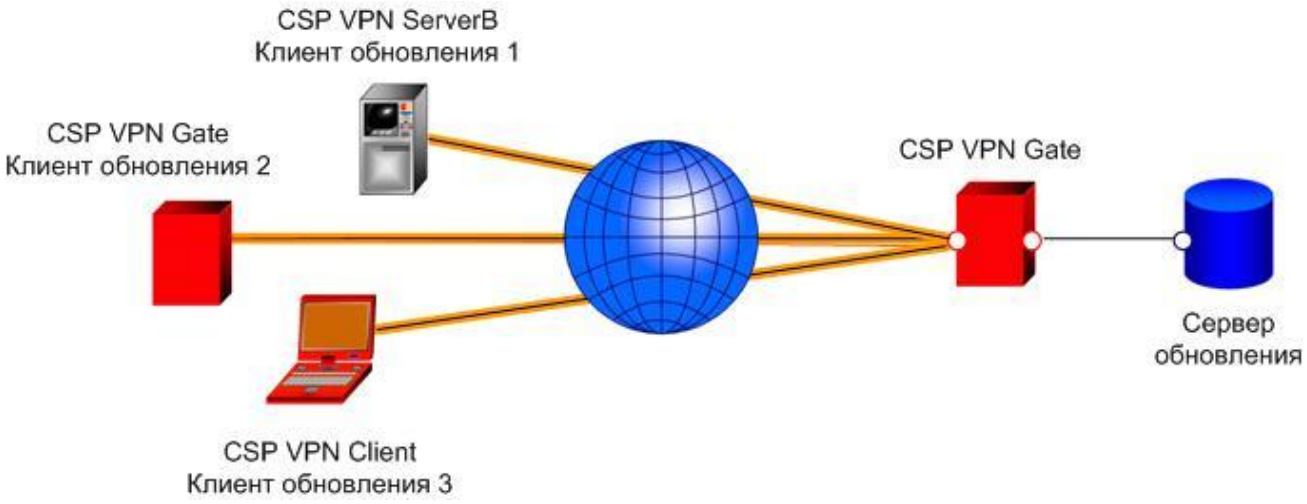

Рисунок 1

Сервер обновления устанавливается на выделенный компьютер, размещенный в защищенной локальной подсети. На Сервере обновления создается Клиент обновления для каждого управляемого vpn-устройства и сами обновления.

Созданный Клиент обновления устанавливается на управляемое vpn-устройство, для которого он и был создан.

Все обмены между Сервером обновления и Клиентом обновления осуществляются по протоколу FTP. Этот трафик должен передаваться по защищенному IPsec-туннелю.

Инициатором сетевого взаимодействия между Клиентом обновления и Сервером обновления всегда выступает Клиент обновления. В случае временной потери соединения на Клиенте обновления предусмотрена возможность “докачки” данных с Сервера обновления.

Возможности продукта

На управляемом vpn-устройстве с установленным продуктом CSP VPN Agent версии 3.1 и ***Клиентом обновления*** могут быть обновлены следующие данные:

- локальная политика безопасности, предписанная данному vpn-устройству (в виде LSP или в виде cisco-like конфигурации)
- политика драйвера по умолчанию продукта CSP VPN Agent
- настройки драйвера продукта CSP VPN Agent
- предопределенные ключи продукта CSP VPN Agent
- локальный сертификат продукта CSP VPN Agent, CA-сертификат, сертификаты партнеров, список отозванных сертификатов
- контейнеры с ключами сертификатов
- настройки протоколирования событий продукта CSP VPN Agent
- лицензия на продукт CSP VPN Agent
- Клиент обновления
- настройки Клиента обновления.

На ***Сервере обновления*** ведется мониторинг состояния и настроек всех управляемых vpn-устройств, предоставляемых ***Клиентами обновления:***

- версия Клиента обновления
- версия CSP VPN Agent
- локальная политика безопасности продукта CSP VPN Agent (в виде LSP или в виде cisco-like конфигурации)
- настройки драйвера продукта CSP VPN Agent
- локальный сертификат продукта CSP VPN Agent, списки отозванных сертификатов, CA сертификат, сертификаты партнеров
- имена предопределенных ключей продукта CSP VPN Agent
- настройки протоколирования событий продукта CSP VPN Agent
- лог-сообщения vpn-продукта CSP VPN Agent и Клиента обновления
- лицензия продукта CSP VPN Agent
- созданные запросы на локальные сертификаты
- имена контейнеров с ключами сертификатов (если нет возможности сбора информация обо всех контейнерах, допускается сбор информации только о контейнерах, созданных с использованием Клиента обновления).

На ***Сервере обновления*** в данной версии появились следующие возможности:

- расширенное отображение, по сравнению с предыдущей версией, информации о процессах обновления на всех управляемых vpn-устройствах, а именно:
  - дата и время последнего успешного соединения каждого vpn-устройства с Сервером обновления
  - IP-адреса vpn-устройств, с которых было осуществлено последнее успешное соединение
  - ближайшее время и дата истечения срока действия одного из сертификатов, размещенных в базе продукта CSP VPN Agent на каждом vpn-устройстве

- выполнение групповых операций, например, одновременное создание обновлений для нескольких vpn-устройств
- использование шаблонов проекта при создании обновлений для vpn-устройств.

Характеристика продукта


Note

Сервер обновления помимо графическиого интерфейса имеет интерфейс управления на основе командной строки.

На Сервере обновления каждый Клиент обновления имеет уникальный идентификатор, а создаваемые обновления имеют порядковые номера. Уникальный идентификатор и порядковый номер входят в состав данных, загружаемых с Сервера обновления. Полученные данные используются Клиентом обновления только в том случае, если содержат верный идентификатор Клиента обновления и если номер обновления больше последнего установленного обновления.

Продукт обеспечивает защиту от злоумышленника, пытающегося с помощью механизма обновления запустить на компьютере с Клиентом обновления “чужеродное” ПО. Предполагается, что злоумышленник не имеет доступа к управлению компьютером с Сервером обновления и доступа к управлению устройствами с Клиентами обновления. Защита осуществляется на основе ЭЦП, позволяющей осуществить аутентификацию и проверить целостность пересылаемых данных от Сервера обновления к Клиенту обновления.

Действительно, перед тем как предоставить данные для скачивания Клиентам обновления, Сервер обновления формирует цифровую подпись для этих данных с использованием секретного ключа рабочего сертификата Сервера обновления. А Клиент обновления перед использованием полученных данных с Сервера обновления проверяет цифровую подпись, используя открытый ключ рабочего сертификата Сервера обновления.

Рабочий сертификат Сервера обновления распространяется среди Клиентов обновления в составе скачиваемых данных. Подлинность рабочего сертификата Сервера обновления проверяется на основе построения цепочки сертификатов до CA сертификата Сервера обновления. CA сертификат Сервера обновления устанавливается на каждый Клиент обновления во время первой инсталляции Клиента обновления на vpn-устройство.

Перевыпуск рабочего сертификата Сервера обновления производится по мере необходимости на Сервере обновления. Время жизни рабочего сертификата, среди прочего, зависит и от объема подписываемых данных, то есть от количества обслуживаемых Клиентов обновления и частоты обновлений. Рекомендуемое время жизни рабочего сертификата - от 1 месяца до 1 года.

В комплект поставки продукта VPN Updater входят каталоги и файлы:

```
setup.exe
setup.ini
sysdls.cab
updater_server.cab
updater_server.msi
version.txt
FileZilla_Server-0_9_34.exe
LINUXRHEL5
SOLARIS
```

Установка Сервера обновления осуществляется запуском файла `setup.exe`.

Note

Если на управляемом vpn-устройстве уже инсталлирован продукт CSP VPN Server/CSP VPN Client версии 3.1, то рекомендуется его деинсталлировать, а затем создать заново дистрибутив вместе с Клиентом обновления, как описано в данном документе. При невозможности выполнить деинсталляцию (большое количество клиентов или др.причины) обращайтесь в службу поддержки по адресу support@s-terra.com.

Если на управляемом vpn-устройстве инсталлирован продукт CSP VPN Server/CSP VPN Client версии 3.0, то необходимо перейти на версию 3.1 для сохранения полной функциональности продукта после выполнения обновления.

Схема стенда

В дальнейшем описании документа приведены примеры для стенда (Рисунок 2), в который включен шлюз безопасности с установленным VPN-продуктом CSP VPN Gate, защищающий подсеть с конечным устройством, на котором установлен Сервер обновления. Для удаленного обновления управляемого vpn-устройства в стенде присутствует компьютер с IP-адресом 40.0.0.101/16. Взаимодействие между управляемым vpn-устройством и Сервером обновления осуществляется по IPsec-туннелю, построенному до шлюза безопасности.

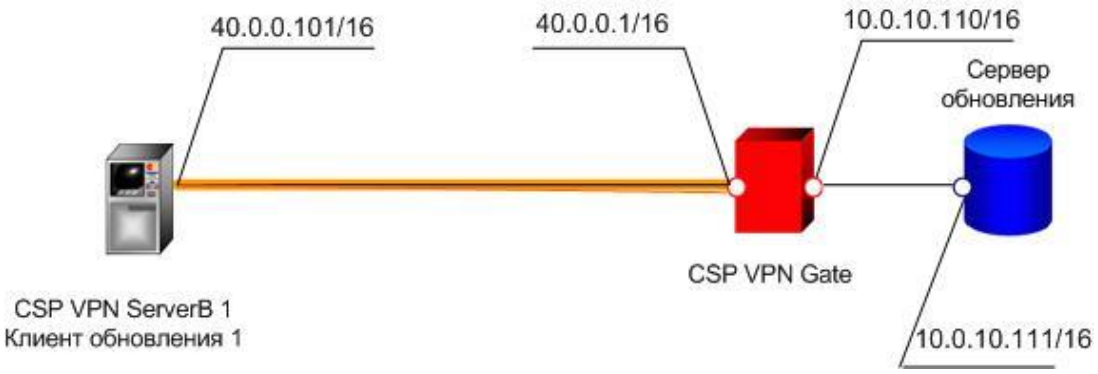

Рисунок 2

Сценарии обновления

Можно выделить два последовательных сценария обновления продукта CSP VPN Agent на управляемом vpn-устройстве. Первый сценарий – подготовка дистрибутивов CSP VPN Agent и Клиента обновления и локальная их установка на управляемом vpn-устройстве. Второй сценарий – создание обновлений на Сервере обновления и передача их vpn-устройству по защищенному VPN соединению.

Далее по тексту управляемые vpn-устройства будем называть клиентами, на которые устанавливается продукт CSP VPN Agent и Клиент обновления.

Сценарий первого обновления

Шаг 1: Установите на выделенный компьютер с установленной ОС Windows Server 2003 Сервер обновления, как описано в разделе «Инсталляция Сервера обновления».

Шаг 2: Настройте Сервер обновления – создайте CA сертификат, рабочий сертификат Сервера обновления, введите лицензию на продукт, как описано в разделе «Настройка Сервера обновления».

Шаг 3: На Сервере обновления для данного управляемого vpn-устройства создайте учетную запись клиента, дистрибутивы Клиента обновления и CSP VPN Agent (см. разделы «Обновление CSP VPN Server/CSP VPN Client», «Обновление CSP VPN Gate»).

Шаг 4: Установите локально на управляемое vpn-устройство сначала дистрибутив CSP VPN Server/CSP VPN Client, а затем – Клиента обновления (см. раздел «Инсталляция Клиента обновления и CSP VPN Server/CSP VPN Client»), а для шлюза – сначала Клиент обновления, затем скрипт с настройками CSP VPN Gate (см. раздел «Инсталляция Клиента обновления и CSP VPN Gate»).

Шаг 5: Установленный Клиент обновления автоматически производит проверку возможности связываться с Сервером обновления и получать обновления.

Сценарий последующих обновлений

Шаг **1:** Сформируйте обновление для данного управляемого vpn-устройства, заполнив форму на Сервере обновления, как описано в разделе «Создание обновлений. Пример успешного обновления клиента». В заданное время автоматически будет создан пакет обновления, который сразу доступен для скачивания.

Шаг 2: Клиент обновления, периодически проверяя наличие доступных для него обновлений, скачает его с Сервера обновления.

Можно задать подряд несколько обновлений с указанием времени создания каждого, и они будут применены в том порядке, в котором были созданы.

Установка и настройка Сервера обновления

Инсталляция Сервера обновления

Инсталляция Сервера обновления осуществляется на выделенном компьютере с установленной ОС Windows Server 2003.

Если планируется управлять vpn-устройствами с установленным продуктом CSP VPN Agent, использующим СКЗИ «КриптоПро CSP 3.6», то на выделенный компьютер установите сначала СКЗИ «КриптоПро CSP 3.6» (вид установки может быть Типовой). СКЗИ потребуется для генерации случайных чисел, используемых при создании ключевых пар на управляемых vpn-устройствах.

Для инсталляции Сервера обновления запустите файл `setup.exe`, который входит в состав дистрибутива продукта VPN Updater. Появится окно с приглашением к инсталляции (Рисунок 3), нажмите кнопку Next.

Рисунок 3

Папку, в которую будет установлен Сервер обновления, оставьте без изменений (Рисунок 4).

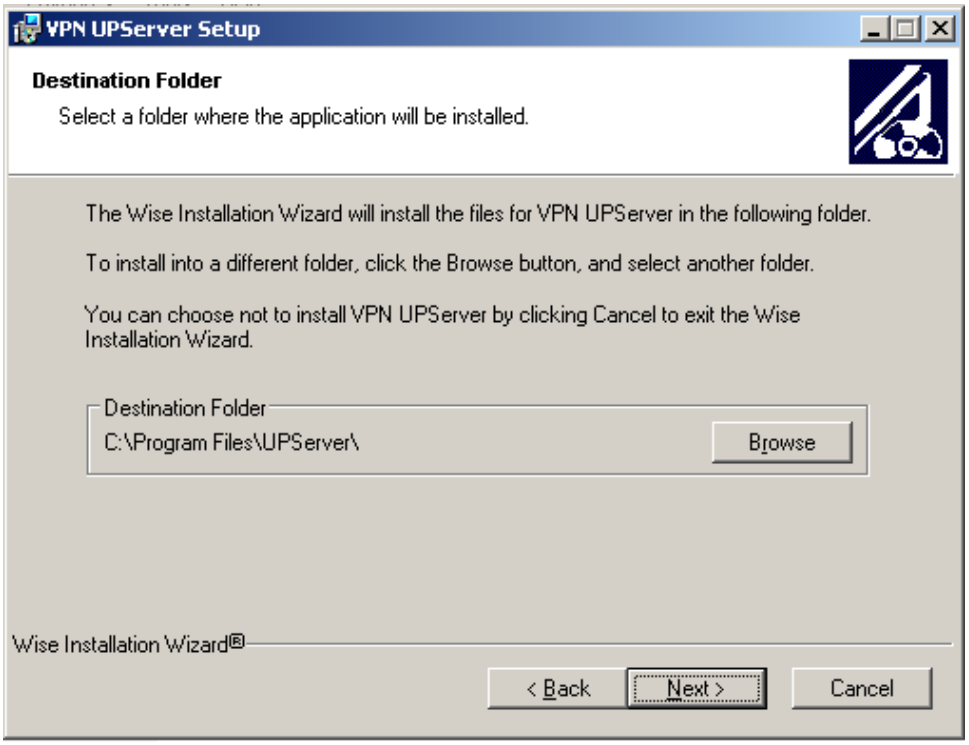

Рисунок 4

Подтвердите готовность к инсталляции – нажмите кнопку Next (Рисунок 5), после чего начнется процесс инсталляции.

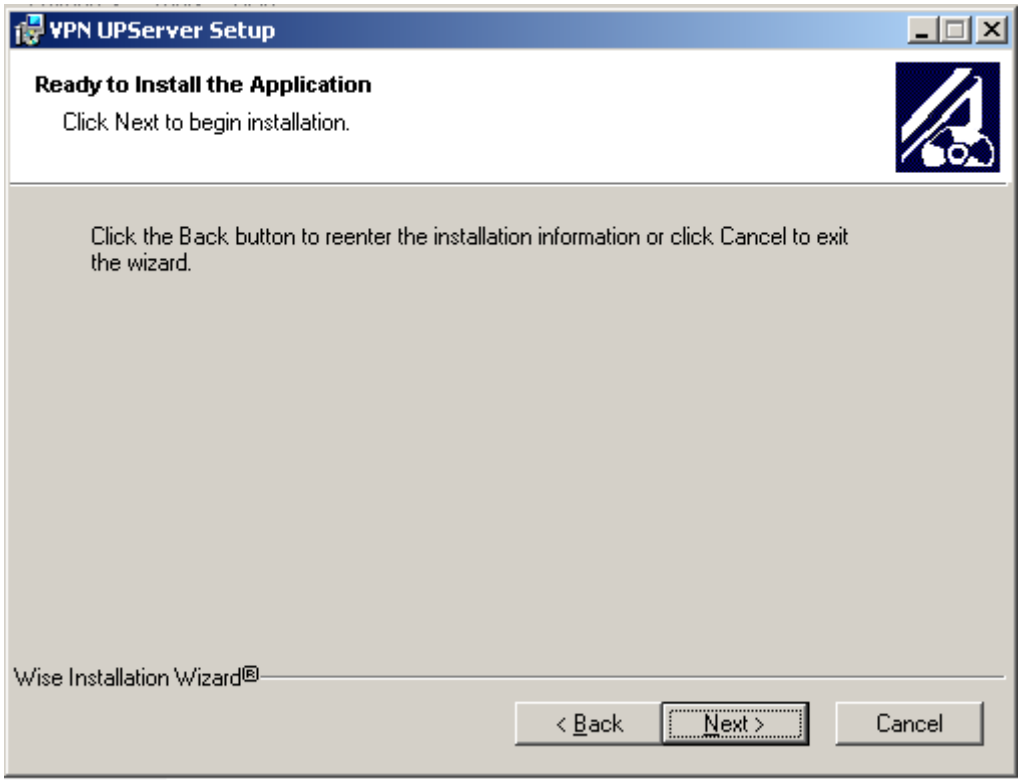

Рисунок 5

Далее появится окно с приглашением к инсталляции продукта FileZilla Server (Рисунок 6). Примите условия лицензионного соглашения – нажмите кнопку I Agree.

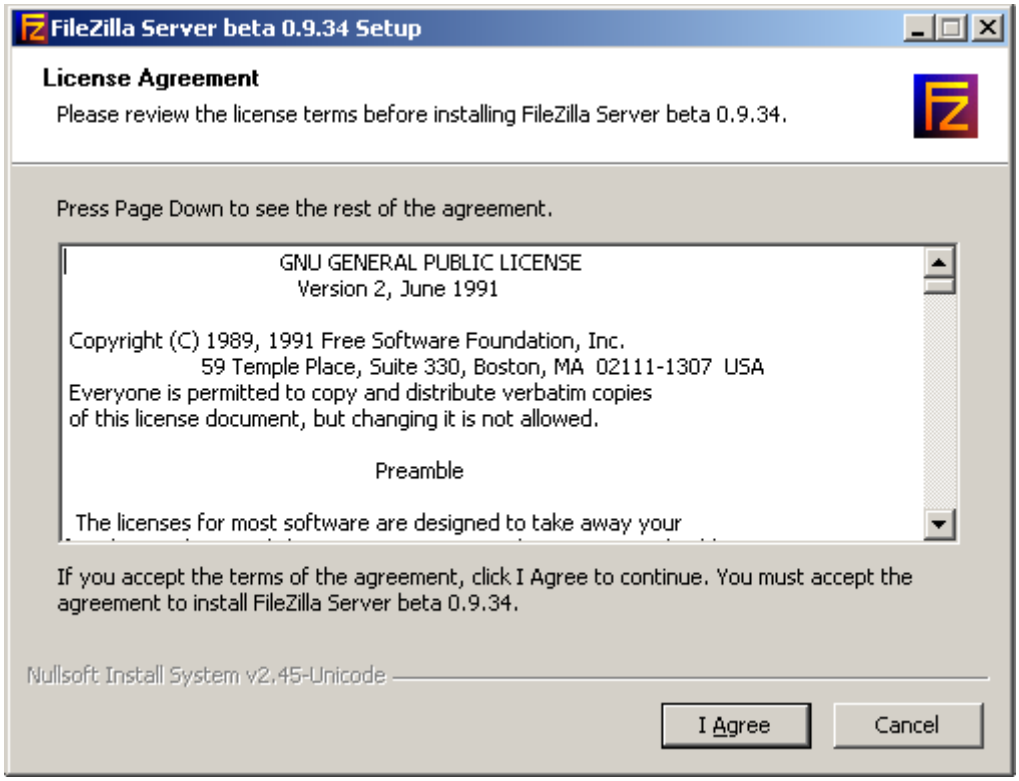

Рисунок 6

В следующем окне (Рисунок 7) предлагается выбрать компоненты для инсталляции. Оставьте настройки по умолчанию и нажмите кнопку Next.

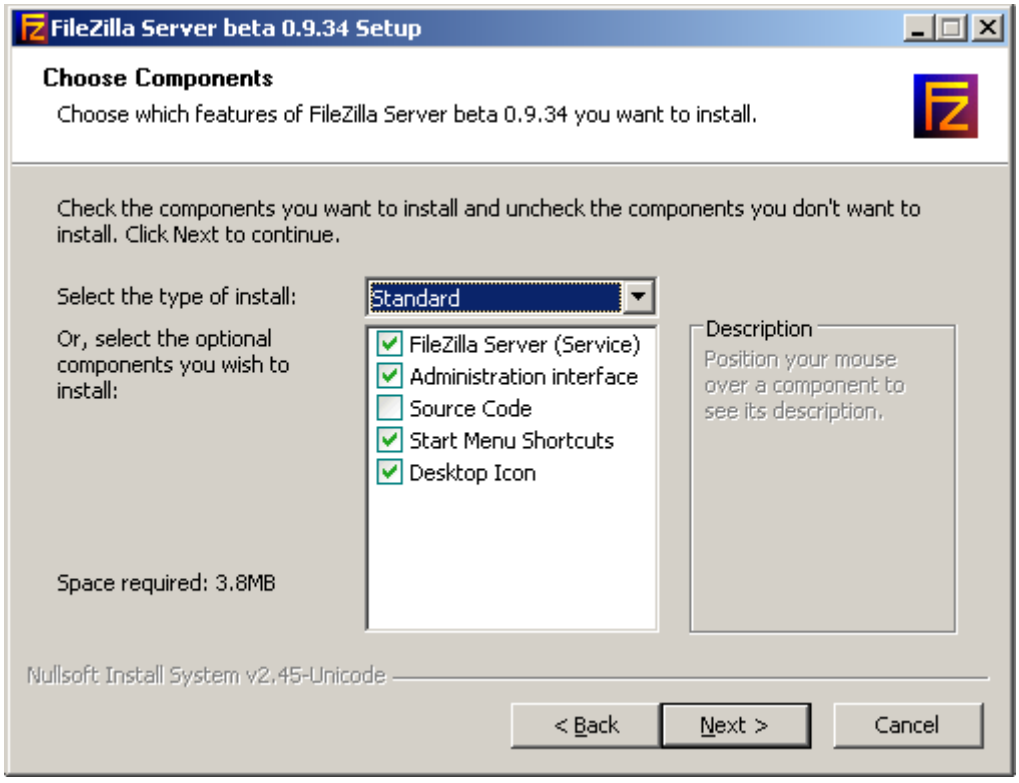

Рисунок 7

Укажите папку, в которую будет установлен продукт FileZilla Server (Рисунок 8).

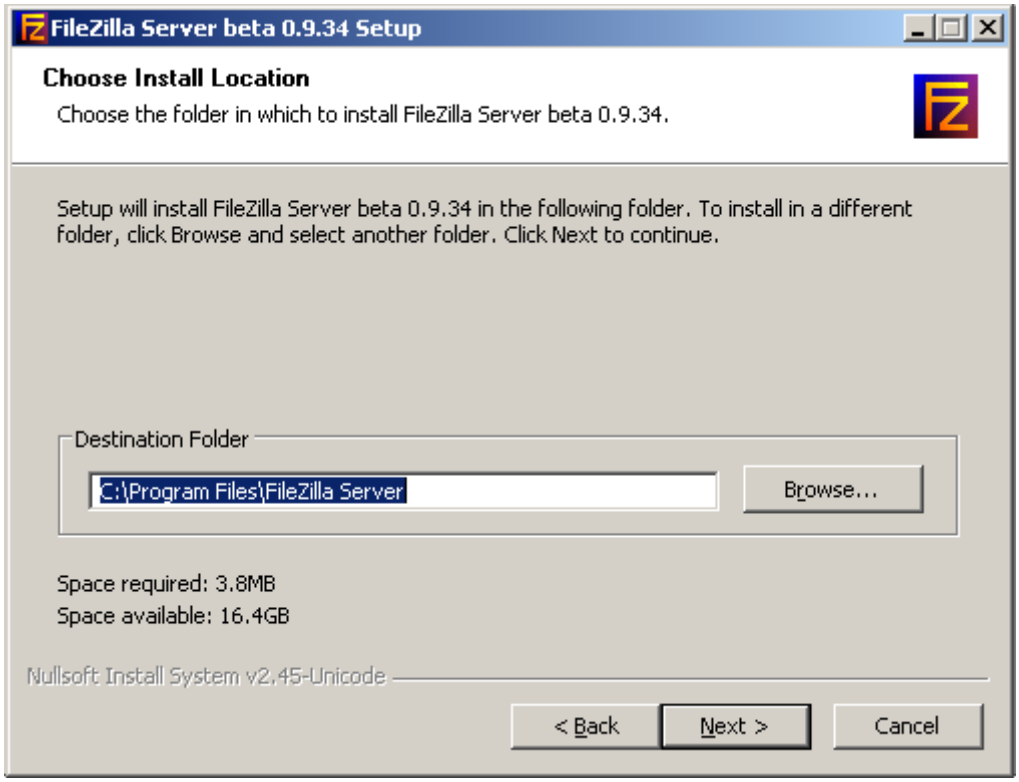

Рисунок 8

В окне выбора настроек для запуска сервиса продукта FileZilla Server оставьте значения по умолчанию и нажмите кнопку Next (Рисунок 9).

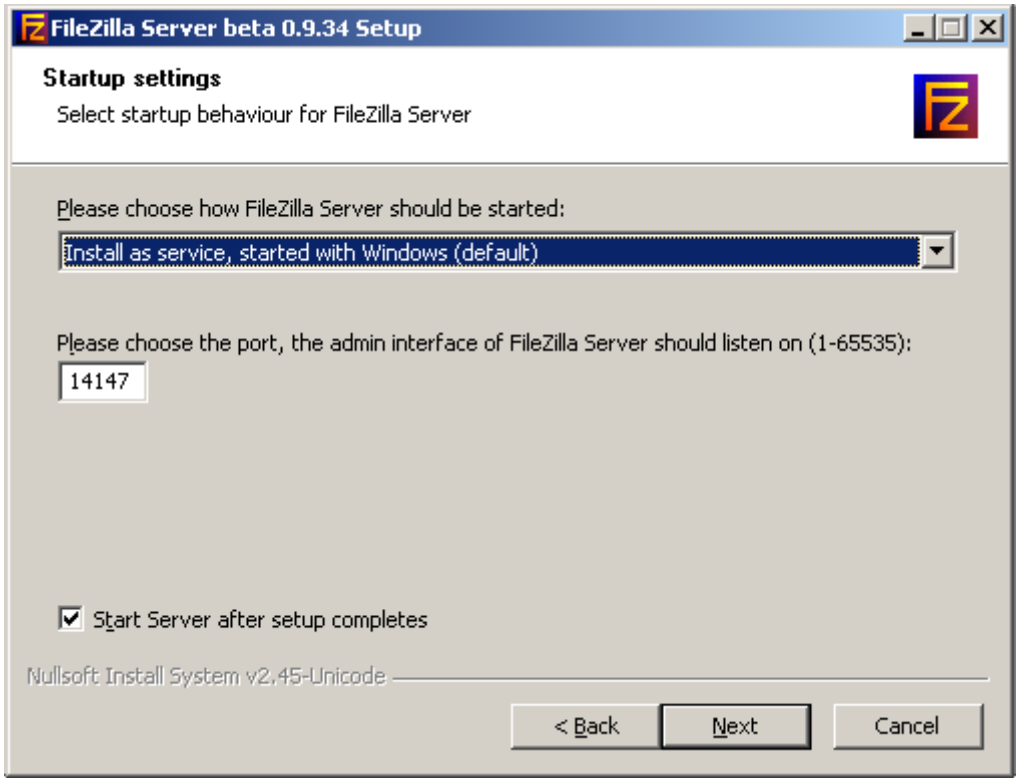

Рисунок 9

В окне с настройками старта консоли управления продуктом FileZilla Server оставьте значения по умолчанию и нажмите кнопку Install (Рисунок 10), после чего запустится процесс установки.

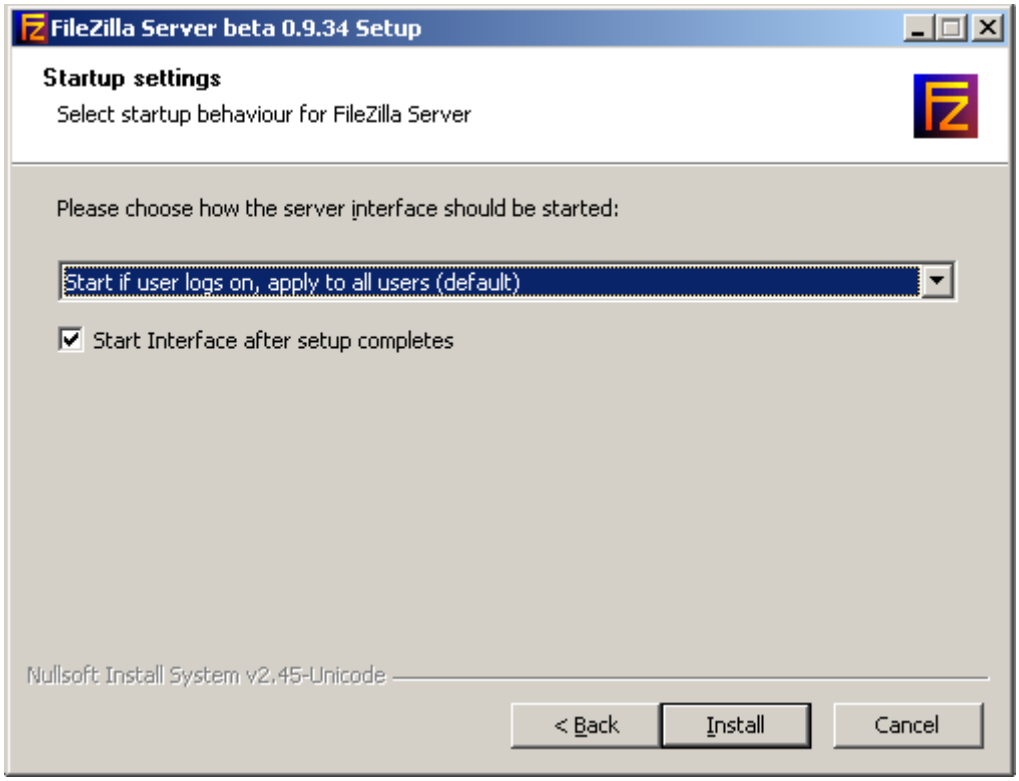

Рисунок 10

По завершению процесса установки нажмите кнопку Close (Рисунок 11).

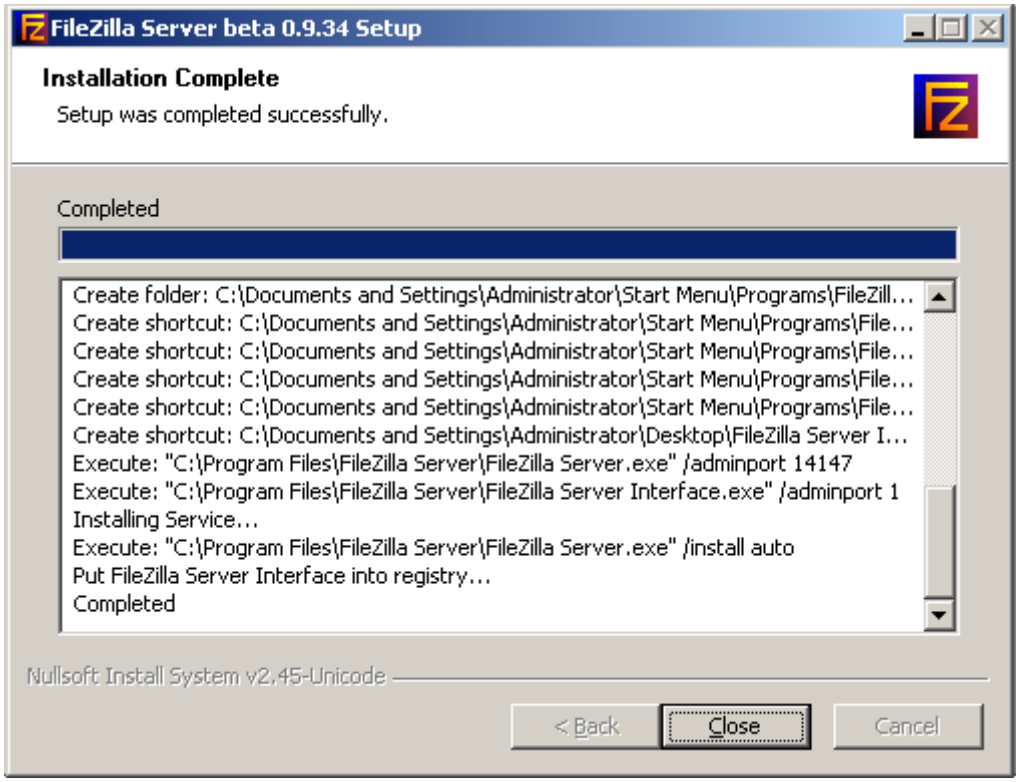

Рисунок 11

Запустится консоль управления продуктом FileZilla Server (Рисунок 12), нажмите кнопку OK.

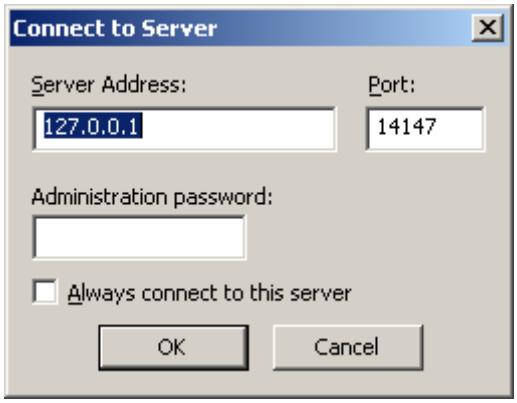

Рисунок 12

Далее должно произойти установление соединения с сервером FileZilla Server (Рисунок 13).

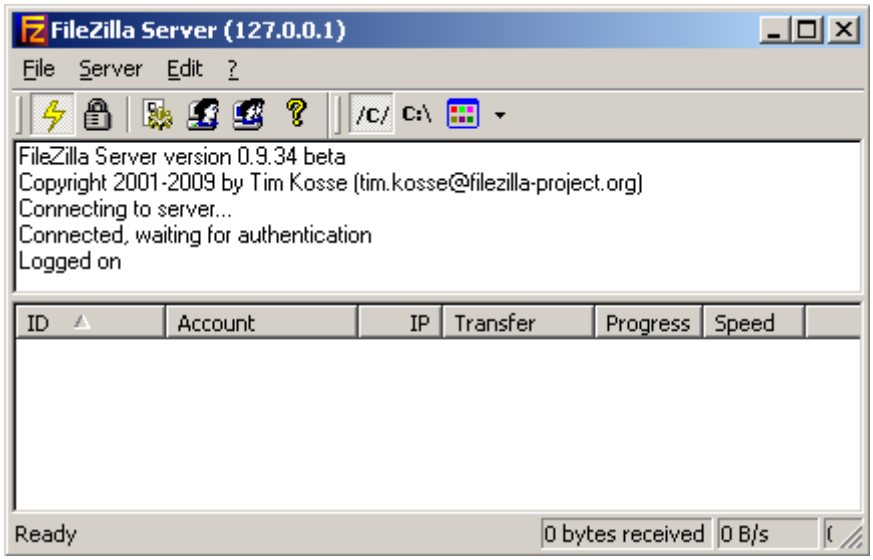

Рисунок 13

После успешного соединения можно закрыть окно консоли продукта FileZilla Server.

Закончите установку продукта Сервер обновления. Нажмите кнопку Finish, процесс инсталляции будет завершен (Рисунок 14).

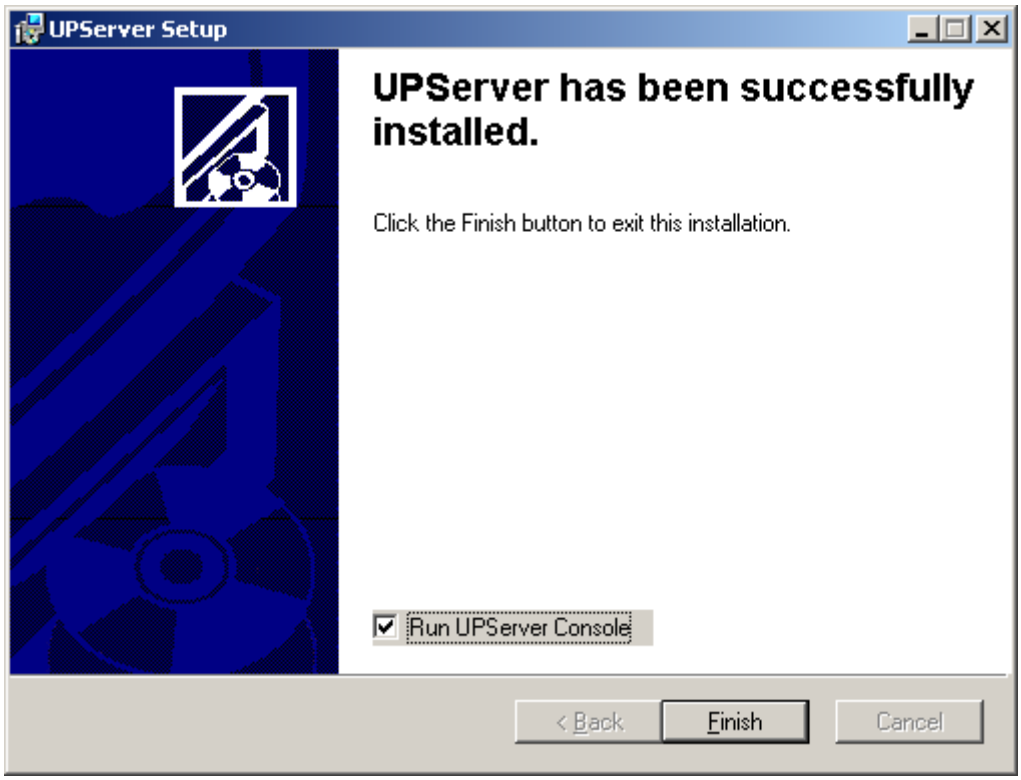
UPServer Setup
UPServer has been successfully installed.
Click the Finish button to exit this installation.
Run UPServer Console
< Back
Finish
Cancel

Рисунок 14

Настройка Сервера обновления

Настройка и управление Сервером обновления производится при помощи специального приложения UPServer Console (`Пуск-Программы-VPN Updater-VPN UPServer Console`) (Рисунок 15).

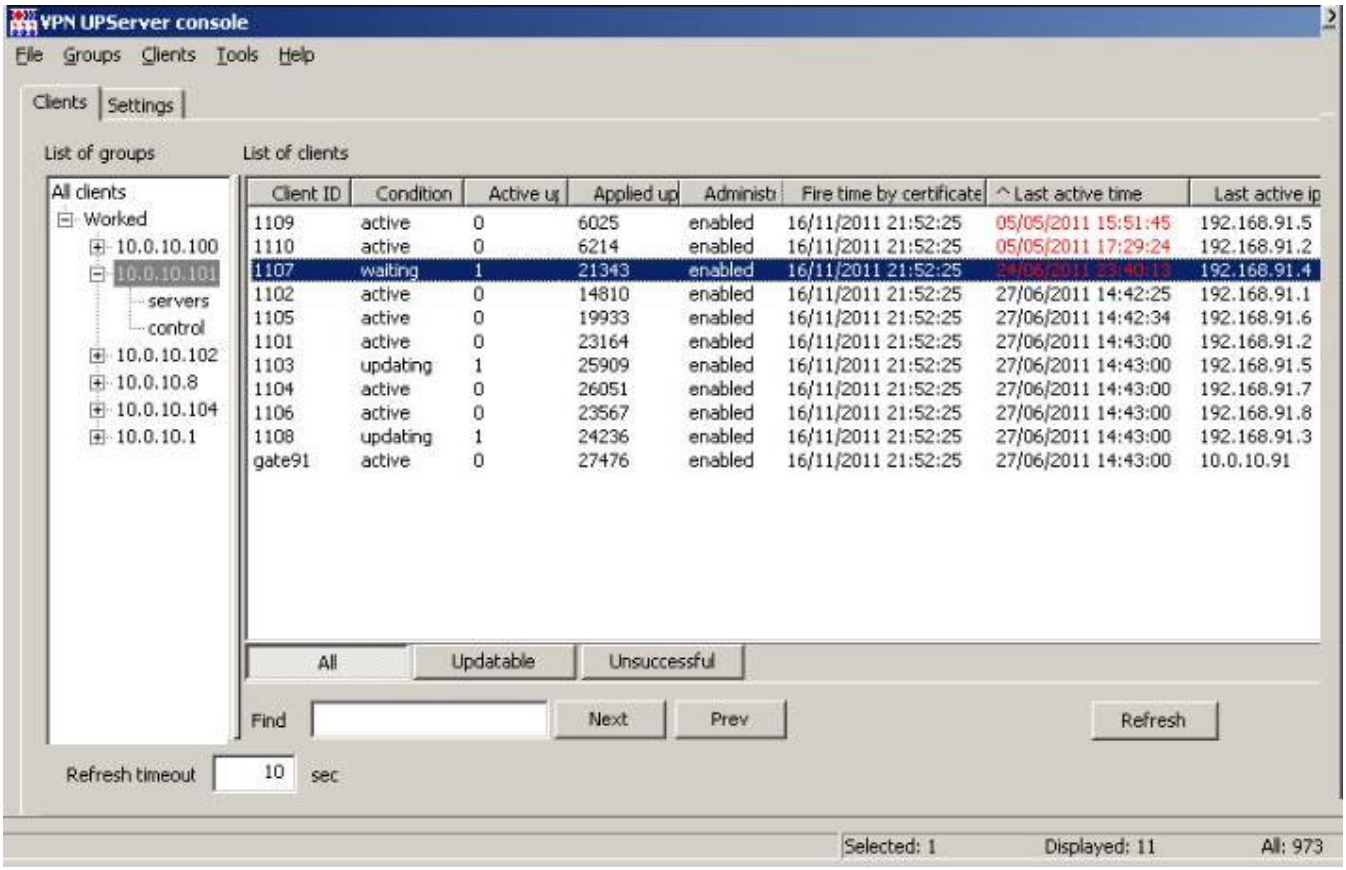

Рисунок 15

Меню этого графического интерфейса описано в главе «Описание меню Сервера обновления».

Начальная настройка Сервера обновления производится во вкладке ***Settings***, а настройка и управление клиентами – во вкладке ***Clients***.

При первом запуске приложения VPN UPServer Console выводится предупреждение о необходимости задать настройки продукта ***Сервер обновления*** (Рисунок 16).

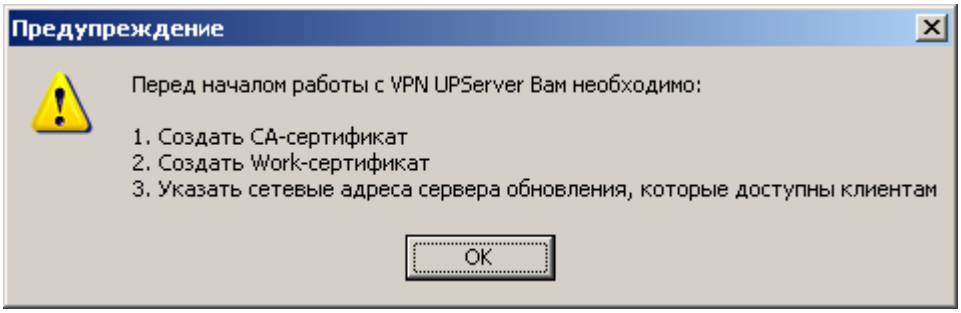

Рисунок 16

Нажмите кнопку OK, откроется окно настроек продукта Сервер обновления (Рисунок 17). Во вкладке Settings введите данные лицензии, создайте CA-сертификат и рабочий сертификат (work certificate) Сервера обновления, а также задайте сетевые адреса Сервера обновления.

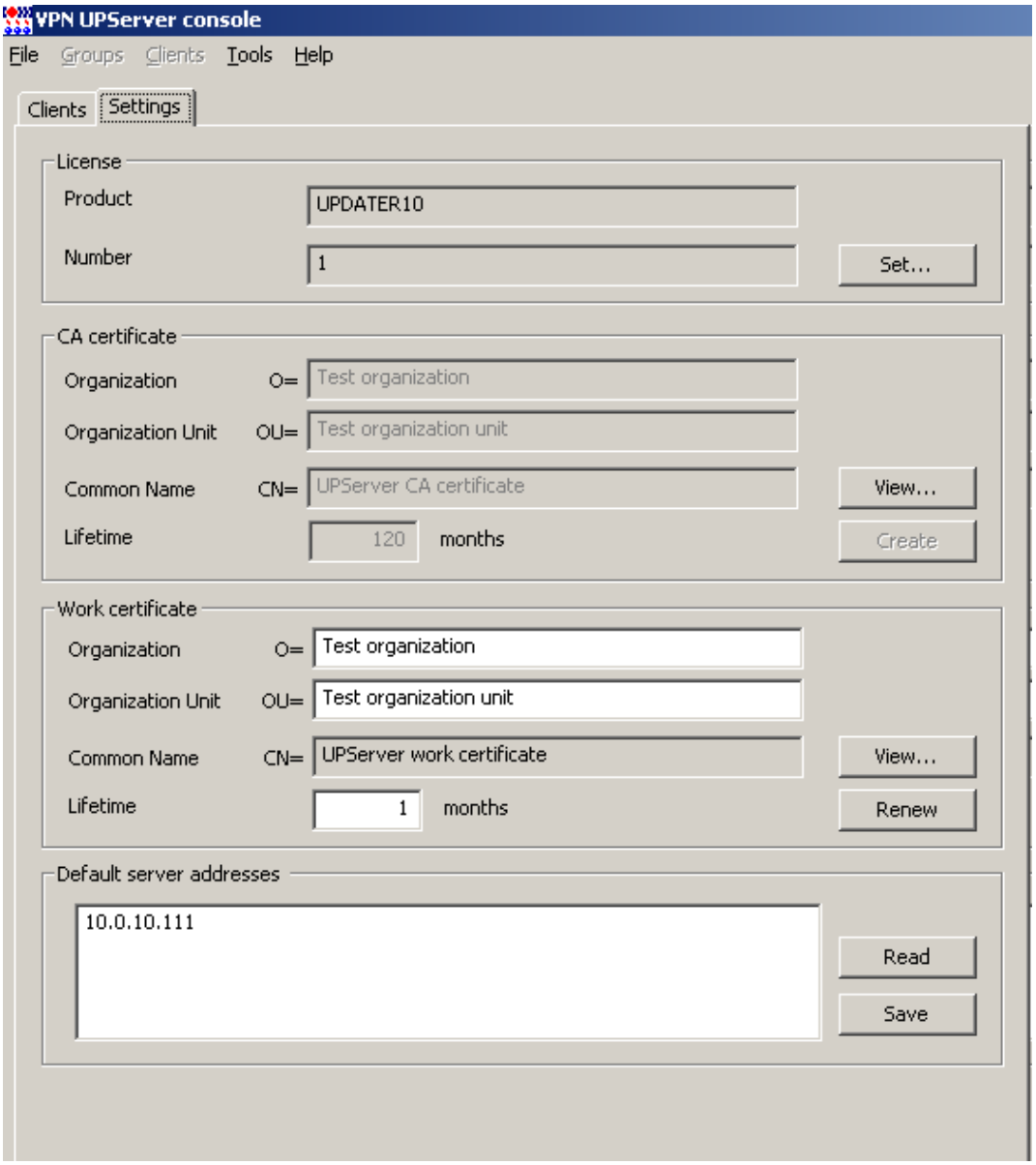

Рисунок 17

Ввод лицензии

Для ввода лицензии на продукт ***Сервер обновления*** нажмите кнопку `Set…`(Рисунок 17).

В появившемся окне Set license (Рисунок 18):

- в поле Product выберите тип продукта из выпадающего списка:

  UPDATER10 – продукт будет работать с количеством Клиентов обновления не более 10

  UPDATER100 – продукт будет работать с количеством Клиентов обновления не более 100

  UPDATER500 – продукт будет работать с неограниченным количеством Клиентов обновления

- в поле Customer code укажите название организации, которой выдана лицензия
- в поле License number введите номер лицензии
- в поле License code введите код лицензии.

Если лицензия была получена в виде файла, то нажмите кнопку `Load from file…` и данные для заполнения полей будут взяты из этого файла.

Если лицензия на продукт не введена, то продукт будет работать с пятью Клиентами обновления и не больше.

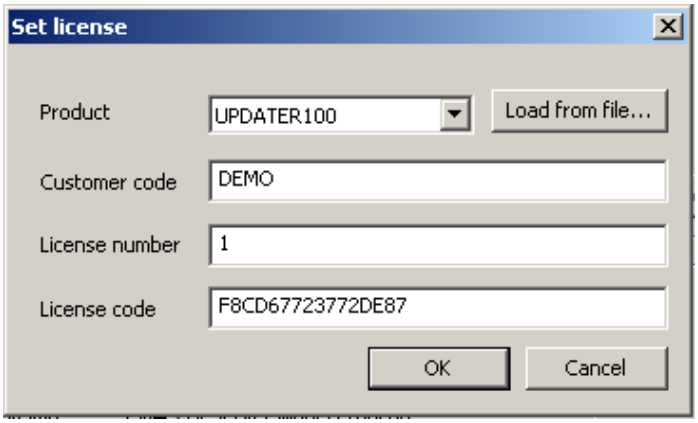

Рисунок 18

Создание CA сертификата

Для создания CA-сертификата ***Сервера обновления*** заполните поля в группе CA certificate (Рисунок 17), например, следующими значениями:

```
O=Test organization
OU=Test organization unit
```

После этого нажмите кнопку `Create`. Перед созданием CA сертификата будет выдано предупреждение (Рисунок 19).

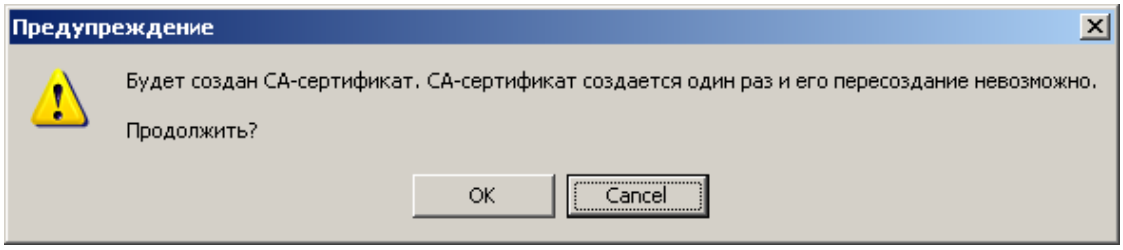

Рисунок 19

Если поля для CA сертификата заполнены верно – нажмите кнопку OK.

После успешного создания CA сертификата будет выдано подтверждение (Рисунок 20). Нажмите кнопку OK и вернитесь в окно настроек.

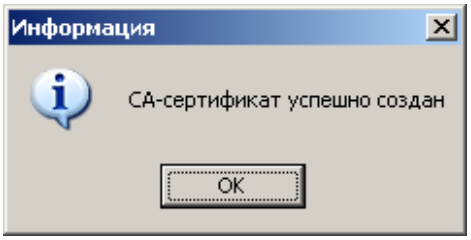

Рисунок 20

Созданный CA-сертификат и его секретный ключ будут храниться в сертификатном хранилище операционной системы. Ключ можно экспортировать и сохранить на другом компьютере для предотвращения потери CA-сертификата при поломке компьютера, на котором установлен Сервер обновления. Замена используемого CA-сертификата Сервера обновления возможна на клиенте только локальной доставкой (инструкция такой замены будет выдаваться по запросу для восстановления системы).

CA-сертификат ***Сервера обновления*** создается только один раз. После каждого выпуска CA-сертификата Сервера обновления необходима локальная доставка нового CA-сертификата на все контролируемые клиенты.

Создание рабочего сертификата

Заполните поля рабочего сертификата Сервера обновления в группе Work certificate (Рисунок 17) и нажмите кнопку `Create`. Перед созданием сертификата будет выдано предупреждение (Рисунок 21):

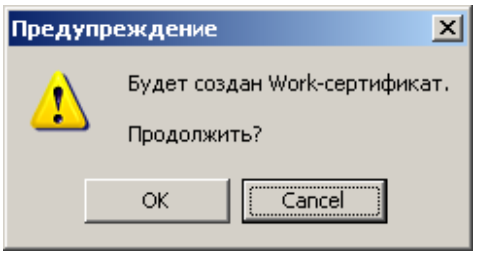

Рисунок 21

Если поля для рабочего сертификата заполнены верно – нажмите кнопку OK.

После успешного создания сертификата будет выдано подтверждение создания рабочего сертификата (Рисунок 22), нажмите кнопку OK в этом окне.

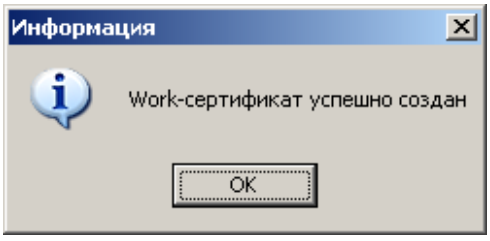

Рисунок 22

После этого кнопка `Create` в группе Work certificate изменится на `Renew` (Рисунок 17).

Задание адресов Сервера обновления

Далее в группе Default server addresses (Рисунок 17) задайте список сетевых адресов Сервера обновления, которые доступны с управляемых vpn-устройств, следуя при этом следующим правилам:

- каждый адрес должен располагаться на отдельной строке, перевод строки осуществляется нажатием клавиши Enter или `Ctrl-Enter`
- сетевой адрес представляет собой IP-адрес или DNS-имя, которое будет транслироваться в IP-адрес на vpn-устройстве в момент создания соединения с Сервером обновления.

После задания адресов обязательно нажмите кнопку `Save`, появится предупреждение (Рисунок 23). Если адреса введены верно, то нажмите кнопку OK, при этом происходит проверка введенных данных и только после этого во все создаваемые дистрибутивы Клиентов обновления по умолчанию будет вноситься список адресов Сервера обновления.

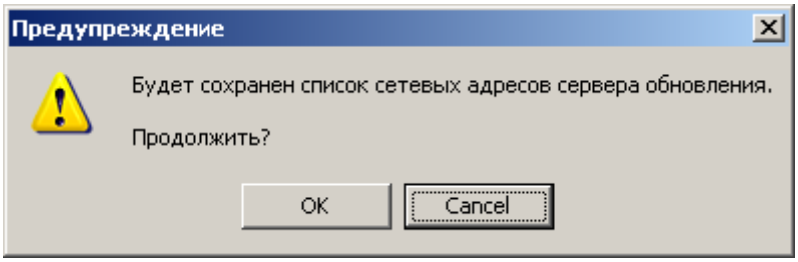

Рисунок 23

Note

На данном этапе категорически не рекомендуется задавать адреса, не принадлежащие Серверу обновления. Адреса, не принадлежащие Серверу обновления, могут быть указаны только при процедуре перевода клиентов на другой Сервер обновления. Инструкция по переводу клиентов на другой Сервер обновления будет выдаваться по запросу пользователя при появлении такой потребности.

Далее перейдите во вкладку `Clients`, создайте учетную запись для каждого управляемого vpn-устройства, дистрибутивы Клиента обновления и CSP VPN Agent.

Обновление CSP VPN Server/CSP VPN Client

Создание клиента на Сервере обновления

На Сервере обновления во вкладке Clients отражается информация обо всех управляемых vpn-устройствах. Эта вкладка предназначена для создания, удаления учетных записей клиентов для управляемых устройств, создания для них Клиентов обновления, обновлений, приостановки работы с клиентом и т.д.

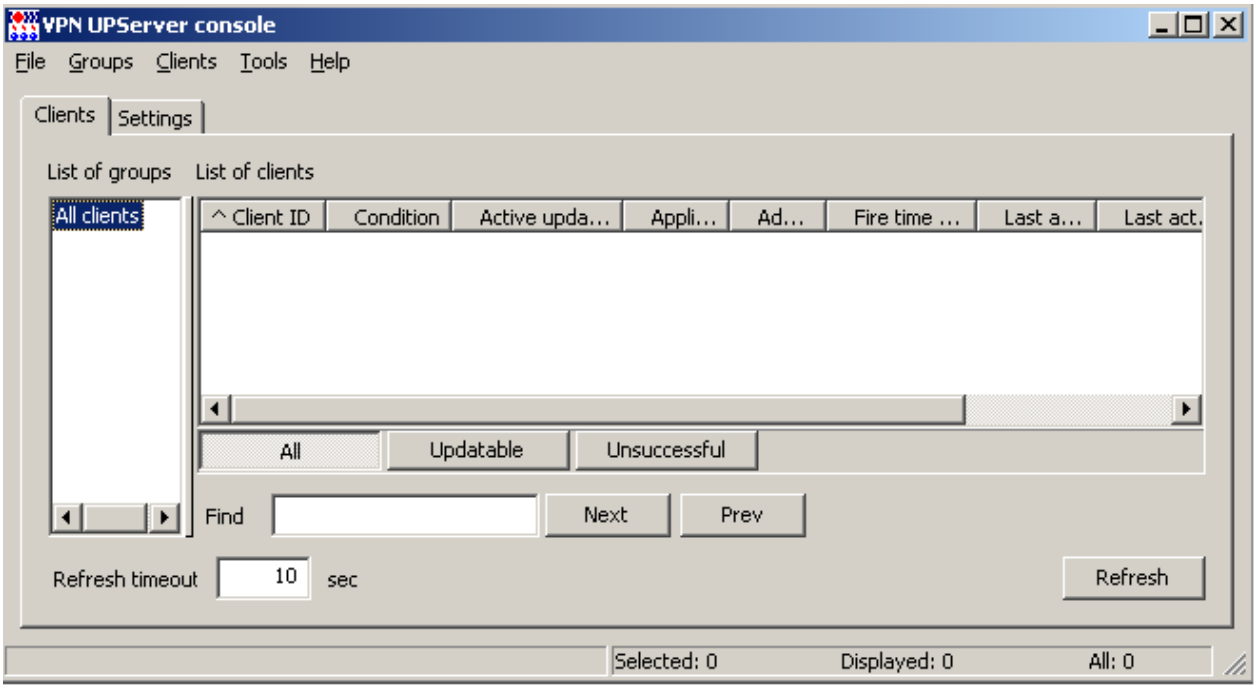

Рисунок 24

Опишем интерфейс вкладки Clients.

`List of groups` – древовидная структура списков групп клиентов, объединенных администратором по территориальному или организационному признаку расположения управляемых компьютеров

`List of clients` – таблица со списком клиентов, входящих в выделенную группу. Столбцы таблицы имеют следующие значения:

`Client ID` – уникальный идентификатор клиента

`Condition` – состояние Клиента обновления, может принимать следующие значения:

- `new` – Клиент обновления зарегистрирован на Сервере обновления и еще ни разу не выходил на связь по сети
- `active` – Клиент обновления готов к приему обновлений
- `waiting` – обновление для клиента создано и выложено на FTP-сервер и ожидается, что Клиент обновления начнет его скачивание
- `updating` – Клиент обновления применяет обновление (в данном состоянии Клиент обновления находится с момента, когда он обнаружил обновление на Сервере обновления и до момента, когда он его применил или отвергнул)
- `failed` – Клиент обновления не смог применить очередное обновление (в этом состоянии клиент продолжает работу на предыдущем комплекте обновления, попытки по применению обновления не предпринимаются, пока

администратор не изменит это состояние на `active`, отменив неуспешное обновление). Ошибка детектируется на основании невозможности скачать то же обновление с Сервера обновления при примененном обновлении

`Active updates` – количество еще неприменeнных обновлений

`Applied updates` – количество успешно примененных обновлений

`Administrative state` – административное состояние обслуживания Клиента обновления, может принимать следующие значения:

- `enabled` – Клиент обновления обслуживается
- `disabled` – Клиент обновления не обслуживается (все его обращения к серверу игнорируются)

`Fire time by certificates` – ближайшая дата и время истечения срока действия одного из сертификатов, размещенных в базе продукта CSP VPN Agent

`Last active time` – дата и время последнего удачного FTP-соединения клиента (когда клиент удачно аутентифицировался на FTP-сервере)

`Last active ip-address` – IP-адрес клиента, с которого было осуществлено последнее удачное FTP-соединение

`Group` – имя группы, к которой принадлежит клиент.

Допускается сортировка по столбцам таблицы клиентов. Значком ^ метится столбец по которому сортируются данные, если данные в таком столбце одинаковые, то они сортируются по Client ID.

Вкладка Clients имеет следующие **кнопки управления**:

для фильтрации отображаемой в таблице информации:

- `All` – в таблице отображаются все клиенты группы
- `Updatable` – в таблице отображаются только те клиенты, которые имеют хотя бы одно неприменeнное обновление или находятся в состоянии не `active`.
- `Unsuccessful` – в таблице отображаются клиенты в состоянии `failed`, которые не смогли применить очередное обновление

`Find` – поле для ввода строки, по которой будет происходить поиск клиентов в таблице, содержащих данную строку в любом поле. Если такой клиент найден - он выделяется в списке клиентов.

`Next` – кнопка запуска поиска следующего клиента, относительно выделенного, удовлетворяющего заданной строке в поле Find. Аналогично нажатию клавиши F3

`Prev` – кнопка запуска поиска предыдущего клиента, относительно выделенного, удовлетворяющего заданной строке в поле Find. Аналогично нажатию клавиш Shift-F3

`Refresh timeout` – поле, в котором задается период времени в секундах обновления информации в таблице клиентов

`Refresh` – кнопка для принудительного обновления информации в таблице клиентов. Нажатие кнопки дает команду для сбора информации обо всех существующих клиентах. Так как процесс сбора информации может быть долговременным, то ожидание по кнопке `Refresh` производится только для выделенных на данный момент клиентов. Отображение обновленной информации для всех остальных клиентов будет произведено позднее, по мере получения полной информации. Аналогично нажатию клавиши F5.

Нижняя строка вкладки отражает:

`Selected` – количество выделенных на данный момент клиентов

`Displayed` - количество отображаемых на данный момент клиентов

`All` - количество всех клиентов на ***Сервере обновления***.

Для создания группы во вкладке Clients выделите группу All clients, а в меню Groups выберите предложение Create (Рисунок 25).

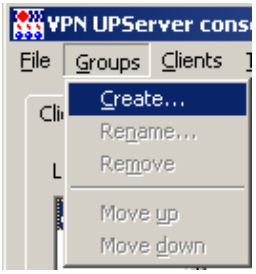

Рисунок 25

В поле Group name введите имя группы, в которой будут созданы в дальнейшем клиенты, например, Office1 (Рисунок 26) и нажмите OK.

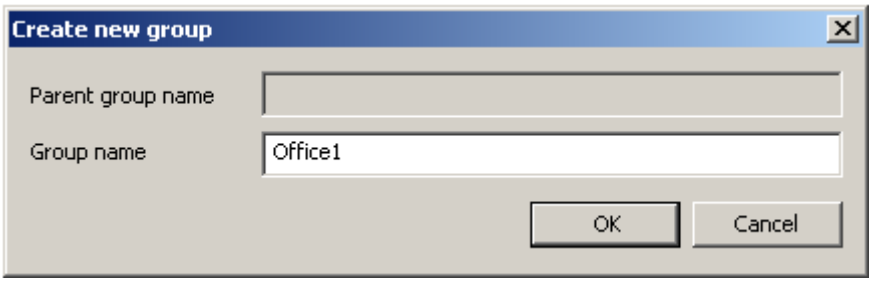

Рисунок 26

В меню Clients выберите предложение Create (Рисунок 27).

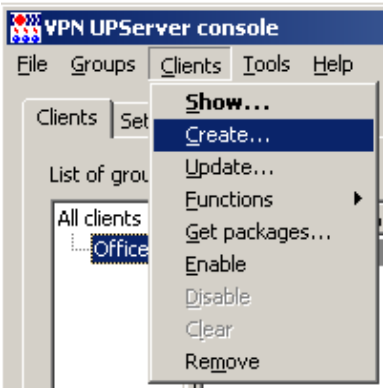

Рисунок 27

Появившееся окно (Рисунок 28) создания нового клиента имеют следующие поля:

- `Client ID` – уникальный идентификатор клиента, может состоять из любых символов, за исключением следующих: <ПРЯМОЙ СЛЕШ>, <ОБРАТНЫЙ СЛЕШ>, <ДВОЕТОЧИЕ>, <ЗВЕЗДОЧКА>, <СИМВОЛ ВОПРОСА>,<ДВОЙНЫЕ КОВЫЧКИ>, <ЗНАК МЕНЬШЕ>, <ЗНАК БОЛЬШЕ>, <ВЕРТИКАЛЬНАЯ ЧЕРТА>, <ТАБУЛЯЦИЯ>. Идентификатор не должен начинаться или заканчиваться символами <ПРОБЕЛ> или <ТОЧКА>, и не должен быть равен “NUL” или “CON” или “COMx”, где x∈[0..9]
- `Product package` – имя файла дистрибутива CSP VPN Server/CSP VPN Client (который был создан с помощью продукта CSP VPN Server AdminTool/ CSP VPN Client AdminTool) или имя файла с данными продукта CSP VPN Server/CSP VPN Client, созданного с помощью окна VPN data maker, вызываемого кнопкой E

- `UPAgent folder` – имя каталога, содержащего дистрибутив Клиента обновления, по умолчанию он уже задан
- `UPAgent settings` – имя файла, содержащего настройки Клиента обновления, по умолчанию имя файла уже задано (см. главу «Настройки Клиента обновления»).

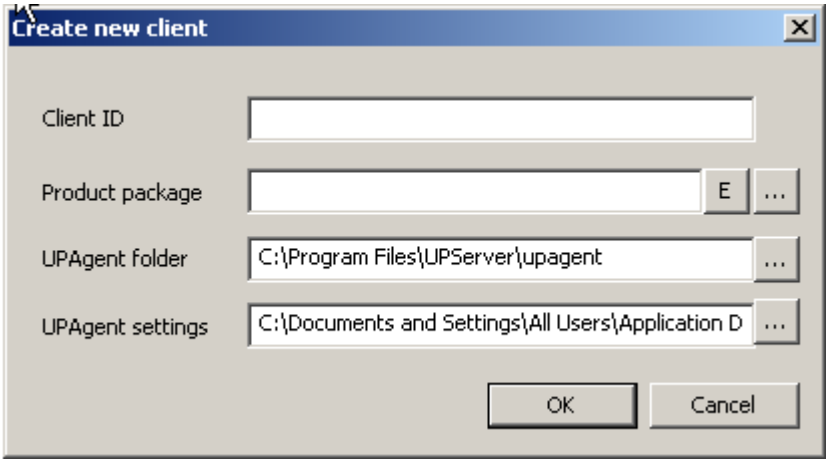

Рисунок 28

В поле Client ID введите идентификатор клиента, например, server01.

Поля `UPAgent folder, UPAgent settings` оставьте без изменений.

В поле `Product package` нажмите кнопку E, появится окно VPN data maker (Рисунок 29), в котором можно задать политику безопасности и все настройки продукта CSP VPN Server/CSP VPN Client.

В целях тестирования создадим файл проекта CSP VPN Server:

- в поле VPN product type выберем Server (Рисунок 29)

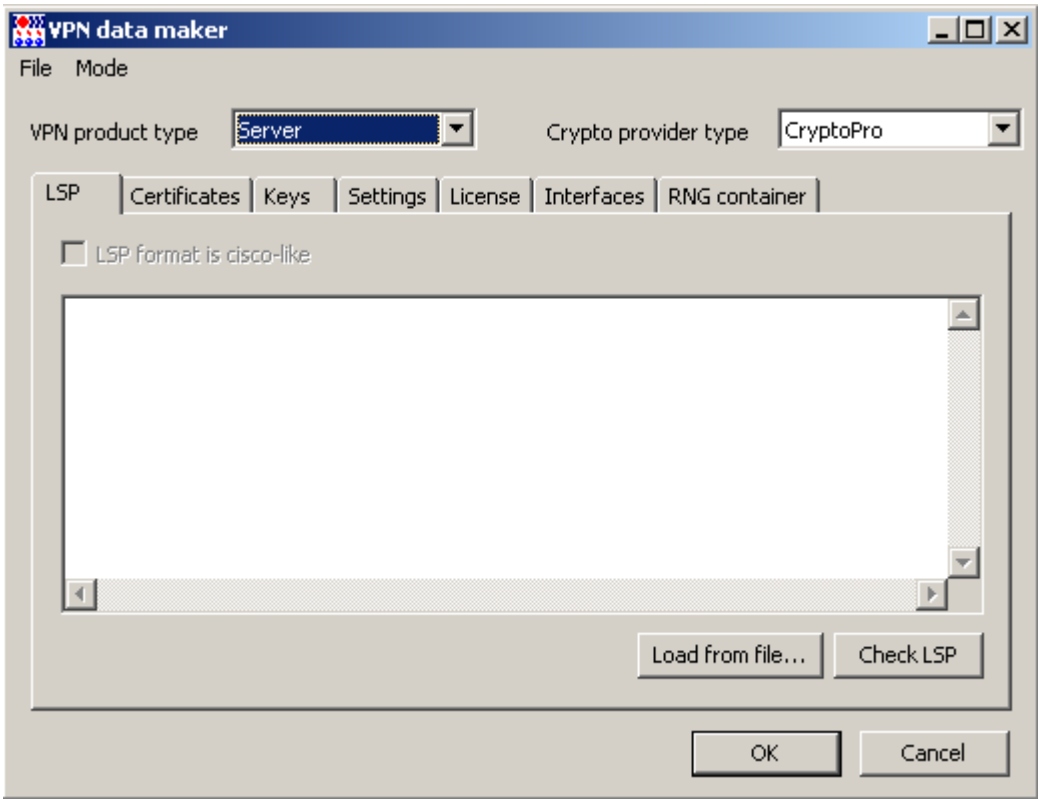

Рисунок 29

- во вкладку LSP скопируем следующую политику безопасности, которая разрешает любой сетевой трафик (Рисунок 30).

```
GlobalParameters (
 Title = "Test LSP"
 Version = "3.1"
 CRLHandlingMode = BEST_EFFORT
)
FilterEntry local_entry_00_00(
)
FilterEntry remote_entry_00_00(
)
FilteringRule filter_rule_00_00(
 LocalIPFilter *= local_entry_00_00
 PeerIPFilter *= remote_entry_00_00
 Action *= (PASS)
)
```

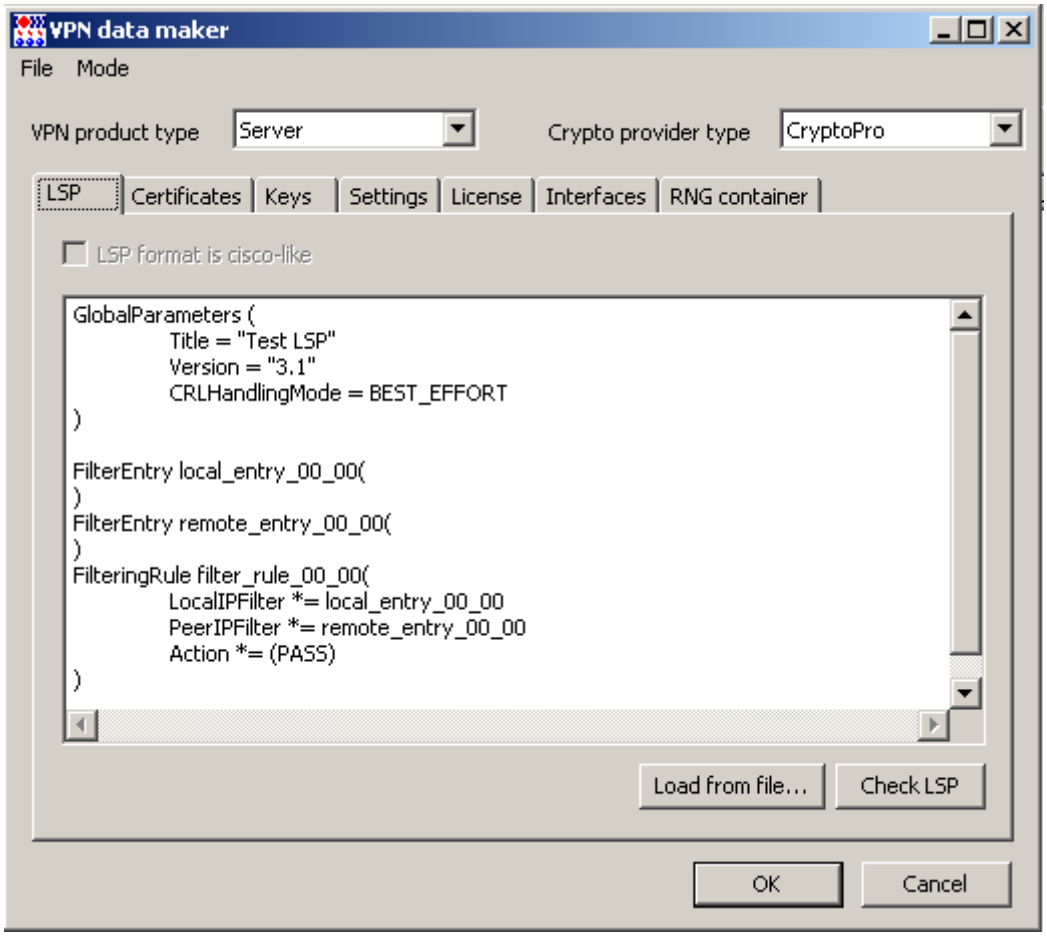

Рисунок 30

- во вкладку License введем данные лицензии (Рисунок 31).

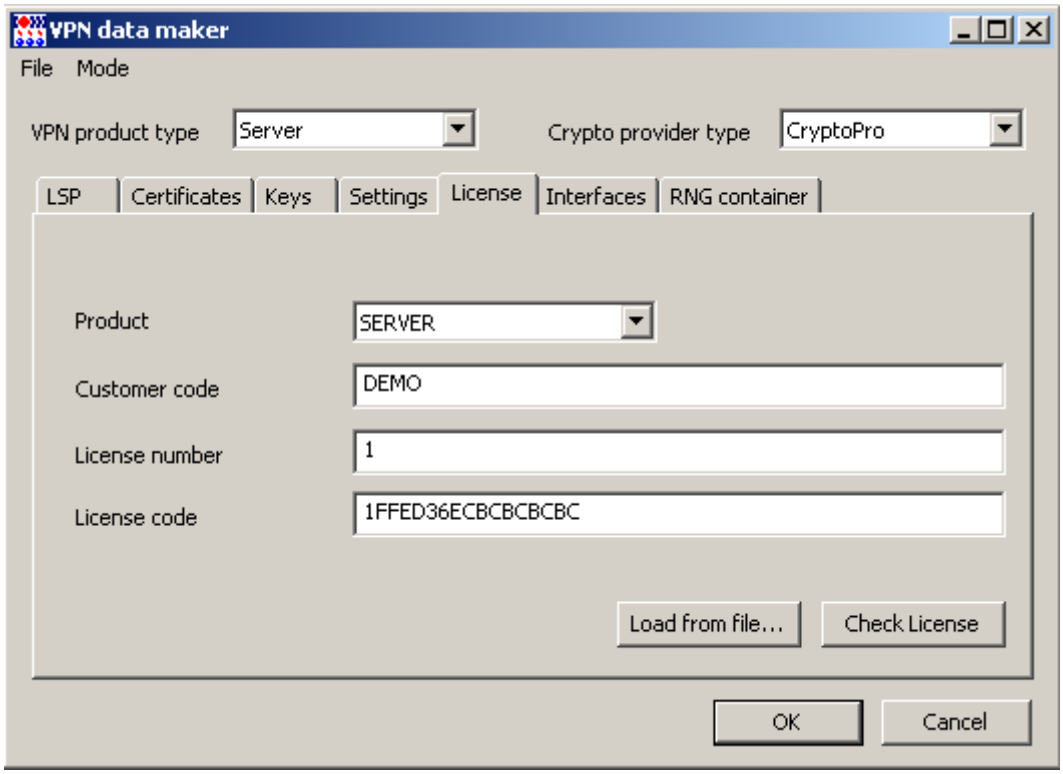

Рисунок 31

- необходимые данные заданы, нажмите кнопку OK (Рисунок 31).

Создается файл с данными продукта CSP VPN Server, имя этого файла прописывается в поле Product package и происходит возврат в окно создания нового клиента (Рисунок 32). Таким образом, все параметры нового клиента заданы, нажмите OK.

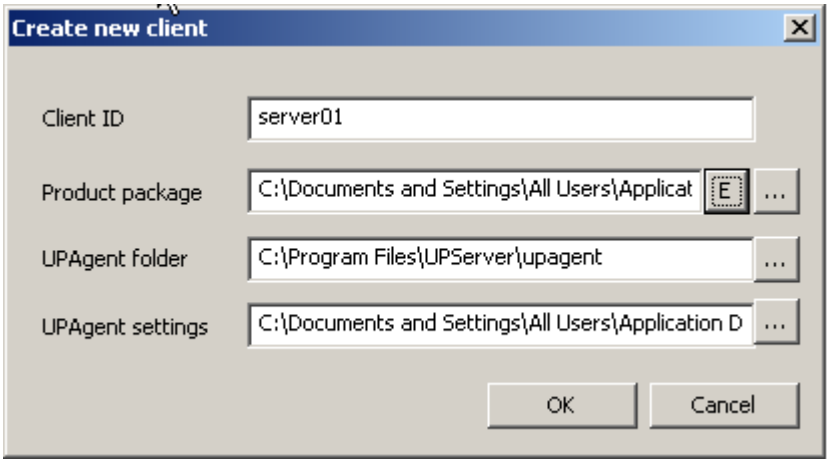

Рисунок 32

Будет создан новый клиент и его отображение появится в таблице клиентов с административным статусом `disabled` для предотвращения преждевременной сетевой активности (Рисунок 33).

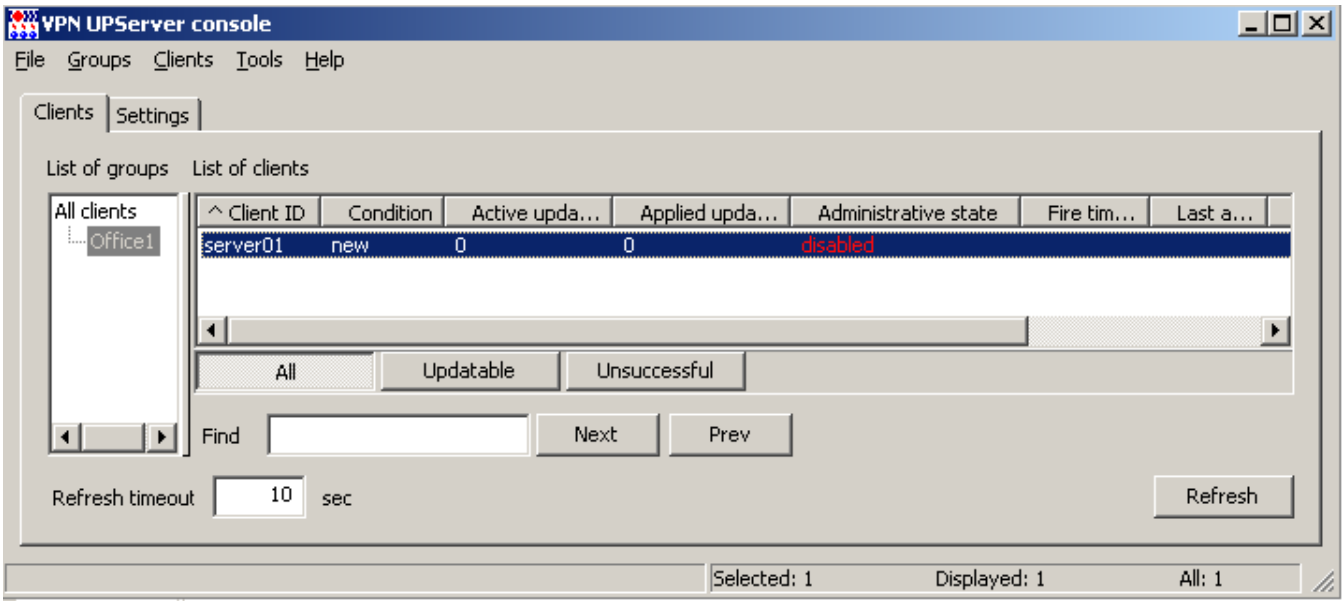

Рисунок 33

Таким образом, создана учетная запись для управляемого vpn-устройства на Сервере обновления.

Создание дистрибутивов Клиента обновления и CSP VPN Server/CSP VPN Client

Далее необходимо сформировать дистрибутивы Клиента обновления и продукта CSP VPN Server/CSP VPN Client для созданного клиента. В таблице клиентов выделите строку с нужным клиентом и в меню Clients выберите операцию `Get packages…` (Рисунок 34).

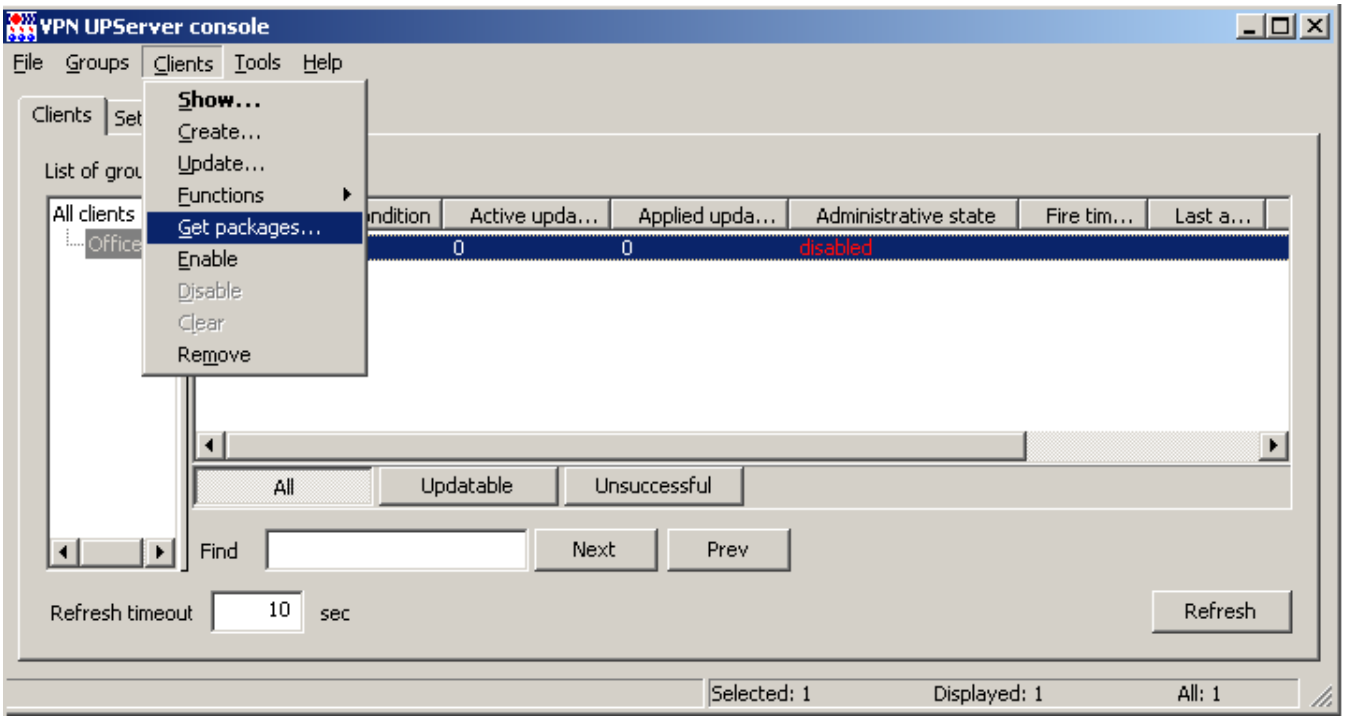

Рисунок 34

Будет выдано окно запроса каталога, в который будут сохранены дистрибутивы, создайте, например, каталог server01 и нажмите OK (Рисунок 35).

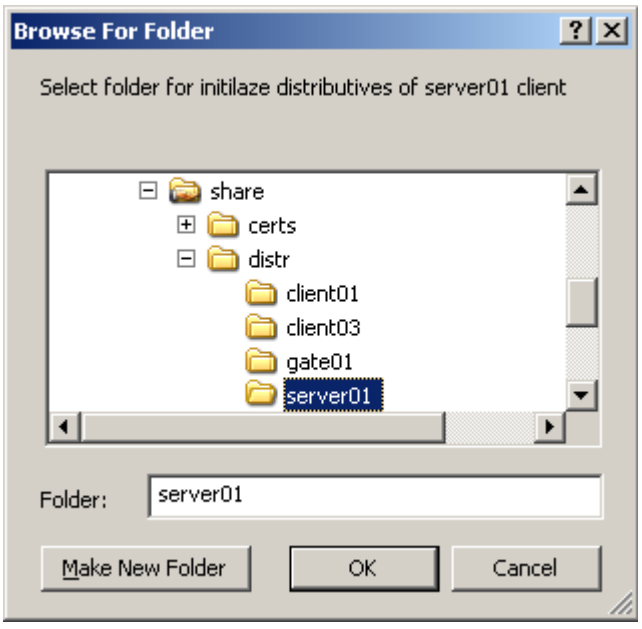

Рисунок 35

После нажатия ОК появится подтверждение успешного сохранения дистрибутивов.

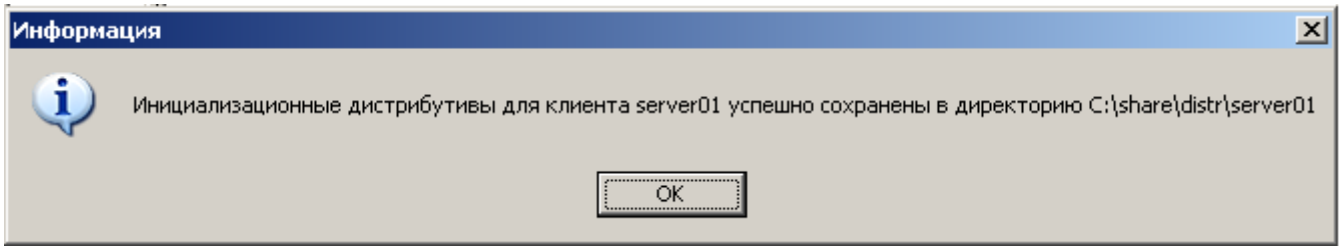

Рисунок 36

Затем перейдите в выбранный каталог (Рисунок 37).

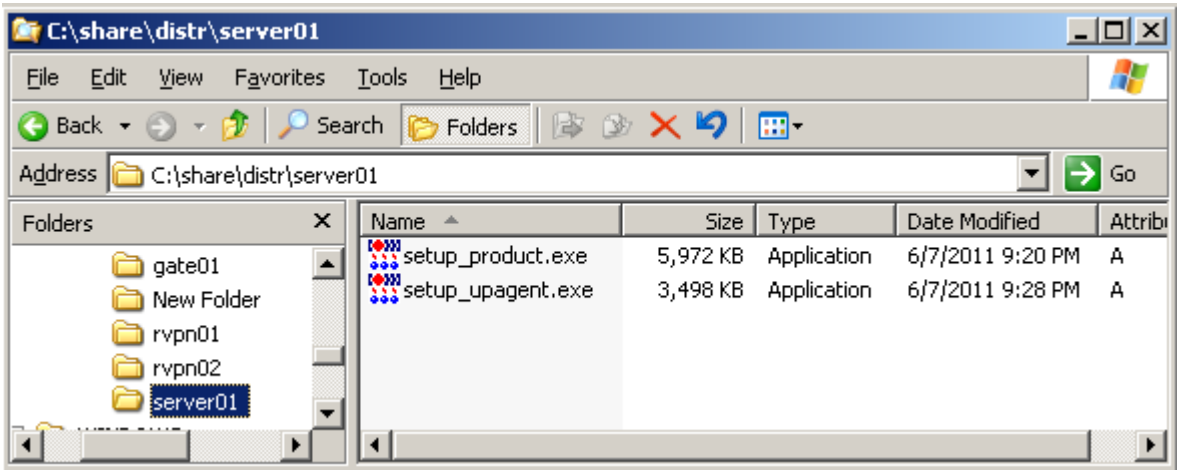

Рисунок 37

В каталоге должны находиться два файла:

- `setup_product.exe` – дистрибутив CSP VPN Server/CSP VPN Client;
- `setup_upagent.exe` – дистрибутив VPN UPAgent (Клиент обновления).

Перед локальной установкой этих дистрибутивов на управляемое vpn-устройство, на Сервере обновления измените административный статус данного клиента (Рисунок 38), выбрав в меню `Clients` предложение `Enable` (или в контекстном меню). Процедура Enable необходима для того, чтобы в момент инсталляции Клиента обновления он смог связаться с Сервером обновления и провести проверку возможности получения обновлений. После изменения статуса клиента на Enable, для него будет сформировано проверочное (тестовое) обновление, и состояние клиента изменится на waiting (Рисунок 38).

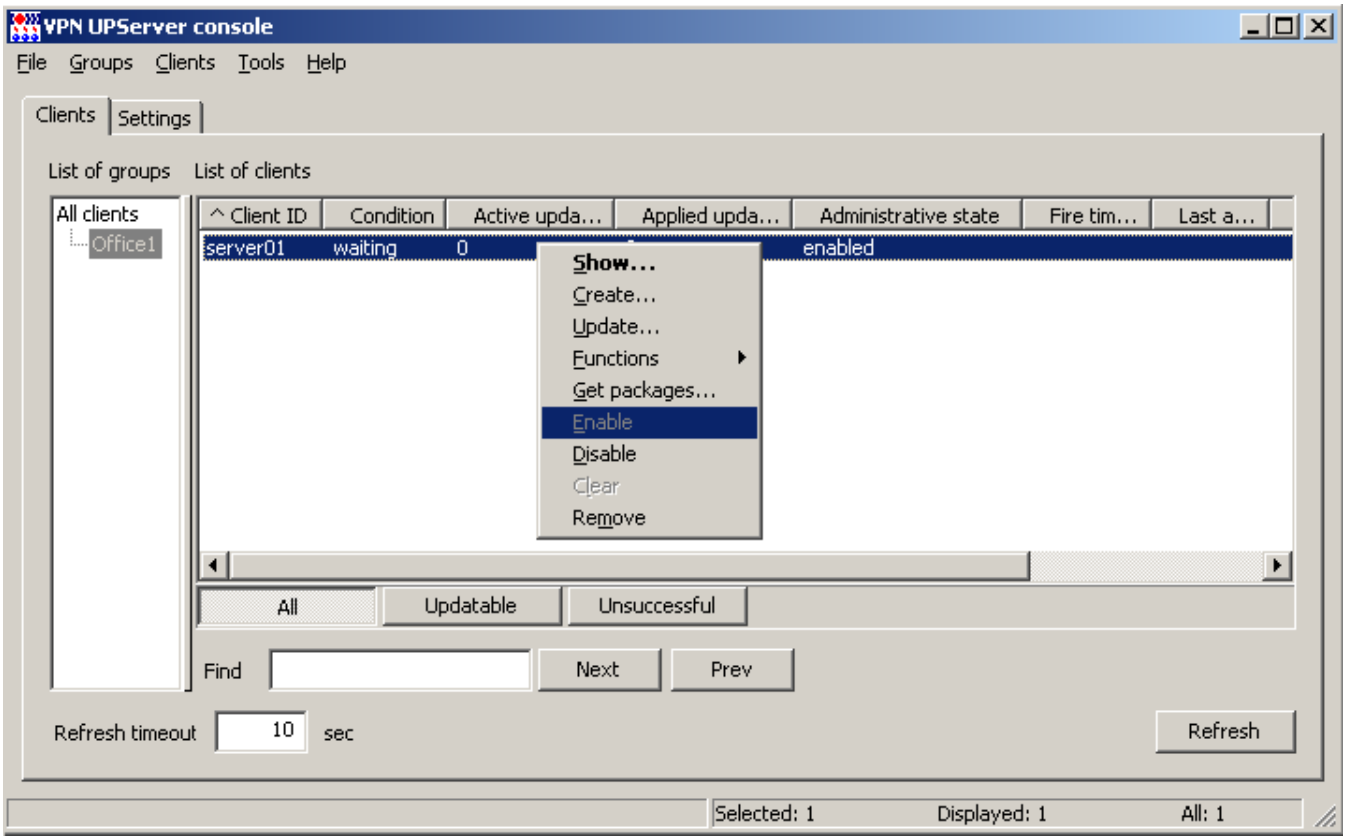

Рисунок 38

После успешного соединения и проверки возможности скачивания обновлений, состояние клиента в таблице клиентов изменится с waiting на updating, а затем на active.

После того, как состояние клиента станет active – Клиент обновления готов к скачиванию обновлений с Сервера обновления.

Инсталляция Клиента обновления и CSP VPN Server/CSP VPN Client

Установка подготовленных дистрибутивов на управляемое vpn-устройство осуществляется локально. Доставьте на клиента два дистрибутива и запустите инсталляцию в следующем порядке:

- сначала `setup_product.exe`
- затем `setup_upagent.exe`.

Если порядок изменить, то Клиент обновления сразу после установки попытается выйти на связь с Сервером обновления не по защищенному соединению.

Процесс установки продукта CSP VPN Server/CSP VPN Client описан в документе («Сервер безопасности CSP VPN Server. Версия 3.1. Руководство администратора»/«Клиент безопасности CSP VPN Client. Версия 3.1. Руководство администратора»), а инсталляция Клиента обновления описана в данном разделе.

Инсталляция Клиента обновления (продукт VPN Upagent) запускается программой `setup_upagent.exe`. В появившемся окне (Рисунок 39) нажмите кнопку Да.

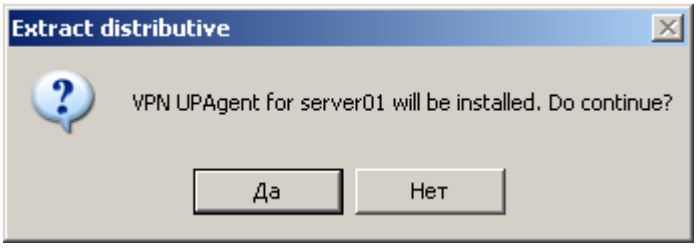

Рисунок 39

Для продолжения инсталляциии нажмите кнопку Next.

Рисунок 40

Выберите каталог для инсталляции Клиента обновления (Рисунок 41).

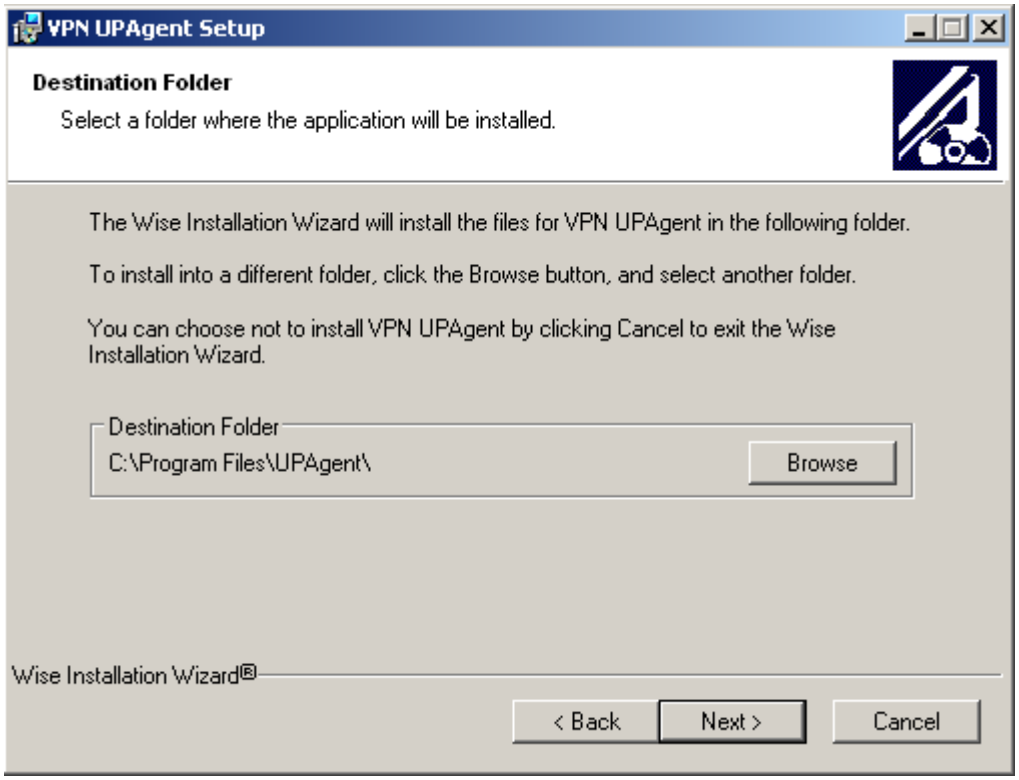

Рисунок 41

В окне подтверждения готовности к установке (Рисунок 42) нажмите кнопку Next.

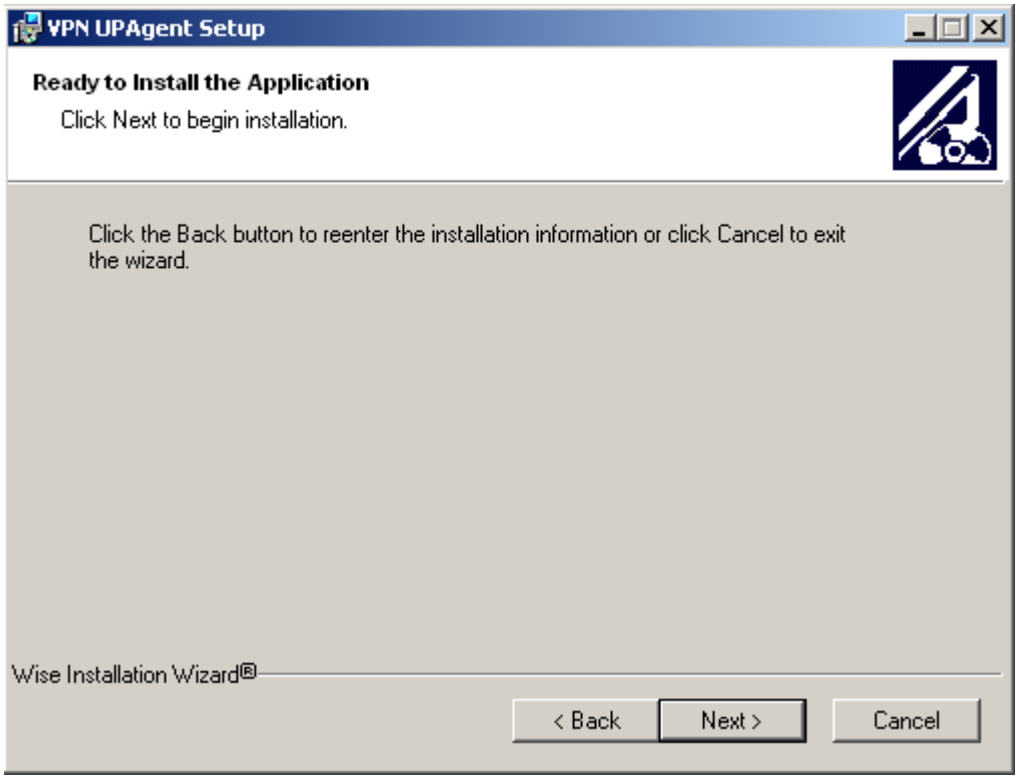

Рисунок 42

Нажмите кнопку Finish (Рисунок 43), инсталляция будет завершена.

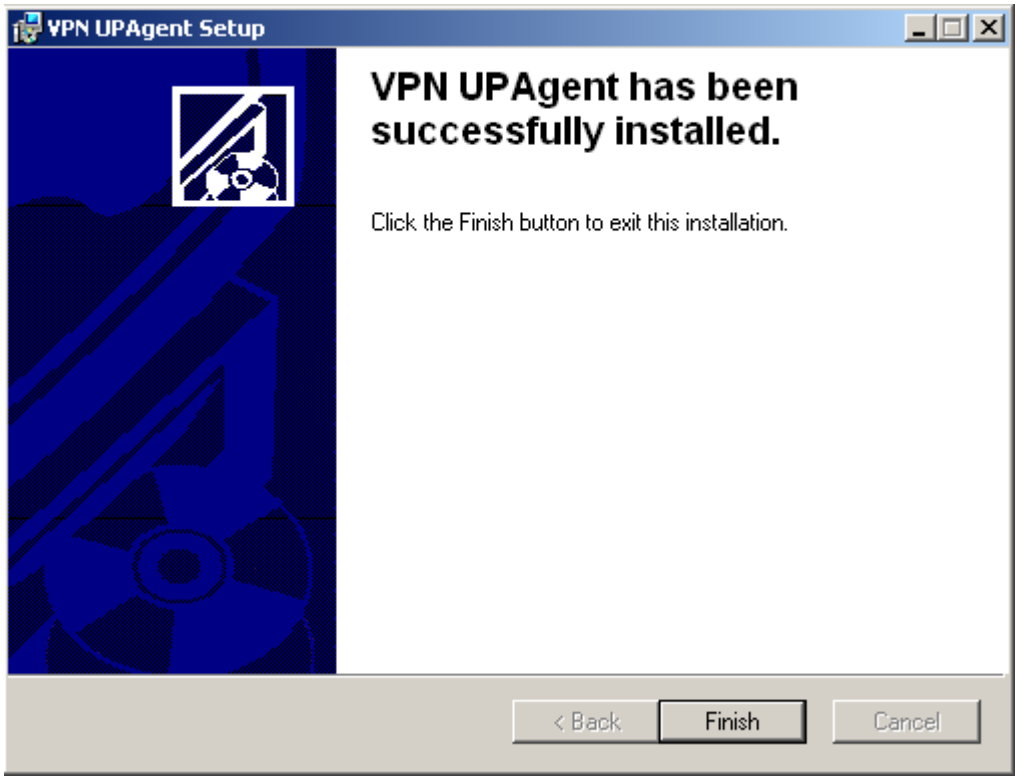

Рисунок 43

По завершению установки Клиент обновления попытается установить связь с Сервером обновления. Этот процесс можно наблюдать в консоли управления продуктом FileZilla Server на компьютере с Сервером обновления.

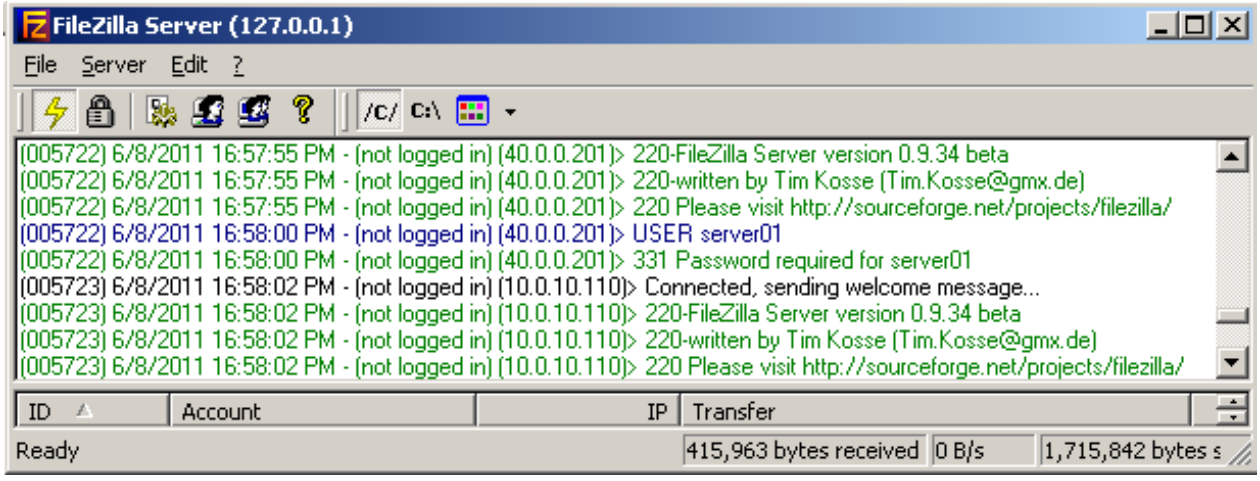

Рисунок 44

После успешного соединения и проверки возможности получения обновлений, состояние клиента в таблице клиентов Сервера обновления изменится с waiting на updating, а затем на active. Это означает, что Клиент обновления готов к скачиванию обновлений.

Создание обновлений. Пример успешного обновления клиента

На Сервере обновления выделите строку с нужным клиентом и в контекстном меню выберите операцию `Update…` для создания обновления.

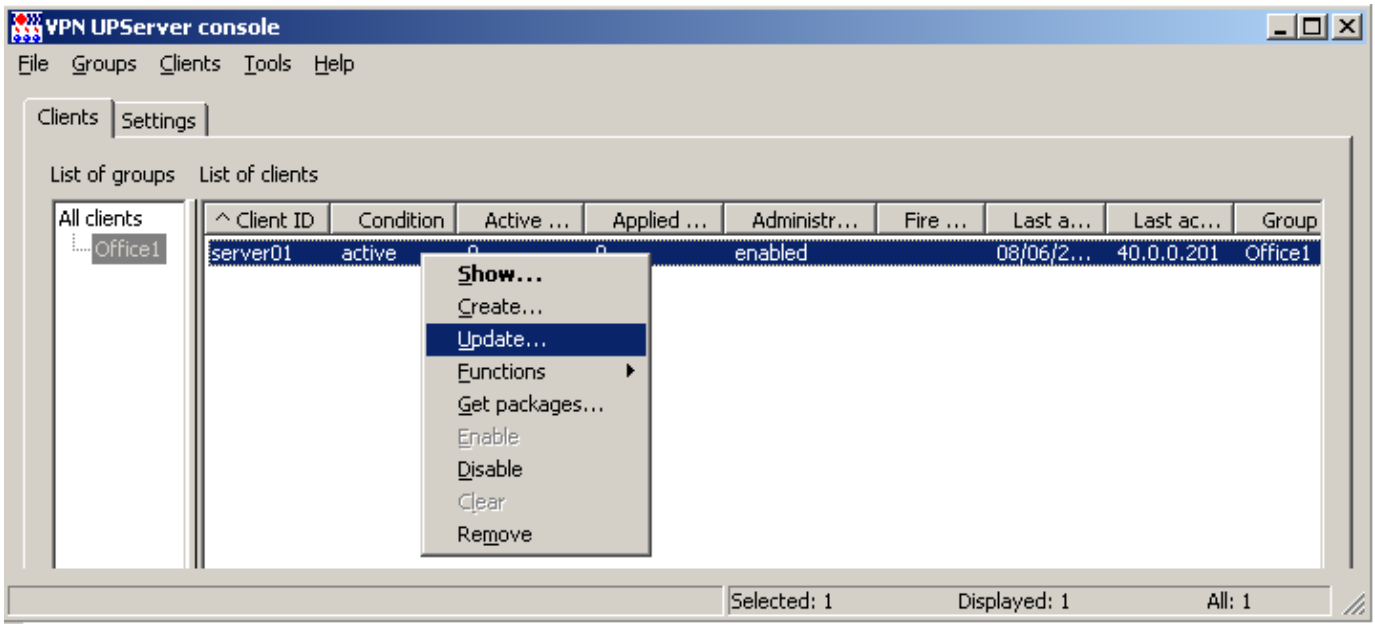

Рисунок 45

После этого будет выдано окно формирования обновления для клиента (Рисунок 46).

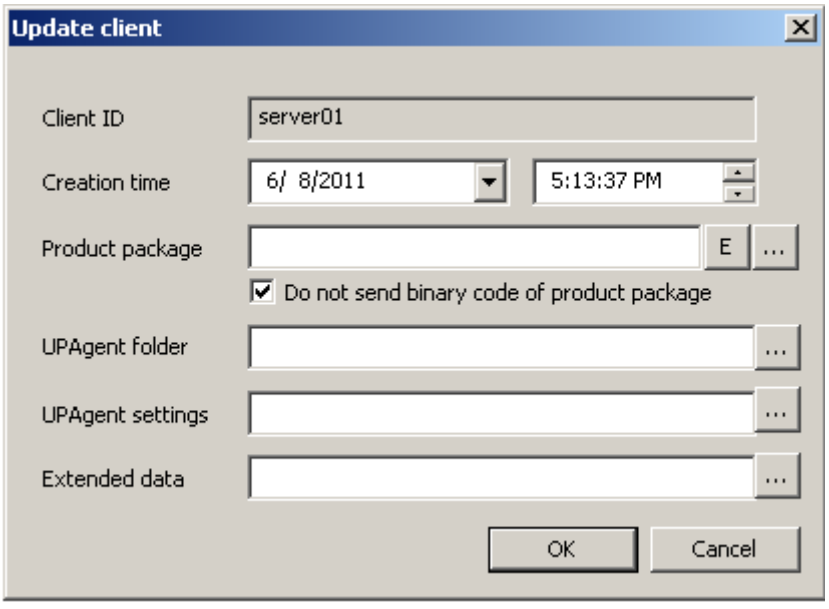

Рисунок 46

В этом окне необходимо заполнить хотя бы одно из полей ***Product package, UPAgent folder, UPAgent settings*** или ***Extended data.*** Значения полей:

Creation time – дата и время, когда Сервер обновления сформирует пакет обновления и сделает его доступным для скачивания Клиентом обновления. Если указанное время уже прошло, то пакет обновления будет сформирован и открыт для скачивания сразу после создания.

Замечание: Клиент обновления скачает созданное для него обновление во время периодических проверок Сервера обновления. Для этого в настройках Клиента обновления задается ***Период проверки новых обновлений на Сервере обновления.*** По умолчанию этот период равен 3600 секунд (см. главу «Настройки Клиента обновления»).

Product package - имя файла дистрибутива CSP VPN Server/CSP VPN Client с внесенными изменениями. Версия продукта не проверятся, а проверяется, что указанный файл является дистрибутивом, созданным с помощью продукта CSP VPN Server AdminTool/CSP VPN Client AdminTool или с помощью окна VPN data maker.

Кнопка E - вызывает окно VPN data maker для создания файла данных продукта CSP VPN Agent. Если поле Product package пустое, то при нажатии на эту кнопку откроется файл данных продукта CSP VPN Agent предыдущего обновления (или если обновлений не было, то файл, указанный при создании клиента). В окне VPN data maker имеется режим использования шаблона проекта для одного или сразу для нескольких клиентов.

Do not send binary code of product package – флаг для указания, что Клиенту обновления будут переданы только конфигурационные данные продукта CSP VPN Agent (без передачи бинарных кодов продукта). Данный флаг позволяет уменьшить размер передаваемых данных.

UPAgent folder – каталог, в котором размещен дистрибутив Клиента обновления (это поле заполняется, если Вы получили новую версию Клиента обновления от разработчика).

UPAgent settings – имя файла, содержащего настройки Клиента обновления (это поле заполняется, если необходимо обновить настройки Клиента обновления. Изменение настроек Клиента обновления описано в разделе «Настройки Клиента обновления»).

Extended data – каталог, в котором размещены расширенные данные и скрипты обновления. Данный каталог может содержать любые данные с любой вложенностью каталогов. В данном каталоге имеются зарезервированные названия файлов:

Файл cook.bat – пакетный файл, который вызывается перед упаковкой каталога для отсылки Клиенту обновления.

Файл может отсутствовать.
Если возвращаемое значение файла отлично от нуля - вся операция подготовки обновления завершается с ошибкой.
Каталогом запуска для файла является каталог, в котором он находится.
Перед вызовом файла `cook.bat` автоматически выставляются следующие переменные окружения:

`UPServerBinDir` – каталог Сервера обновления, в котором располагаются исполняемые файлы

`UPServerDir` – каталог Сервера обновления, в котором располагаются данные продукта

`UPAgentID` – идентификатор Клиента обновления, для которого готовится обновление

`VPNProductType` – тип VPN-продукта, установленного на удаленном компьютере (SERVER,CLIENT,GATE)

`VPNProductVersionMajor` – старшая версия VPN-продукта, установленного на управляемом vpn-устройстве (например, 3.1)

`VPNProductVersionMinor` – младшая версия VPN-продукта, установленного на управляемом vpn-устройстве (например, 10330)

`VPNProductCryptoProvider` – криптопровайдер, используемый VPN-продуктом, который установлен на управляемом vpn-устройстве (CP,SC)

`UPAgentGroup` – идентификатор группы, к которой принадлежит UPAgent

`UPAgentOS` – тип операционной системы, для которой был собран UPAgent (WIN2K,SOLARIS,LINUXRHEL5)

`UPAgentCPU` – тип процессора системы, для которой был собран UPAgent (i386,i486,i686)

`UPAgentLastActiveTime` – время, в которое UPAgent установил соединение с FTP-сервером (dd/mm/yyyy hh:mm:ss)

`UPAgentLastIPAddr` – сетевой адрес, с которого UPAgent установил соединение с FTP-сервером

`VPNProductFireTimeByCert` – ближайшая дата истечения срока действия сертификатов VPN-устройства, на котором установлен UPAgent.

Файл backup.bat – пакетный файл, который вызывается на Клиенте обновления перед запуском процедуры обновления.

Файл может отсутствовать.
Если возвращаемое значение файла отлично от нуля - вся операция обновления завершается с ошибкой.
Каталогом запуска для файла является каталог, в котором он находится.

Файл update.bat – пакетный файл, который вызывается на Клиенте обновления для завершения процедуры обновления.

Файл может отсутствовать.
Если возвращаемое значение файла отлично от нуля - вся операция обновления завершается с ошибкой.
Каталогом запуска для файла является каталог, в котором он находится.

Файл restore.bat – пакетный файл, который вызывается на Клиенте обновления в случае неудачи во время процедуры обновления или при завершении с ошибкой выполнения пакетного фала update.bat.

Файл может отсутствовать.
Строго не рекомендуется возвращать значение, отличное от нуля, так как Клиент обновления будет периодически вызывать этот скрипт, пока он не завершится успехом.
Каталогом запуска для файла является каталог, в котором он находится.

Перед вызовом файлов ***backup.bat, update.bat, restore.bat*** автоматически выставляются следующие переменные окружения:

`UPAgentBinDir` – каталог Клиента обновления, в котором располагаются исполняемые файлы

`UPAgentDir` – каталог Клиента обновления, в котором можно сохранять данные

`VPNProductBinDir` – каталог продукта CSP VPN Agent, в котором располагаются исполняемые файлы

`UPAgentID` – идентификатор Клиента обновления

`UPServerAddr` – рабочий адрес Сервера обновления

`VPNProductType` – тип VPN-продукта, установленного на управляемом vpn-устройстве (SERVER,CLIENT,GATE)

`VPNProductVersionMajor` – старшая версия VPN-продукта, установленного на управляемом vpn-устройстве (например, 3.1)

`VPNProductVersionMinor` – младшая версия VPN-продукта, установленного на управляемом vpn-устройстве (например, 10330)

`VPNProductCryptoProvider` – криптопровайдер, используемый VPN-продуктом, который установлен на управляемом vpn-устройстве (CP,SC)

`UPAgentVersionMajor` – старшая версия UPAgent, установленного на управляемом vpn-устройстве (например, 1.2)

`UPAgentVersionMinor` – младшая версия UPAgent, установленного на управляемом vpn-устройстве (например, 11687).

Для проверки механизма обновления нажмите кнопку E в окне Update client (Рисунок 46) и в открывшемся окне VPN data maker во вкладке LSP внесите изменения – в атрибуте Title измените «Test LSP» на «Test UPDATE LSP» (Рисунок 47) и нажмите кнопку OK.

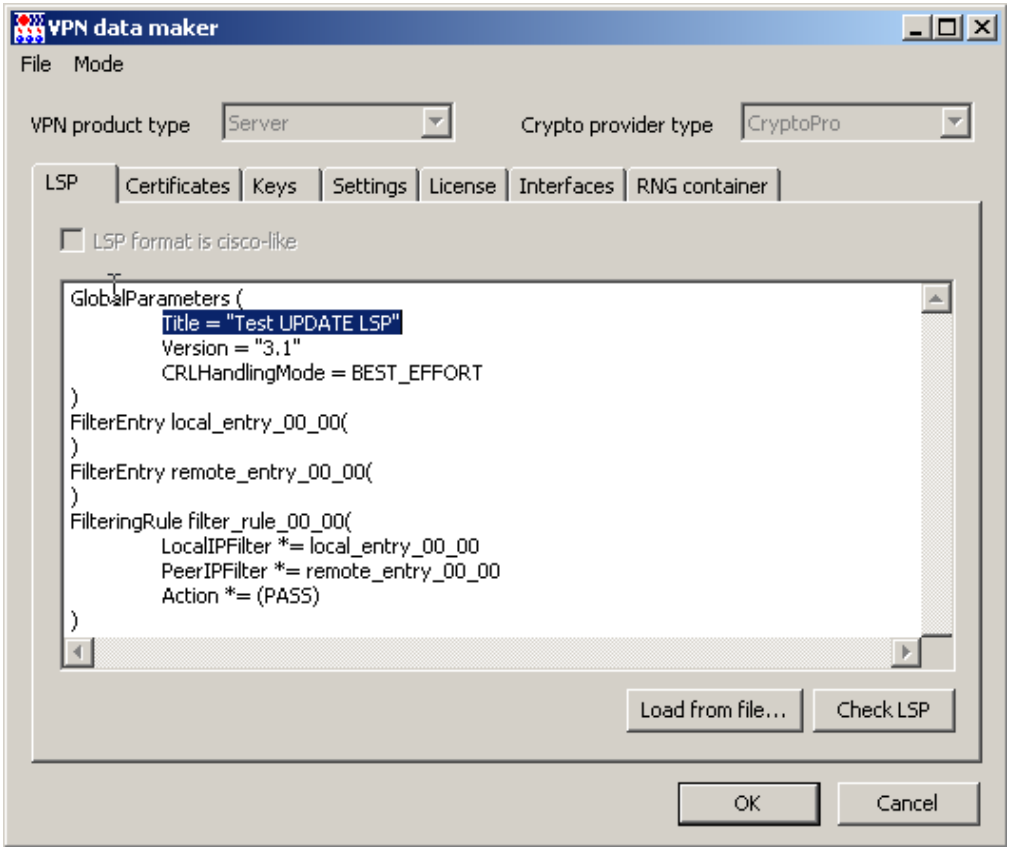

Рисунок 47

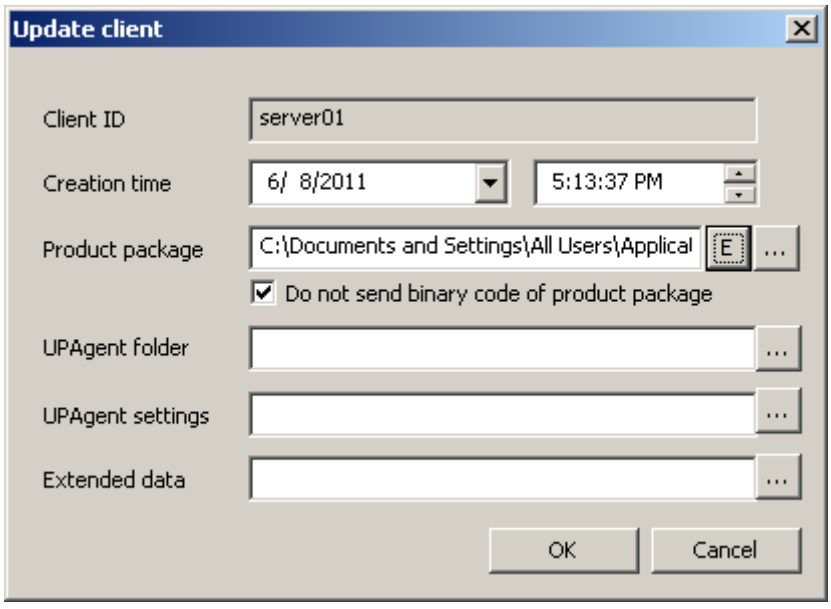

Рисунок 48

Нажатие кнопки OK (Рисунок 47) приводит к созданию файла данных продукта CSP VPN Server и возвращению к окну обновления клиента (Рисунок 48) с заполненным полем Product package. Нажмите кнопку OK, запустится механизм создания обновления.

После нажатия кнопки OK в окне создания обновления будет создано обновление и в таблице клиентов для данного клиента количество активных обновлений (столбец Active updates) увеличится на единицу. Если повторно выполнить операцию создания обновления, то добавится еще одно обновление, и оно станет в очередь обновлений. Отметим, что порядок применения обновлений соответствует порядку их создания, даже если Creation time первого обновления является более поздним, чем Creation time последующих обновлений.

В момент времени, указанный в поле Creation time, произойдет формирование пакета обновления и предоставление его для скачивания Клиентом обновления, а состояние обновления изменится с `active` на `waiting`.

После того, как Клиент обновления выйдет на связь и скачает обновление, состояние клиента в таблице изменится с `waiting` на `updating` (Рисунок 49).

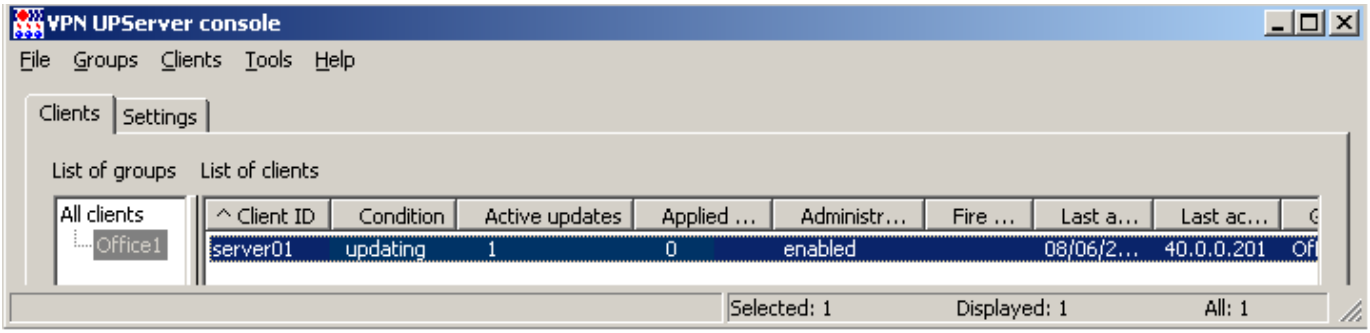

Рисунок 49

После успешного завершения обновления, состояние клиента в таблице клиентов изменится с `updating` на `active`, количество готовых активных обновлений уменьшится на единицу, а количество успешных примененных обновлений увеличится на единицу. В этом состоянии клиент готов для последующих обновлений (Рисунок 50).

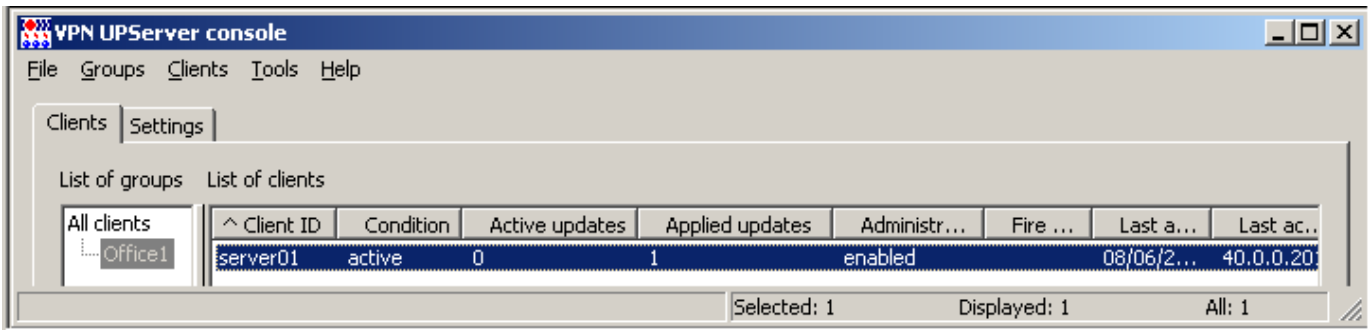

Рисунок 50

Посмотреть параметры выполненного обновления на клиенте можно, используя пункт меню Show (см. раздел «Информация о клиенте на Сервере обновления»).

Пример неуспешного обновления клиента см. в разделе «Пример неудачного обновления клиента».

Информация о клиенте на Сервере обновления

Посмотреть параметры VPN-продукта на управляемом vpn-устройстве после проведенного обновления можно на Сервере обновления с помощью предложения Show меню Clients (или контекстного меню).

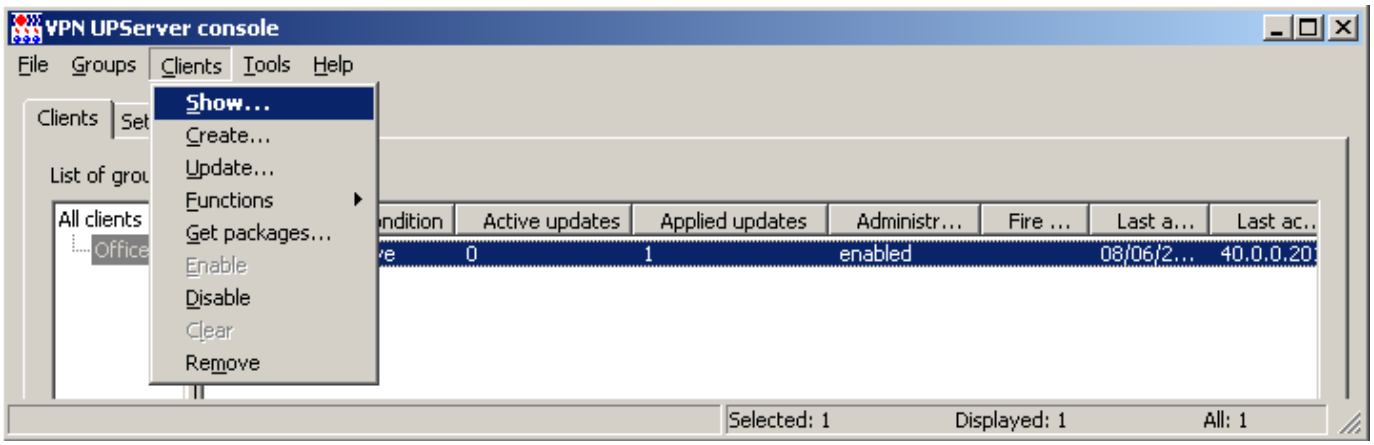

Рисунок 51

В результате будет выдано окно с разными вкладками (Рисунок 52), в которых отражена информация о проведенных обновлениях, настройках Клиента обновления, действующей в данный момент политике безопасности на клиенте, используемых предопределенных ключах или сертификатах, об интерфейсах клиента и т.п.

Во вкладке UPLog ведется лог событий по обновлению клиента.

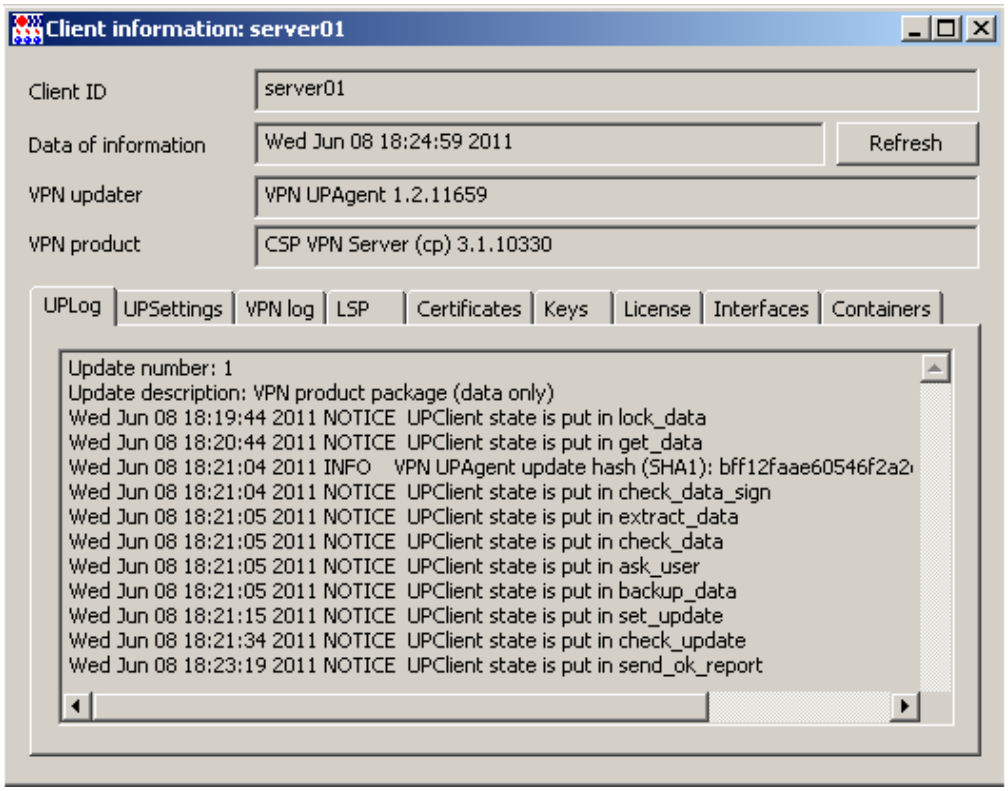

Рисунок 52

Во вкладке UPSettings (Рисунок 53) отражены настройки Клиента обновления. Описание этих настроек дано в главе «Настройки Клиента обновления».

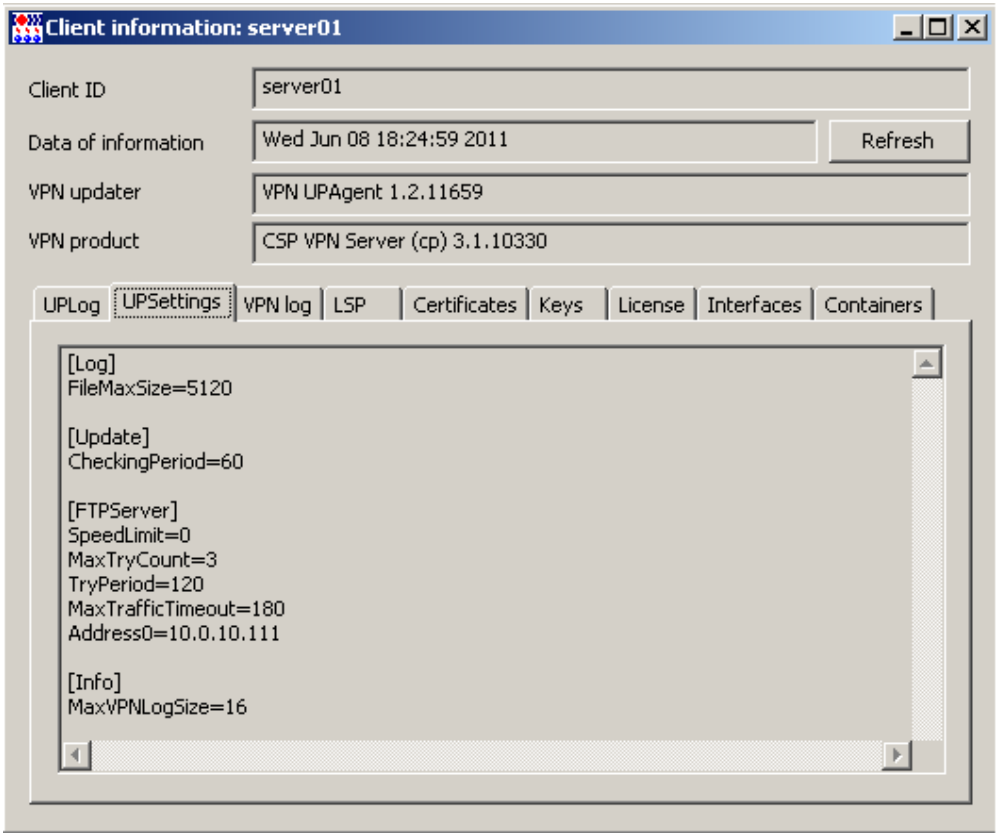

Рисунок 53

Во вкладке VPN log отражается протоколирование событий, связанных с работой VPN-продукта CSP VPN Agent.

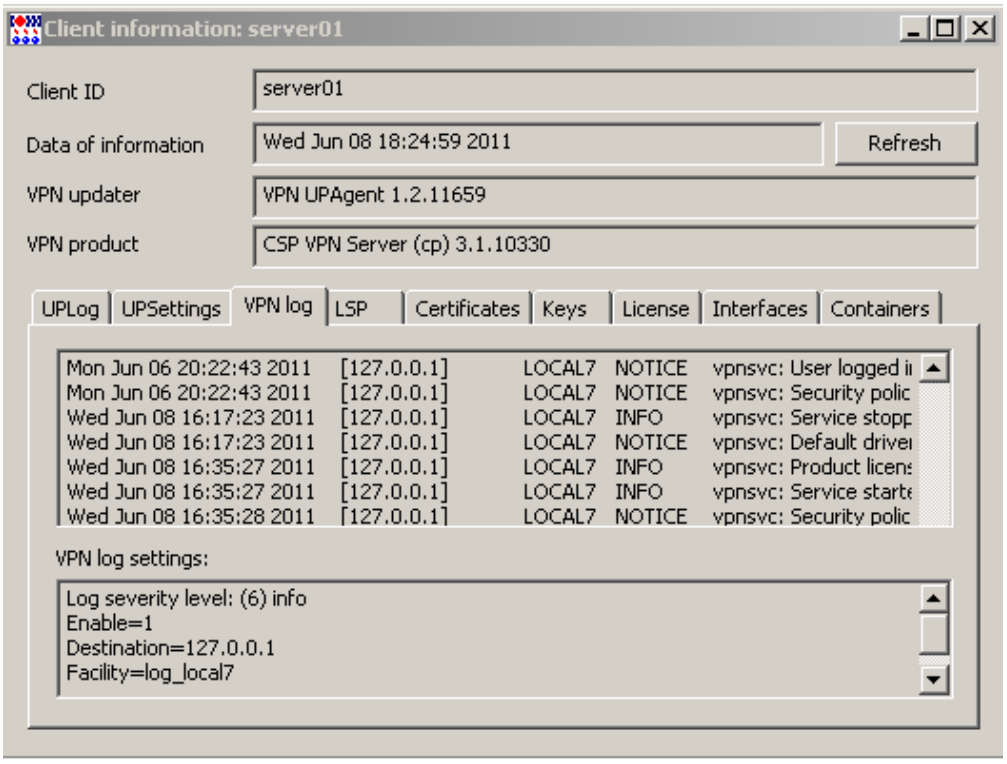

Рисунок 54

Вкладка LSP показывает загруженную политику безопасности на клиенте (Рисунок 55).

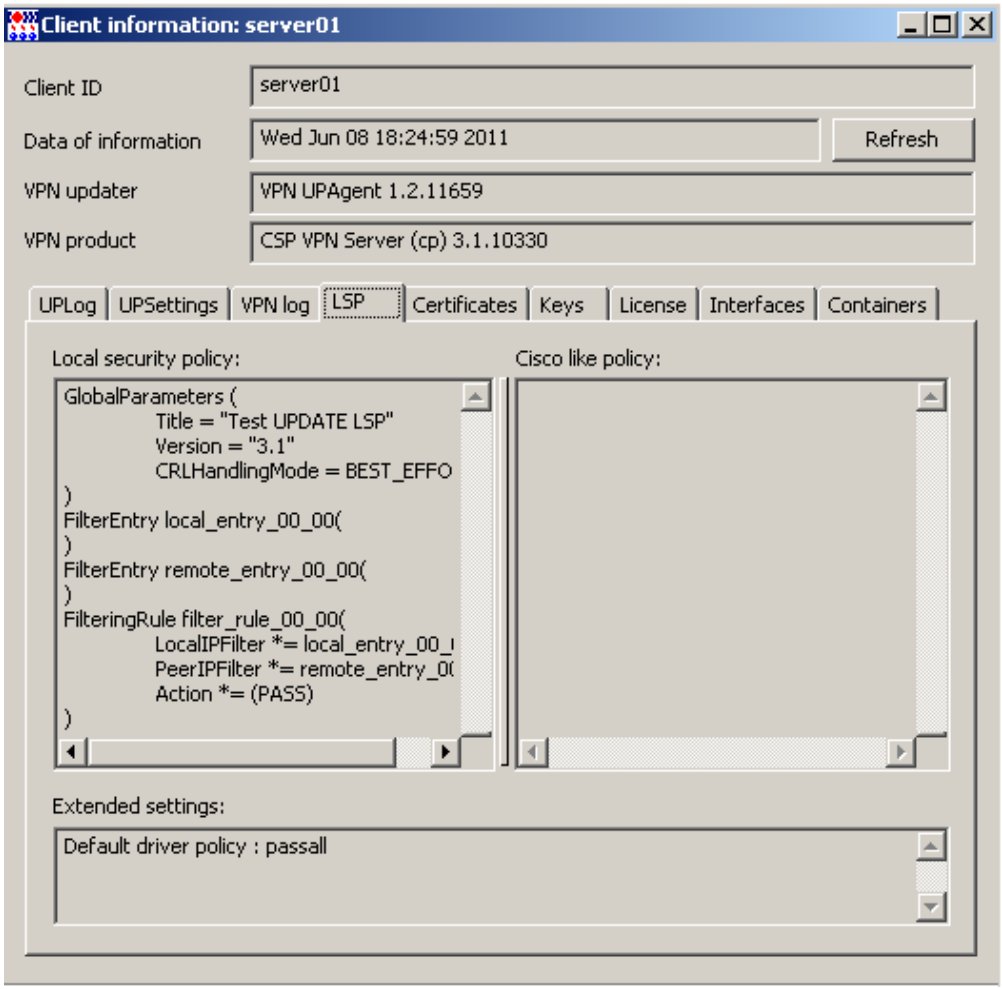

Рисунок 55

Вкладка Keys показывает только имена предопределенных ключей, используемых при работе с партнерами, не показывая их значений.

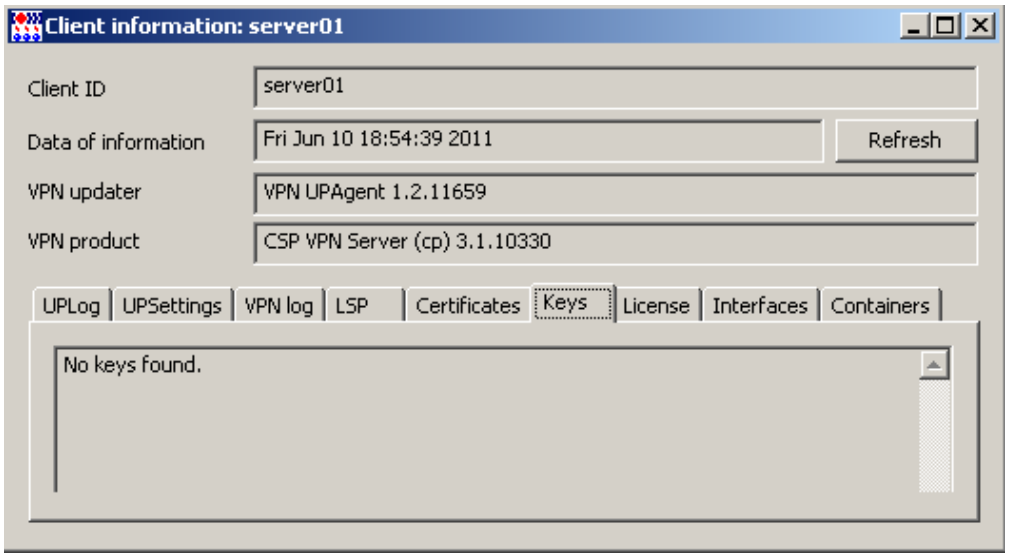

Рисунок 56

Вкладка License показывает данные лицензии на продукт CSP VPN Agent.

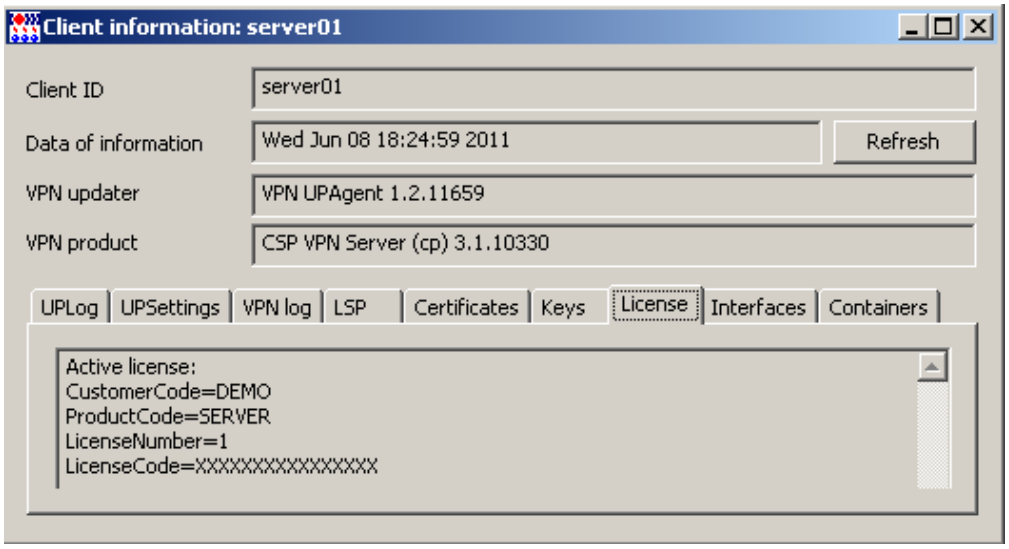

Рисунок 57

Вкладка Interfaces содержит информацию обо всех сетевых интерфейсах управляемого vpn-устройства.

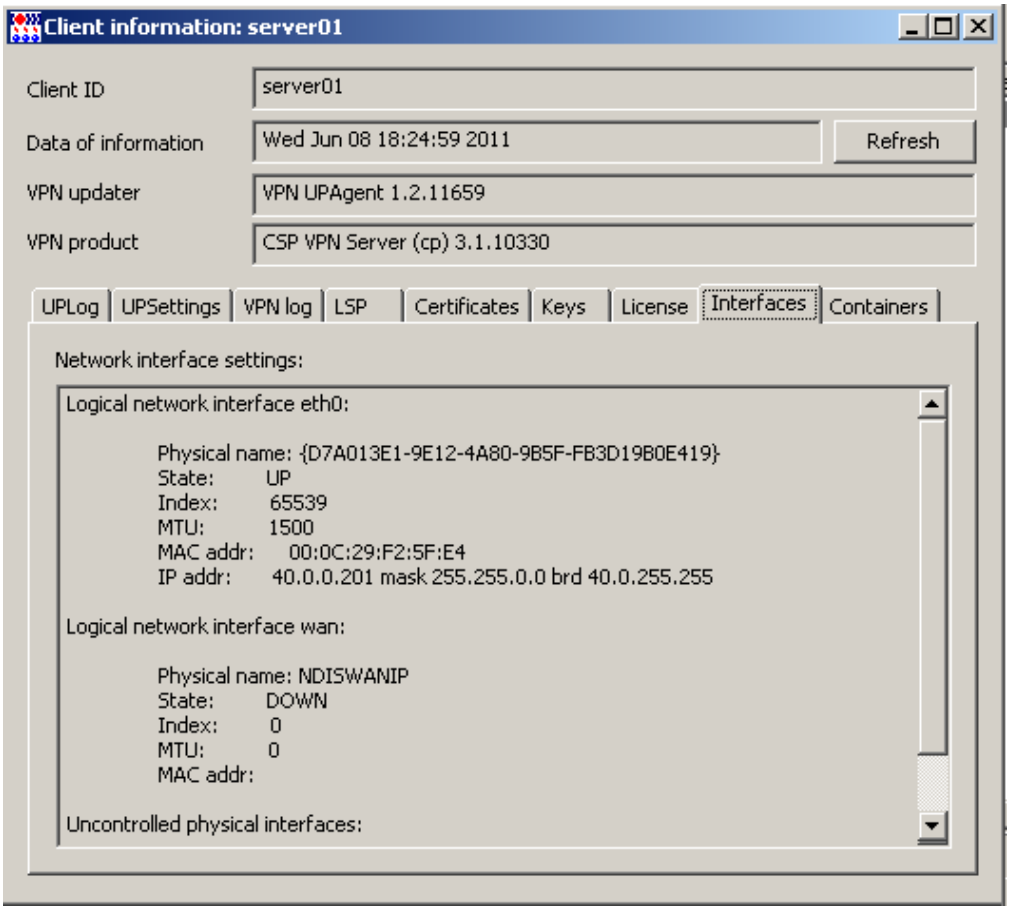

Рисунок 58

Вкладка Containers показывает созданные на управляемом vpn-устройстве запросы на сертификаты, используемые и неиспользуемые контейнеры с ключевыми парами.

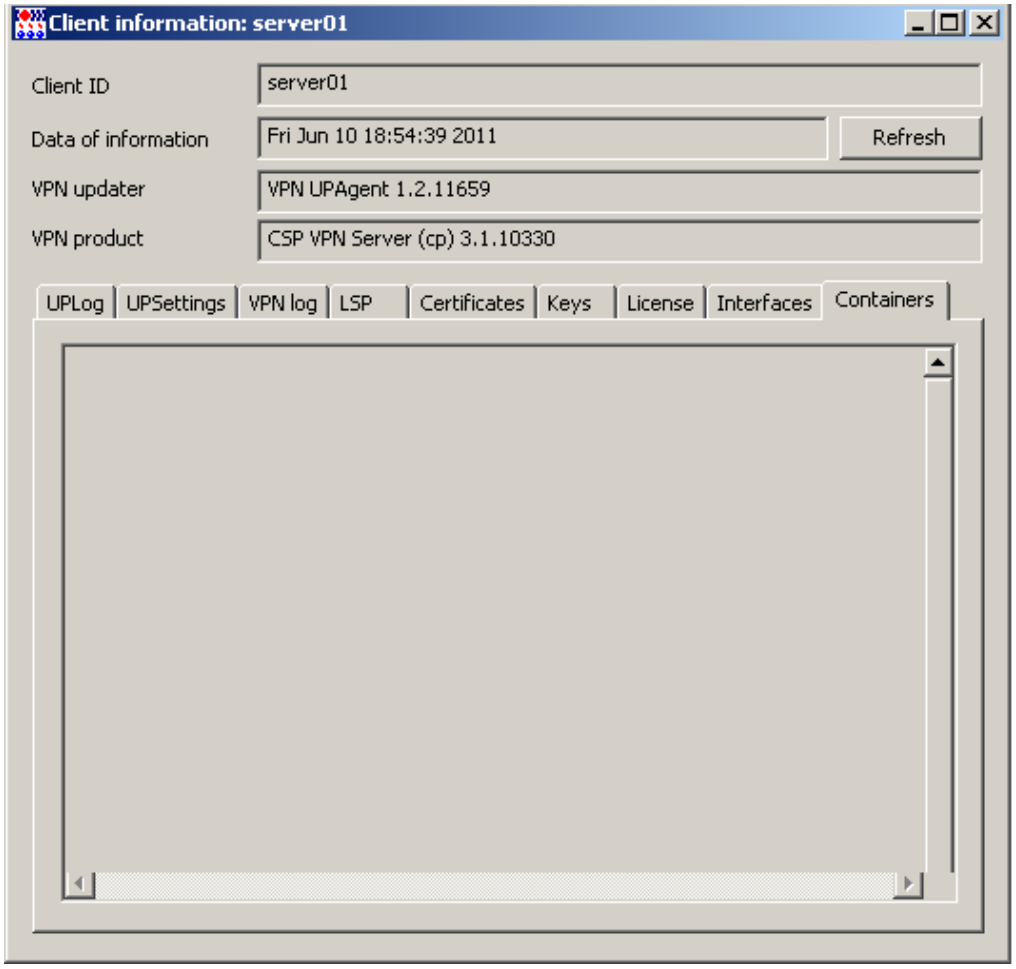

Рисунок 59

Пример неудачного обновления клиента

Для проверки неудачного обновления клиента укажите неверный адрес Сервера обновления в настройках Клиента обновления. Во вкладе Settings измените, например, адрес 10.0.10.111 на адрес 10.0.10.112 и нажмите кнопку Save (Рисунок 60).

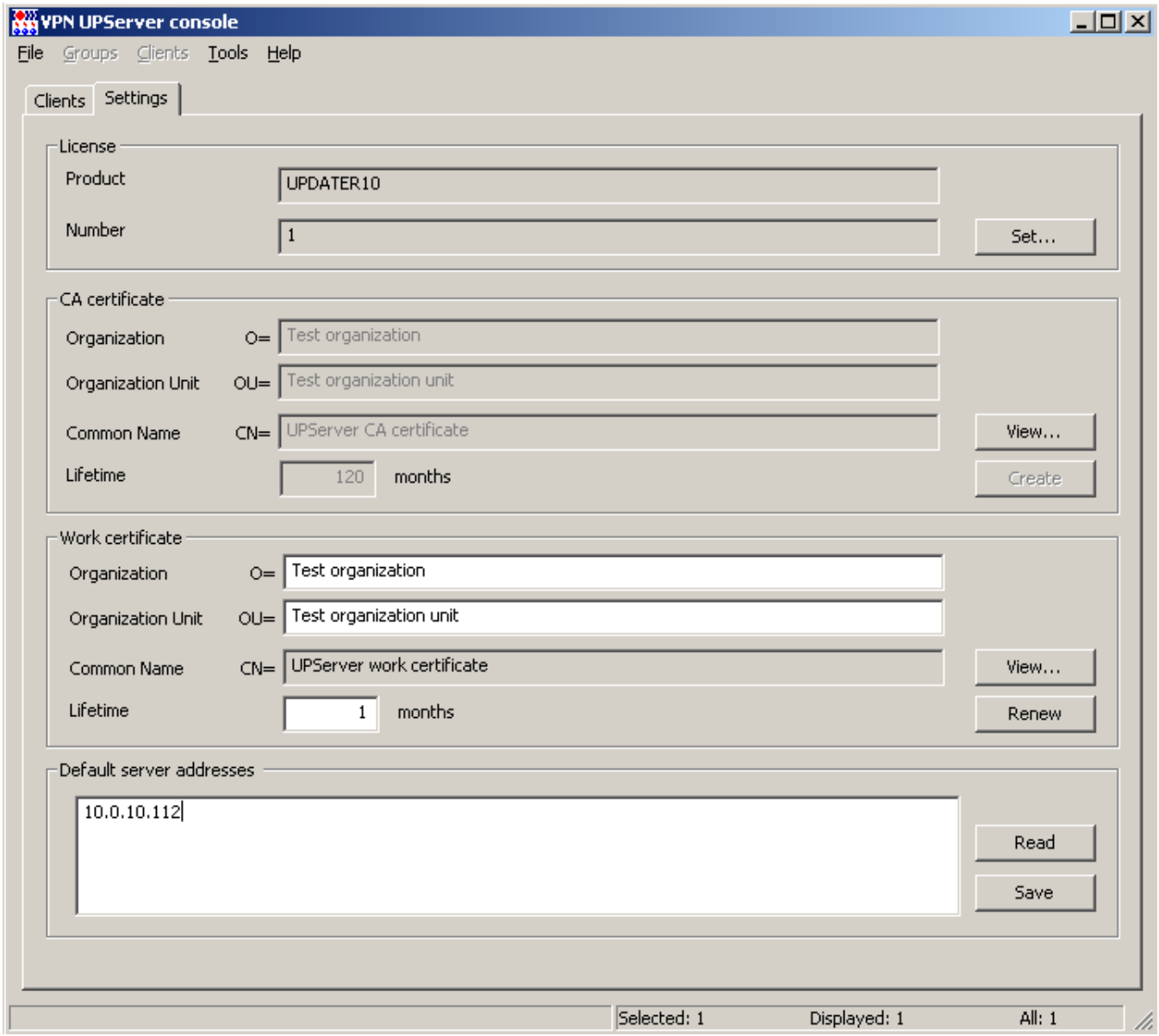

Рисунок 60

В окне Предупреждение нажмите кнопку ОК (Рисунок 61).

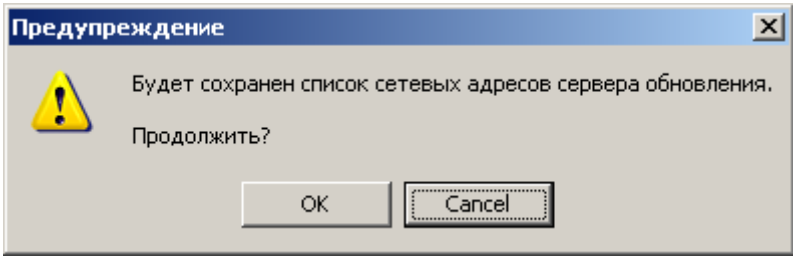

Рисунок 61

Создайте новое обновление для существующего клиента. Перейдите на вкладку Clients и выберите операцию `Update…`

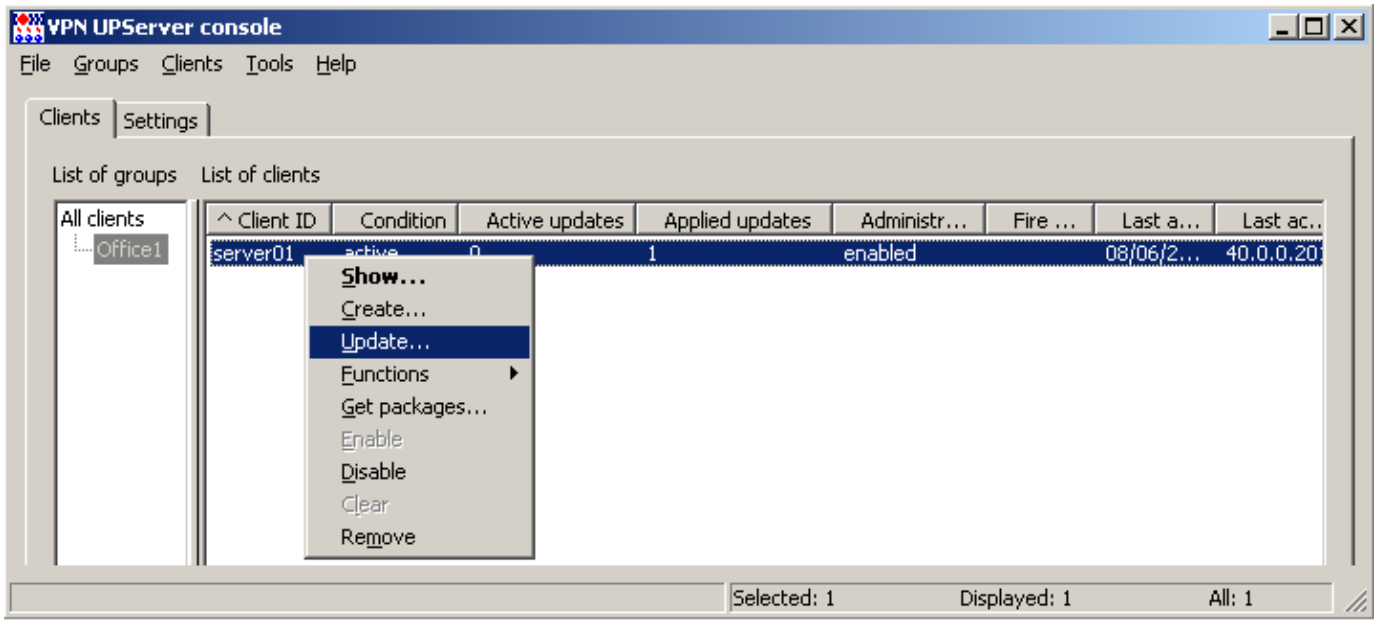

Рисунок 62

В открывшемся окне создания обновления (Рисунок 63) задайте файл настроек Клиента обновления, в котором уже записан неверный адрес Сервера обновления. Расположение файла зависит от операционной системы: `"C:\ProgramData\UPServer\csettings.txt"` *или* `"C:\Documents and Settings\All Users\Application Data\UPServer\csettings.txt"`.

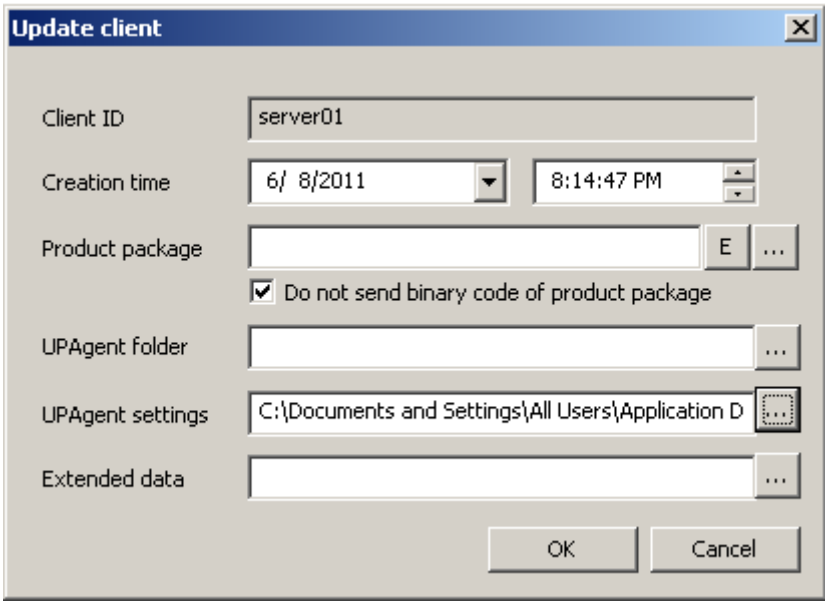

Рисунок 63

После нажатия кнопки OK количество активных обновлений увеличится на единицу, и через некоторое время состояние изменится с `active` на `waiting`.

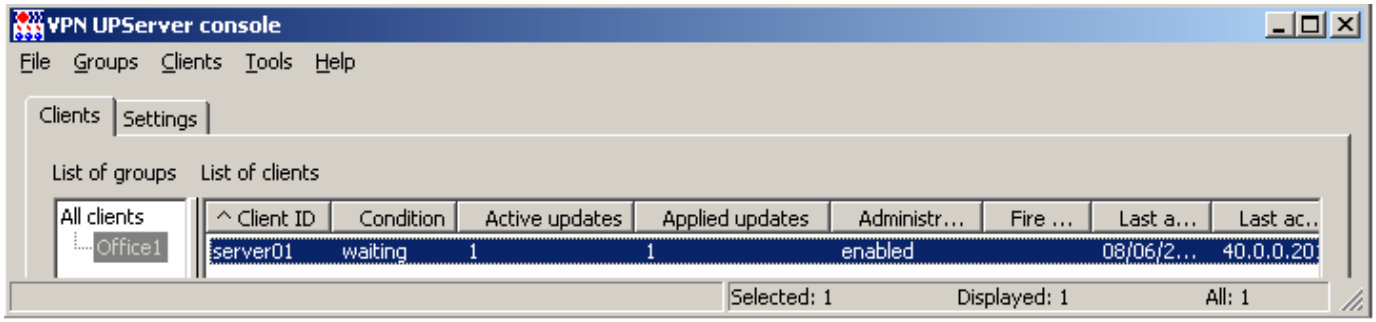

Рисунок 64

Поле того, как Клиент обновления обнаружит обновление, состояние изменится с `waiting` на `updating`.

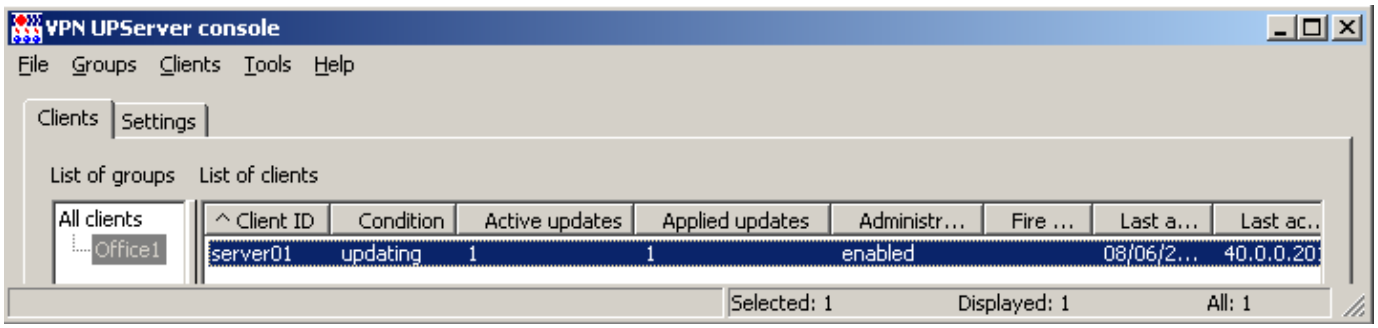

Рисунок 65

По истечении некоторого времени (если настройки по умолчанию не менялись, то примерно через 6 минут) состояние изменится с `updating` на `failed` (Рисунок 66).

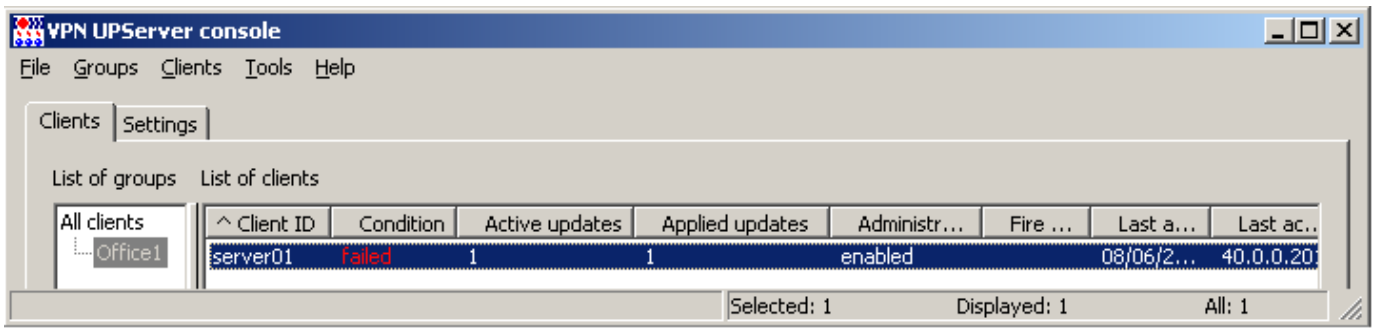

Рисунок 66

Состояние failed означает, что Клиент обновления отверг обновление и вернулся к старой конфигурации. Причины неприятия обновления можно посмотреть, открыв окно информации о клиенте (Show в контекстном меню – (Рисунок 67)), и во вкладке UPLog - лог операции обновления (Рисунок 68).

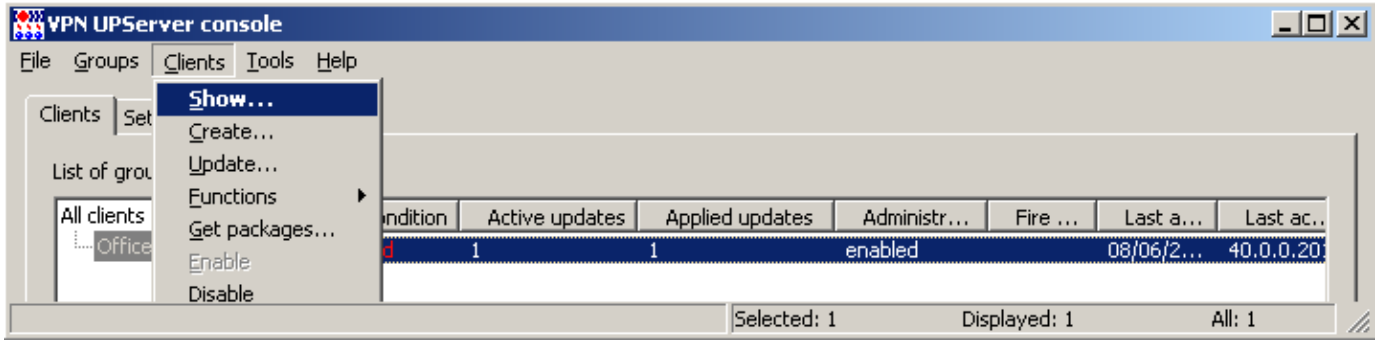

Рисунок 67

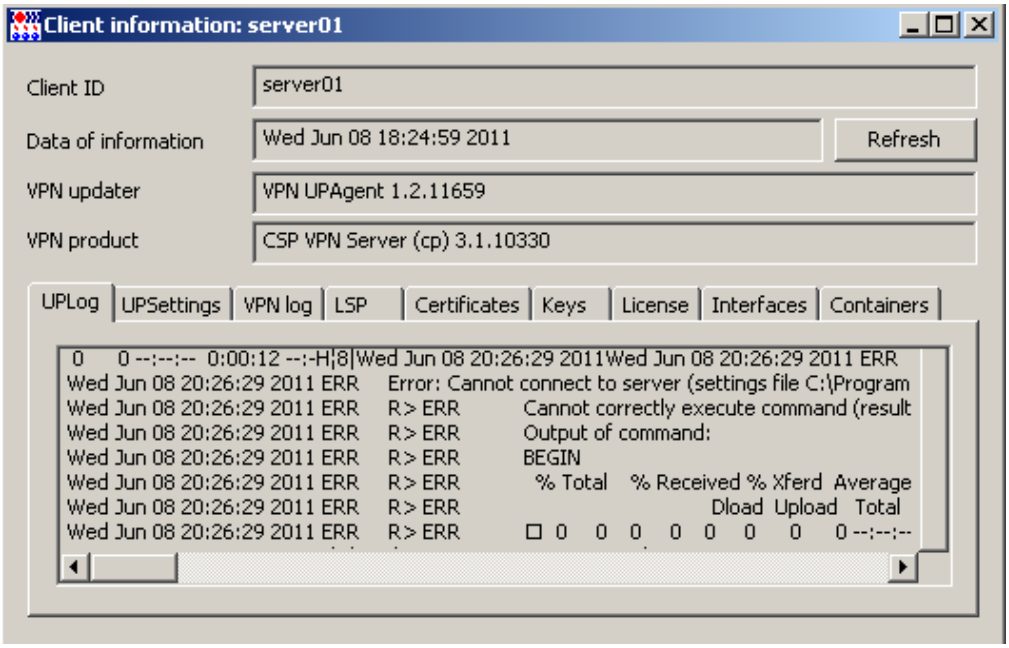

Рисунок 68

Для отмены неудачного обновления для данного клиента в меню Clients выберите предложение `Clear` (Рисунок 69).

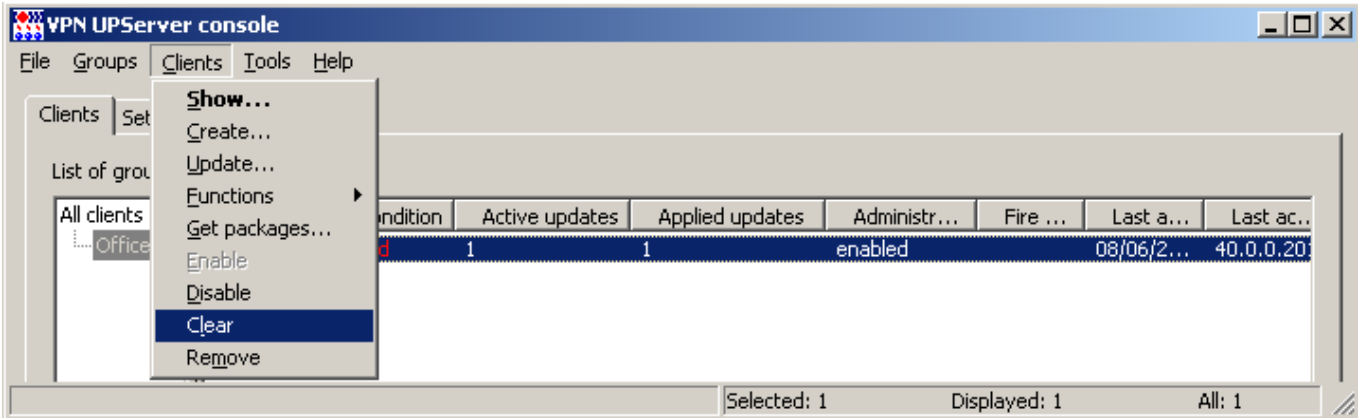

Рисунок 69

Выдается предупреждение с просьбой подтвердить удаление всех не примененных обновлений. Нажмите кнопку ОК (Рисунок 70).

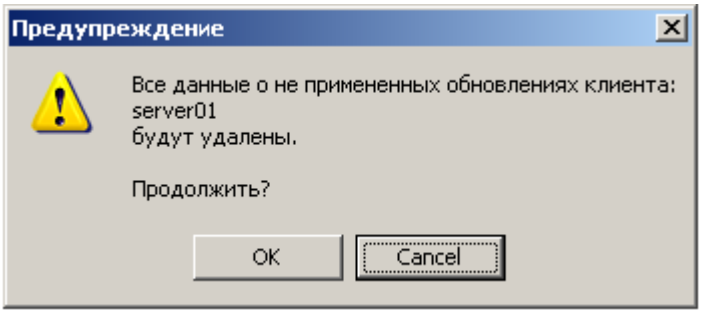

Рисунок 70

После этого количество активных обновлений станет равным нулю и через некоторое время состояние изменится с `failed` на `active` (Рисунок 71).

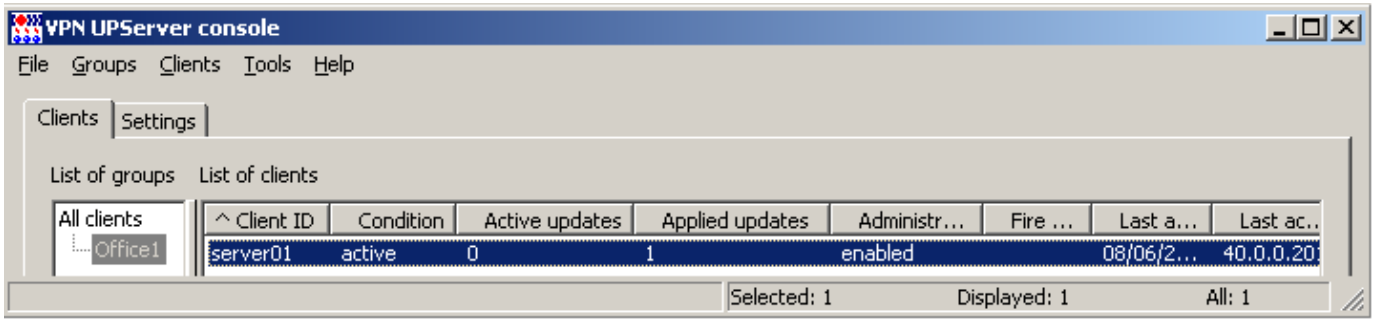

Рисунок 71

В этом состоянии клиент готов для последующих обновлений.

Не забудьте изменить адрес Сервера обновления во вкладке Settings на правильное значение.

Обновление CSP VPN Gate

Создание клиента на Сервере обновления

Создание учетной записи клиента для управляемого vpn-устройства с CSP VPN Gate осуществляется также как и для CSP VPN Server/CSP VPN Client, за некоторыми исключениями.

Создайте клиента для CSP VPN Gate на Сервере обновления, например, в той же группе Office1. Выделите группу, в меню Clients выберите предложение Create (Рисунок 72).

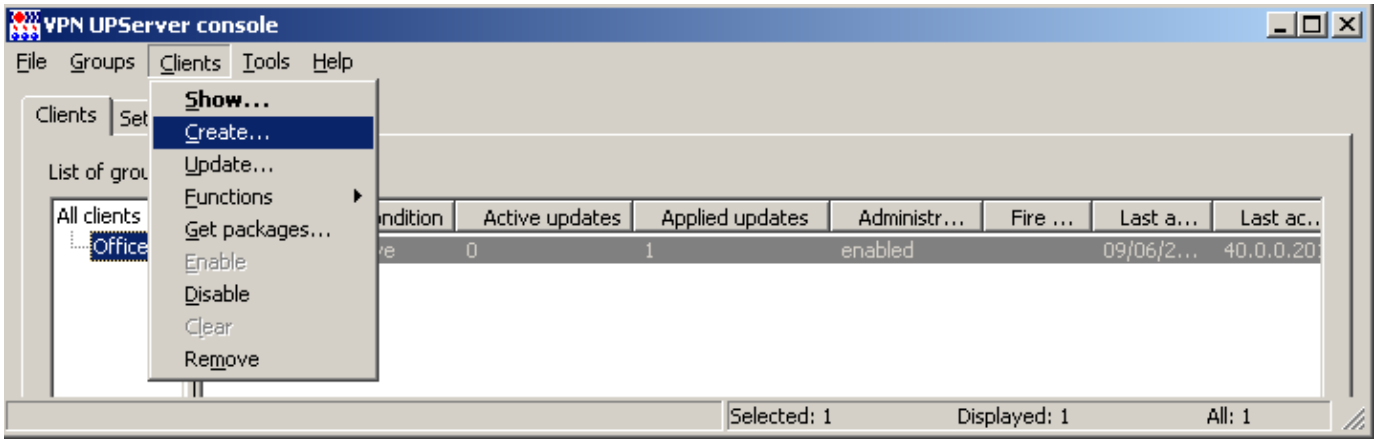

Рисунок 72

В окне создания клиента введите уникальный идентификатор клиента, например, gate01, и нажмите кнопку E (Рисунок 73).

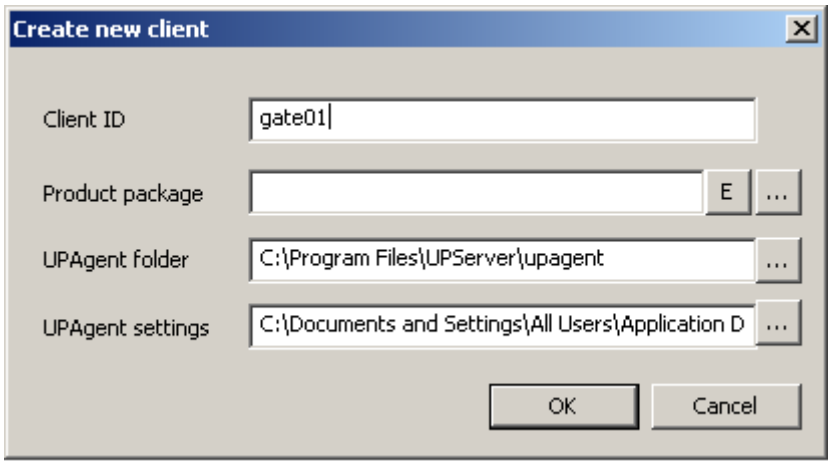

Рисунок 73

В открывшемся окне VPN data maker во вкладке LSP (Рисунок 74) установите флажок LSP format is cisco-like и скопируйте во вкладку, например, следующую политику безопасности (политику можно ввести и не в формате cisco-like команд):

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit clear
crypto isakmp identity address
```

```
username cscons privilege 15 password 0 csp
hostname cspgate
enable password csp
!
interface FastEthernet0/0
 ip address 40.0.0.1 255.255.0.0
!
interface FastEthernet0/1
 ip address 10.0.10.110 255.255.0.0
!
interface FastEthernet0/2
 no ip address
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
!
End
```

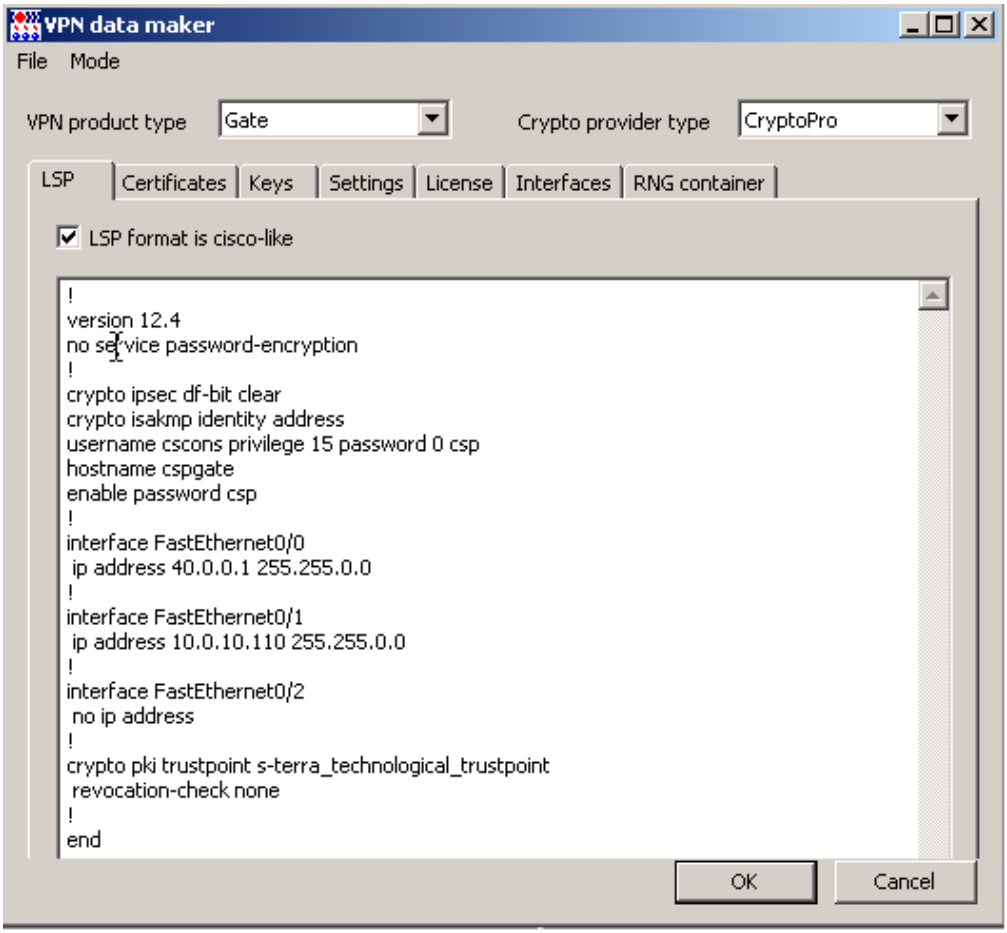

Рисунок 74

Во вкладке License введите данные лицензии на продукт CSP VPN Gate, для которого создается клиент на Сервере обновления (Рисунок 75).

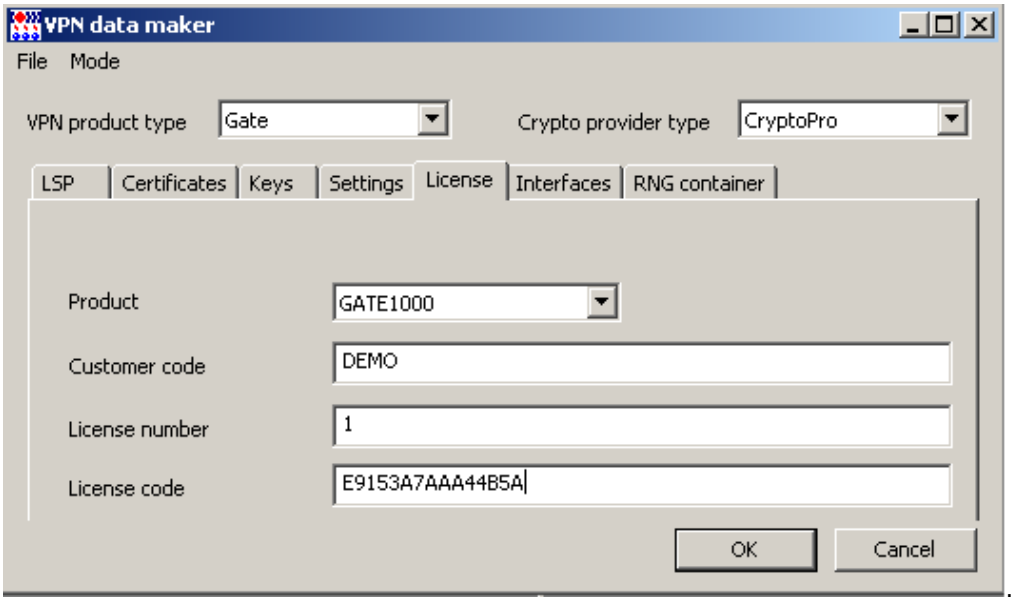

Рисунок 75

Остальные вкладки можно оставить без изменений и нажать кнопку OK.

В окне создания нового клиента gate01 также нажмите кнопку OK (Рисунок 76).

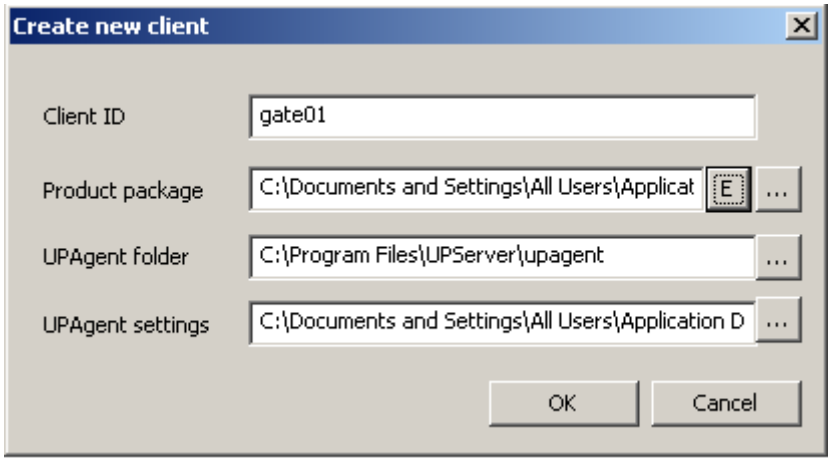

Рисунок 76

Измените статус созданного клиента, выполнив операцию Enable (Рисунок 77).

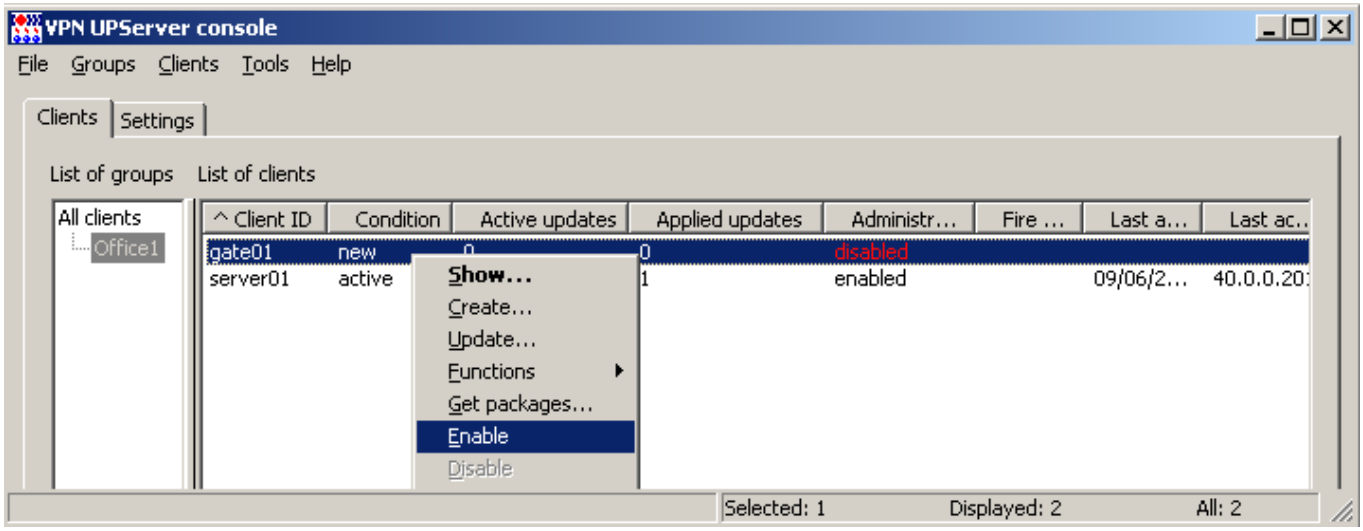

Рисунок 77

Создание дистрибутивов Клиента обновления и CSP VPN Gate

Для создания дистрибутивов Клиента обновления и CSP VPN Gate для клиента gate01 выберите операцию Get packages (Рисунок 78) .

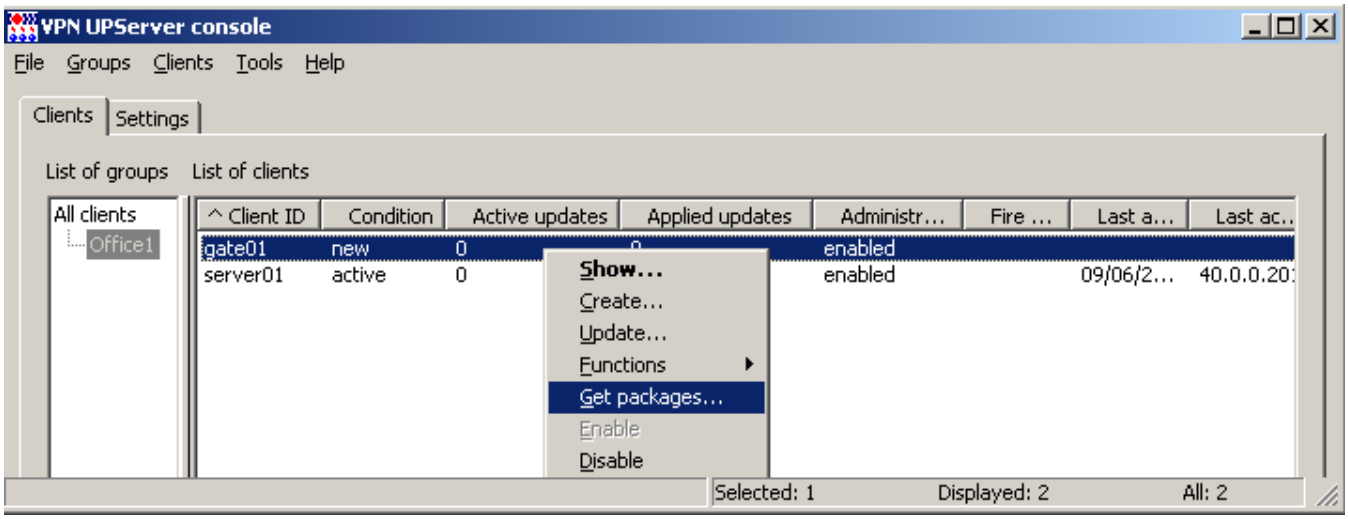

Рисунок 78

В открывшемся окне укажите каталог для сохранения дистрибутивов (Рисунок 84).

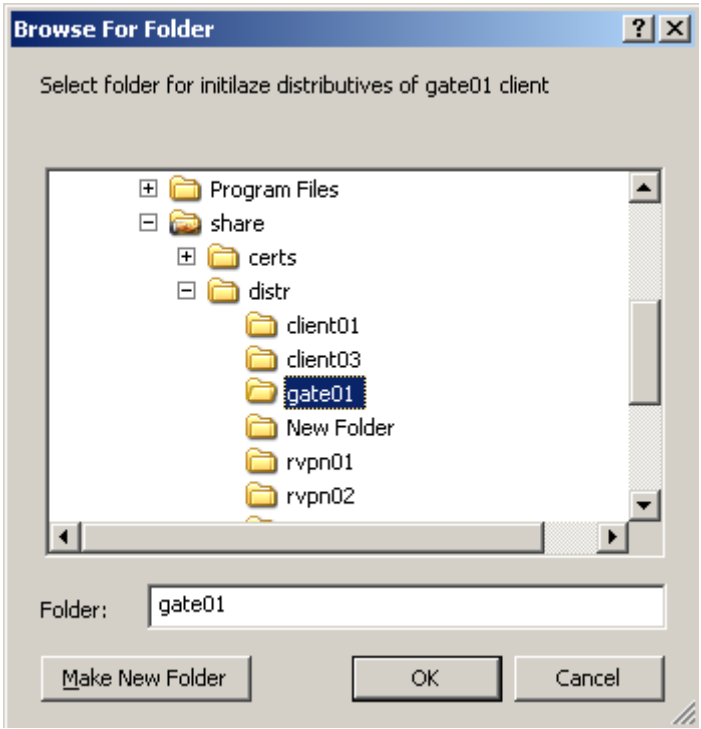

Рисунок 79

В указанный каталог будут сохранены два файла (Рисунок 80):

- `setup_product.sh` – скрипт, содержащий данные для продукта CSP VPN Gate;
- `setup_upagent.sh` – скрипт, содержащий данные для VPN UPAgent (Клиент обновления).

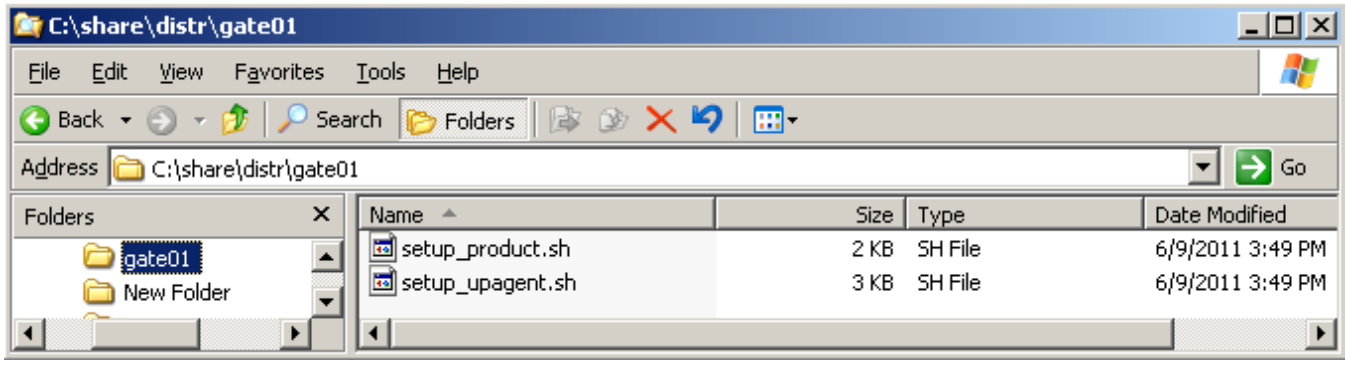
C:\share\distr\gate01
File Edit View Favorites Tools Help
Back Search Folders
Address C:\share\distr\gate01
Go
Folders
gate01
New Folder
Name Size Type Date Modified
setup_product.sh 2 KB SH File 6/9/2011 3:49 PM
setup_upagent.sh 3 KB SH File 6/9/2011 3:49 PM

Рисунок 80

Инсталляция Клиента обновления и CSP VPN Gate

Установка созданных скриптов осуществляется в другом порядке, чем на vpn-устройство с CSP VPN Server/CSP VPN Client, а именно – сначала скрипт `setup_upagent.sh`, а затем - `setup_product.sh`. Такой порядок обусловлен тем, что для успешного выполнения скрипта `setup_product.sh`, необходим установленный Клиент обновления.

На vpn-устройство с работающим продуктом CSP VPN Gate версии 3.1 установка созданных скриптов осуществляется локально, так как Клиент обновления на этом устройстве еще не установлен. Поэтому доставьте скрипты на шлюз безопасности по заслуживающему доверия каналу связи и выполните их локальную установку.

Скрипты являются текстовыми файлами, их можно скопировать (например, в Wordpad) и для доставки на шлюз использовать терминальную программу, например, Putty Configuration, которая распространяется бесплатно (Рисунок 81).

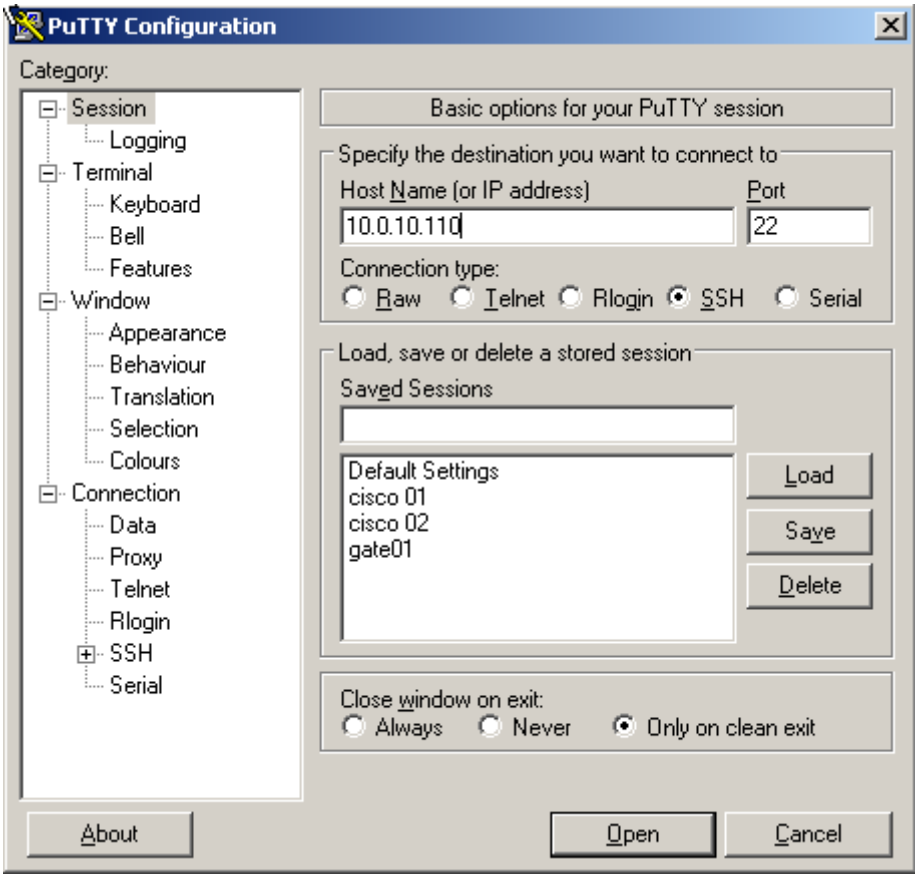

Рисунок 81

После открытия терминальной сессии со шлюзом в появившееся окно вставьте скопированный скрипт, например, в каталог `/tmp`, и нажмите Ctrl-C (Рисунок 82).

Рисунок 82

Аналогичным образом доставьте на шлюз второй скрипт `setup_product.sh`.

Измените права доступа к скриптам, выполнив команды:

```
[root@cspgate ~]# chmod +x /tmp/setup_upagent.sh
[root@cspgate ~]# chmod +x /tmp/setup_product.sh
```

Запустите скрипты на выполнение:

```
[root@cspgate ~]# /tmp/setup_upagent.sh
Info: libidn is already installed
Info: Link /var/log/upagent to /tmp is make successfully
```



```
Info: VPNUPAgent is installed successfully
Adding new rndm:
Nick name: cpsd
Name device: CPSD RNG
Level: 1
Succeeded, code:0x0
File decompression...

cacert.cer
reg.txt
settings.txt

...Done
Starting VPN UPAgent watchdog daemon.done.
Initialization is successful
```

```
[root@cspgate ~]# /tmp/setup_product.sh
VPN data are set successfully
Stopping VPN UPAgent watchdog daemon..done.
Starting VPN UPAgent watchdog daemon.done.
```

При запуске скрипта `setup_upagent.sh` выполняется проверка - установлен ли продукт VPNUPAgent. Если он еще не установлен, то устанавливаются необходимые дистрибутивы и настраивается среда функционирования. В процессе установки дистрибутивов возможны интерактивные запросы на подтверждение действий.

Дистрибутивы продукта VPNUPAgent размещены на шлюзе в каталоге `/packages/VPNUPAgent`. Если это не так, то в каталоге установленного Сервера обновления имеется архив `vpnupagent.tar`:

```
для ОС Red Hat Enterprise Linux 5
C:\Program Files\UPServer\upagent\LINUXRHEL5\vpnupagent.tar

для ОС Solaris 10
C:\Program Files\UPServer\upagent\SOLARIS\vpnupagent.tar
```

Далее самостоятельно выполните действия по размещению архива на шлюзе:

```
mkdir /packages
cd /packages
tar xvf vpnupagent.tar
```

При успешном выполнении скриптов устанавливается соединение с Сервером обновления для проверки возможности скачивания обновлений. Состояние клиента в таблице клиентов Сервера обновления изменится с waiting на updating, а затем на active. В состоянии active клиент готов к скачиванию обновлений (Рисунок 83).

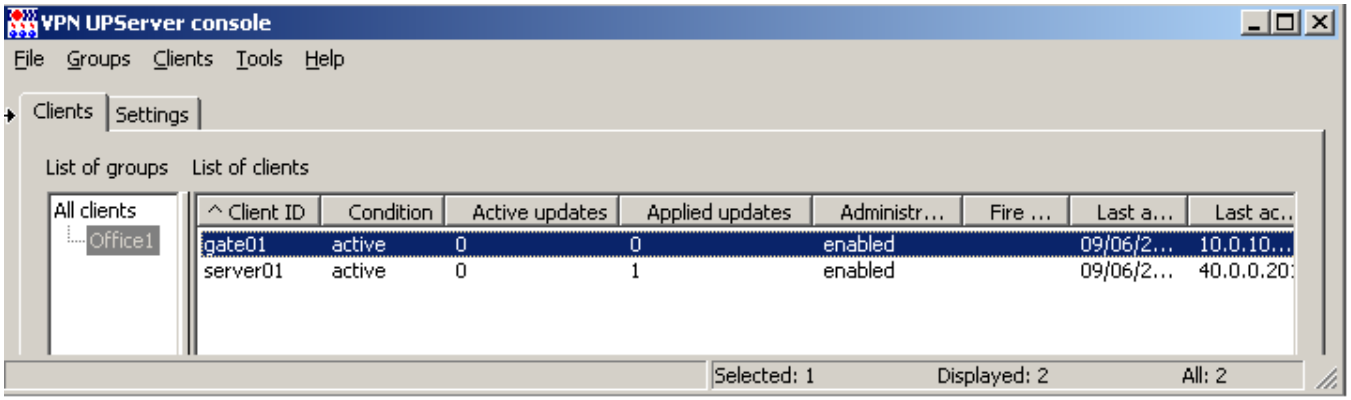

Рисунок 83

Создание обновлений для CSP VPN Gate

Создание обновлений для клиента с установленным продуктом CSP VPN Gate выполняется также как и для CSP VPN Server/CSP VPN Client. Данная процедура была описана в разделе «Создание обновлений. Пример успешного обновления клиента».

Обновление сертификата

Сценарий обновления сертификата на управляемом vpn-устройстве осуществляется в несколько этапов:

1. создайте на Сервере обновления учетную запись клиента для данного vpn-устройства, установите на нем дистрибутивы Клиента обновления и продукта CSP VPN Agent, как описано в предыдущих главах
2. на Сервере обновления для клиента подготовьте обновление, которое включает в себя случайную последовательность чисел, имя контейнера для ключевой пары и пароль на этот контейнер
3. Клиент обновления скачает подготовленное обновление, на клиенте создастся ключевая пара и запрос на сертификат
4. на Сервере обновления появится новая информация о клиенте - создан контейнер с ключевой парой и запрос на сертификат. С Сервера обновления отошлите запрос в Центр сертификации, а затем получите локальный сертификат для клиента
5. на Сервере обновления подготовьте обновление для данного клиента, включающее новый локальный сертификат и имя контейнера
6. скачав и применив обновление, Клиент обновления установит новый сертификат.

Предположим, что на клиенте установлен и работает продукт CSP VPN Server с криптографией КриптоПро CSP. Для аутентификации продукт использует локальный сертификат с полем `CN=Certificate of client server01 new`. Контейнер с секретным ключом размещен в Реестре - `\\.\REGISTRY\REGISTRY\\vpn4c9934df`. Требуется заменить имеющийся сертификат на новый. Далее опишем все перечисленные действия.

Настройка ДСЧ на клиенте с CSP VPN Server/CSP VPN Client

Для возможности создания новой ключевой пары и запроса на сертификат на клиенте, выберите в качестве ДСЧ датчик, называемый «КриптоПро Исходный Материал». Для этого на клиенте запустите КриптоПро CSP 3.6, во вкладке Оборудование нажмите Настроить ДСЧ. В открывшемся окне предложение «КриптоПро Исходный Материал» переместите в верхнюю строку, как первый датчик случайных чисел и нажмите кнопку ОК (Рисунок 84).

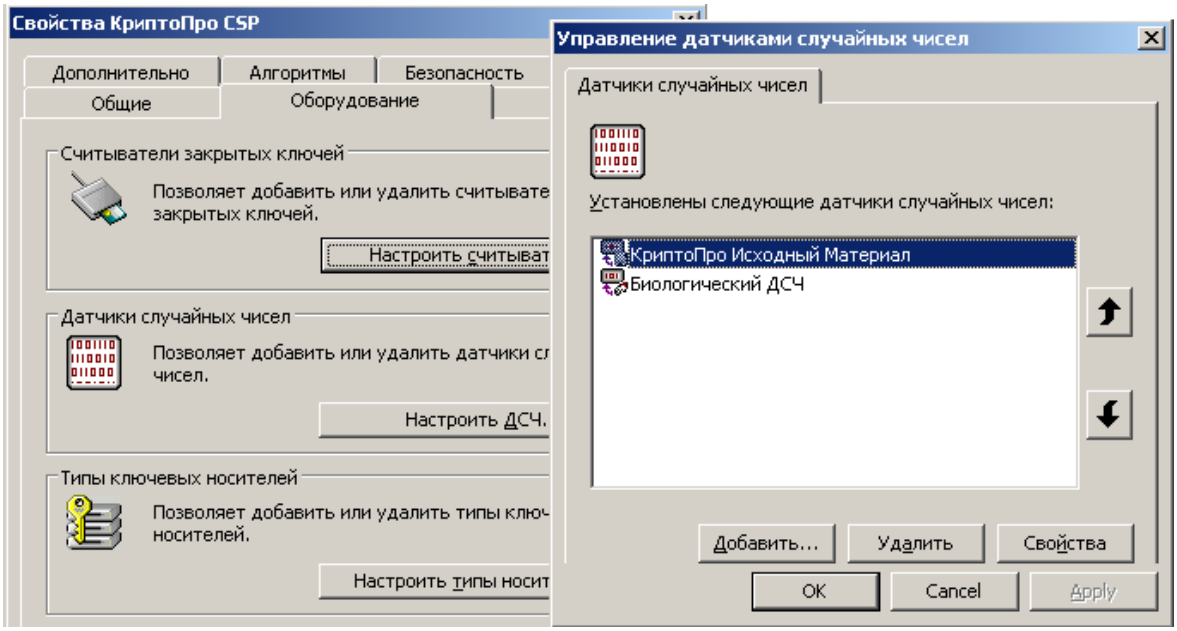

Рисунок 84

Настройка ДСЧ на клиенте с CSP VPN Gate

Для возможности создания новой ключевой пары и запроса на сертификат на шлюзе безопасности настройка ДСЧ, называемого «КриптоПро Исходный Материал», осуществляется автоматически при инициализации Клиента обновления (скрипт `setup_upagent.sh` вызывает другой скрипт `/packages/VPNUPAgent/install.sh`).

Создание обновления с параметрами ключевой пары и запроса на сертификат

На Сервере обновления выделите в таблице строку с клиентом, для которого надо обновить сертификат, и в контекстном меню выберите предложение Functions – Key pairs – Generate для создания ключевой пары и запроса на сертификат (Рисунок 85).

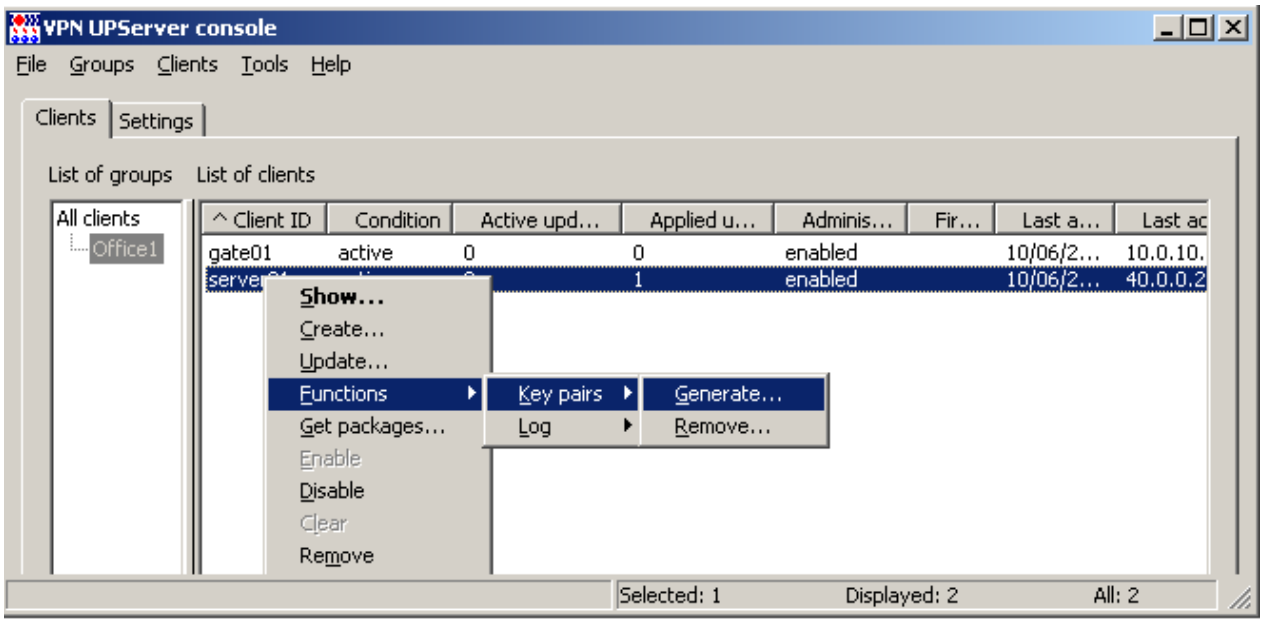

Рисунок 85

В открывшемся окне (Рисунок 86) заполните поля:

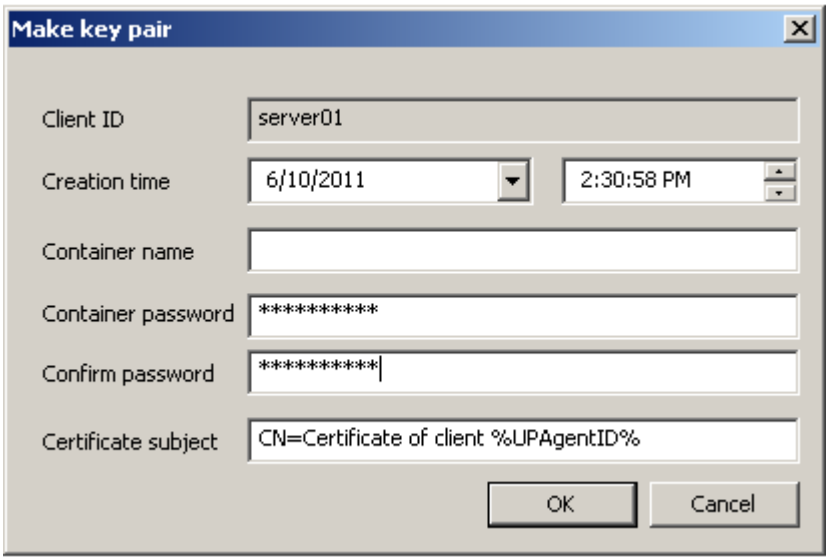

Рисунок 86

- Creation time – время, когда Сервер обновления сделает доступным для клиента обновление, содержащее необходимые данные для создания ключевой пары и запроса на сертификат
- Container name – имя контейнера на клиенте, в который будет записана ключевая пара. Если это поле не задано, то имя контейнера будет подобрано автоматически
- Container password – пароль для защиты контейнера. Если это поле не задано, то пароль для контейнера будет считаться пустым
- Confirm password – поле для повторного ввода пароля. Должен совпадать со значением Container password
- Certificate subject – строка, используемая в качестве поля Subject при создании запроса на сертификат. В этой строке можно использовать макросы, такие как %UPAgentID%, %UPAgentGroup% и т.п, которые будут заменены на их значения (список макросов, которые можно использовать, совпадает с переменными, передаваемыми в файл cook.bat при его запуске).

При нажатии кнопки OK предлагается выполнить «биологическую» инициализацию ДСЧ – понажимайте клавиши или перемещайте указатель мыши (Рисунок 87). Если на Сервере обновления установлен аппаратный ДСЧ, то данное окно не выводится.

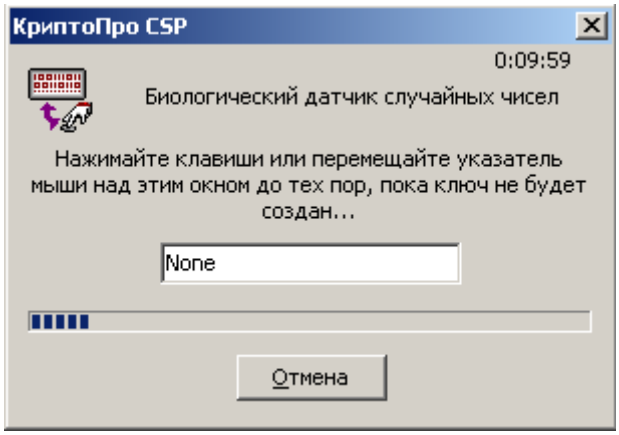

Рисунок 87

После этого в таблице клиентов появится новое обновление с параметрами ключевой пары и контейнера для данного клиента.

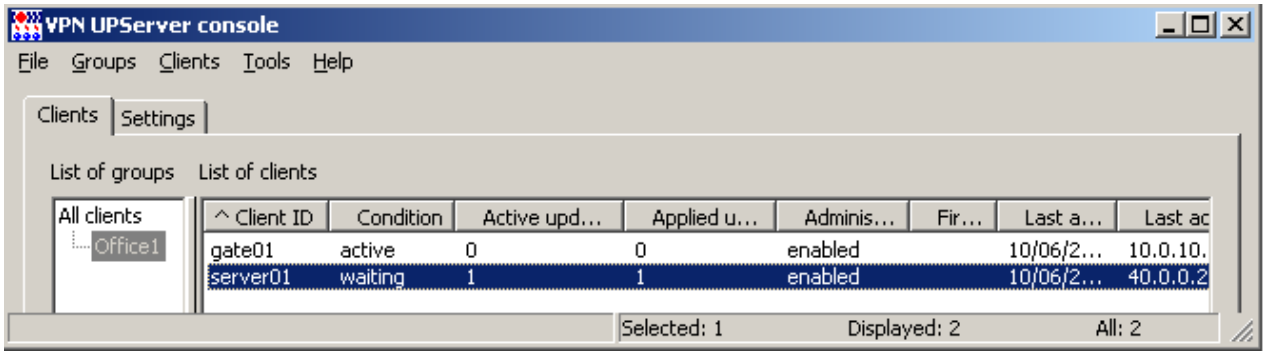

Рисунок 88

Создание на клиенте ключевой пары и запроса на сертификат

Через некоторое время обновление будет применено на клиенте (Рисунок 89), сопровождаясь созданием контейнера с ключевой парой и запроса на сертификат, которые можно увидеть на Сервере обновления.

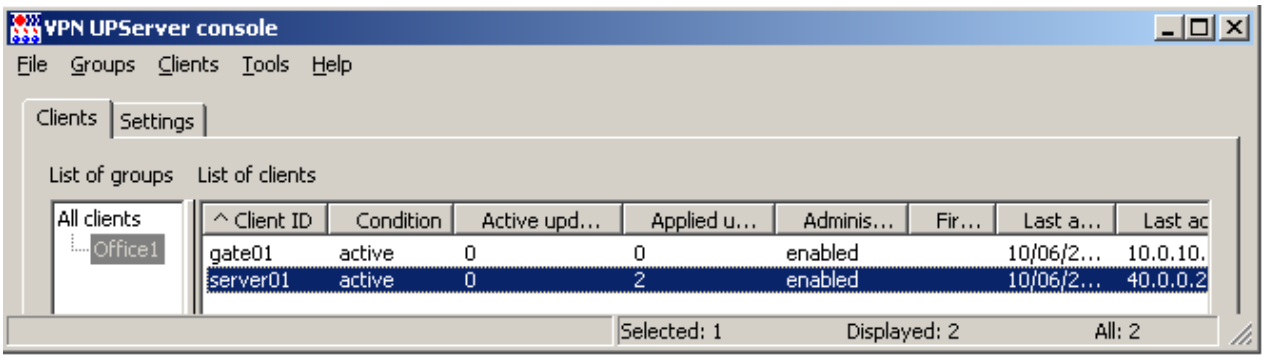

Рисунок 89

В контекстном меню для данного клиента выберите предложение Show.

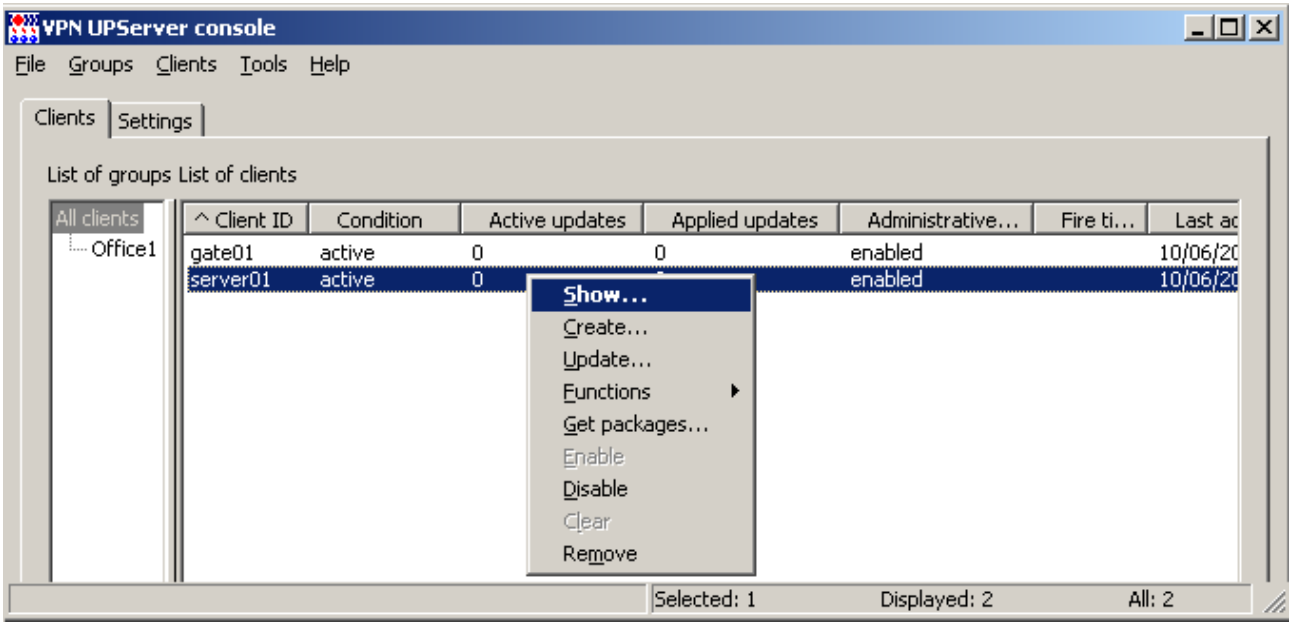

Рисунок 90

Во вкладке Containers для клиента server01 появилась запись о созданном контейнере (Рисунок 91):

- container name – имя созданного контейнера
- is used: FALSE – признак того, что контейнер еще не используется продуктом CSP VPN Server
- password id – уникальный идентификатор пароля к контейнеру
- certificate subject – строка, которая использовалась в качестве Subject при создании запроса на сертификат
- тело запроса на сертификат.

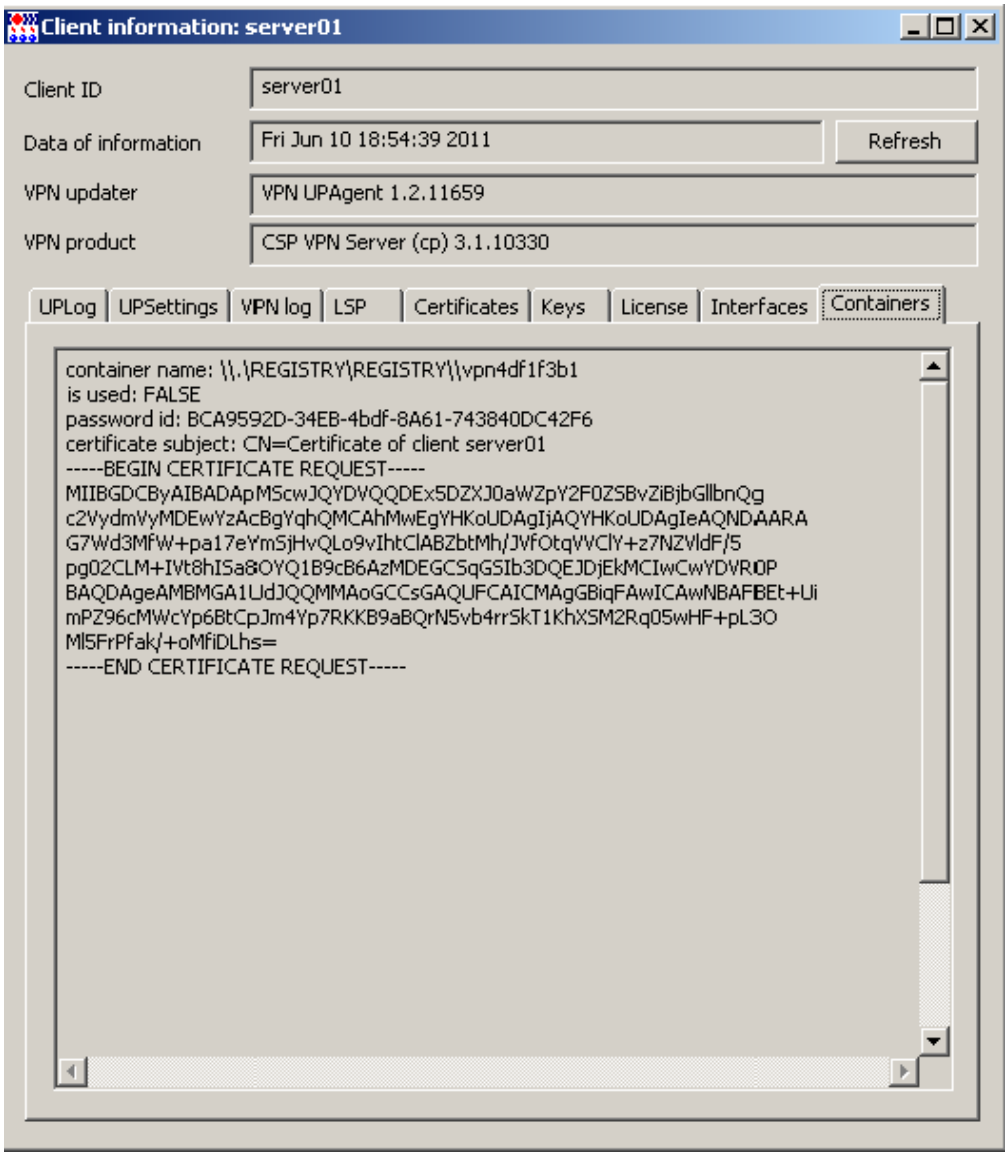
Client information: server01
Client ID
server01
Data of information
Fri Jun 10 18:54:39 2011
Refresh
VPN updater
VPN UPAgent 1.2.11659
VPN product
CSP VPN Server (cp) 3.1.10330
UPLog
UPSettings
VPN log
LSP
Certificates
Keys
License
Interfaces
Containers
container name: \\.\REGISTRY\REGISTRY\\vpn4df1f3b1
is used: FALSE
password id: BCA9592D-34EB-4bdf-8A61-743840DC42F6
certificate subject: CN=Certificate of client server01
-----BEGIN CERTIFICATE REQUEST-----
MIIBGDCByAIBADApMScwJQYDVQQDEx5DZXJ0aWZpY2F0ZSBvZiBjbGllbnQg
c2VydmVyMDEwYzAcBgYqhQMCAhMwEgYHKoUDAgIjAQYHKoUDAgIeAQNDAARA
G7Wd3MfW+pa17eYmSjHvQLo9vIhtClABZbtMh/JWfOtqVVClY+z7NZVldF/5
pg02CLM+IVt8hISa8OYQ1B9cB6AzMDEGCSqGSIb3DQEJDjEkMCIwCwYDVR0P
BAQDAgeAMBMGA1UdJQQMMAoGCCsGAQUFCAICMAgGBiqFAwICAwNBAFBEt+Ui
mPZ96cMWcYp6BtCpJm4Yp7RKKB9aBQrN5vb4rrSkT1KhX5M2Rq05wHF+pL3O
Ml5FrPfak/+oMfiDLhs=
-----END CERTIFICATE REQUEST-----

Рисунок 91

Создание сертификата

Используя тело запроса на сертификат, скопированного из вкладки Containers, отошлите его в Центр сертификации, используя, например, средства Microsoft Windows (Рисунок 92) или другие средства.

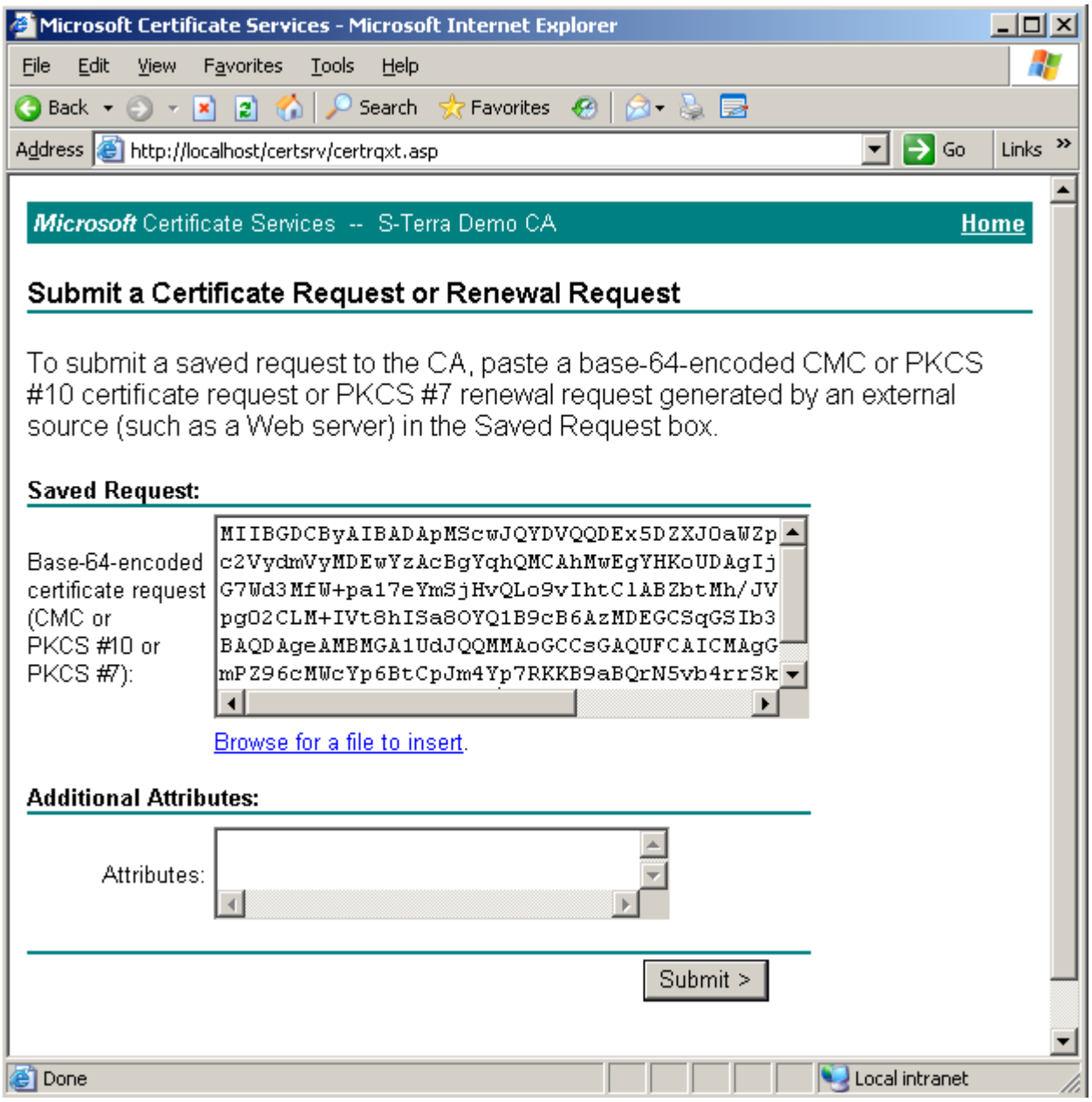

Рисунок 92

После получения созданного сертификата для клиента сохраните его на Сервере обновления.

Создание обновления с новым сертификатом

На Сервере обновления в контекстном меню выберите предложение Update (Рисунок 93).

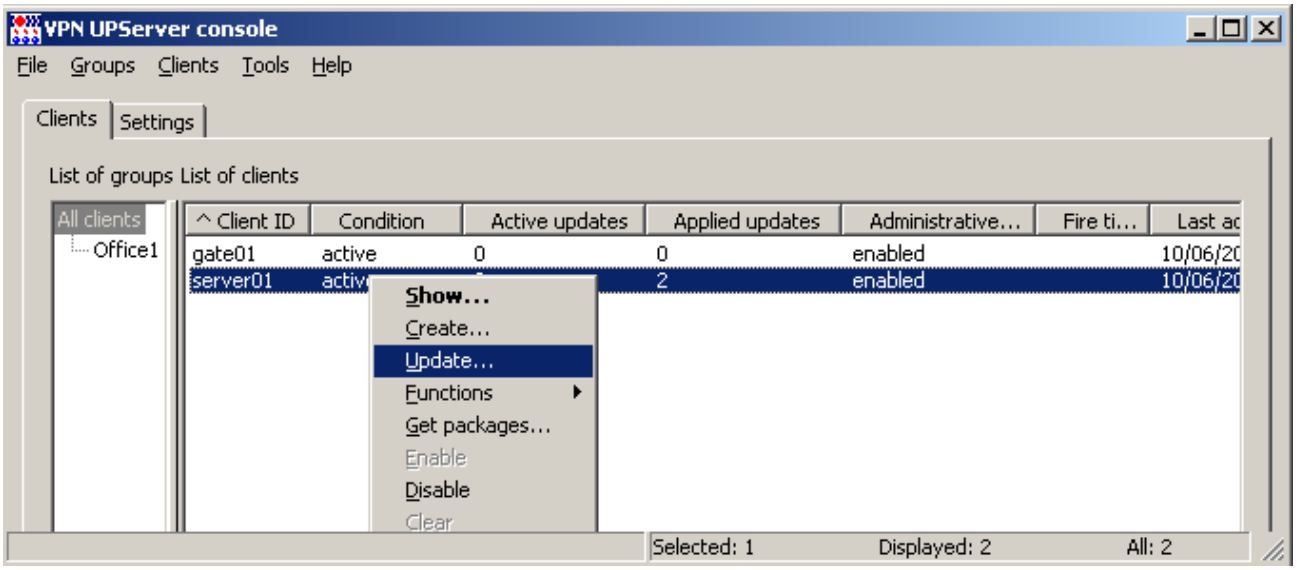

Рисунок 93

В открывшемся окне обновления клиента нажмите кнопку E (Рисунок 94).

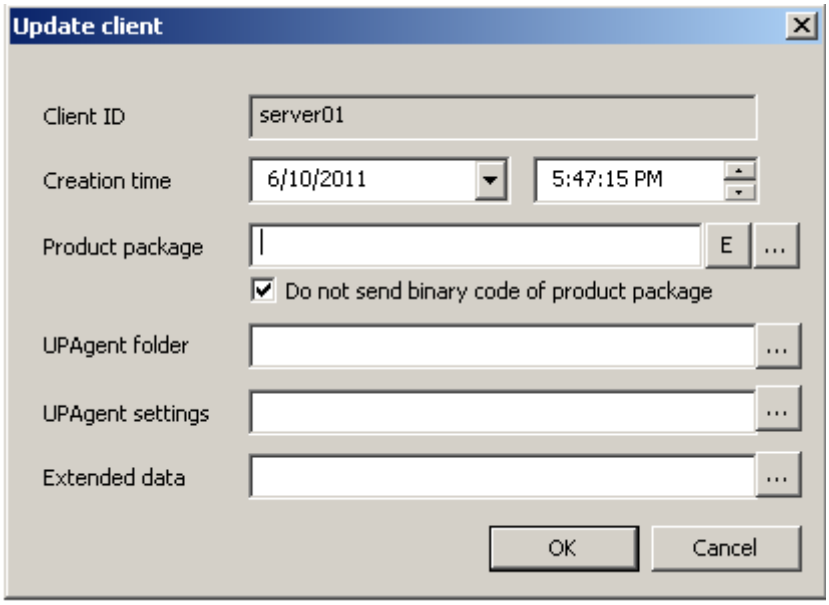

Рисунок 94

В окне VPN data maker перейдите во вкладку Certificates (Рисунок 95).

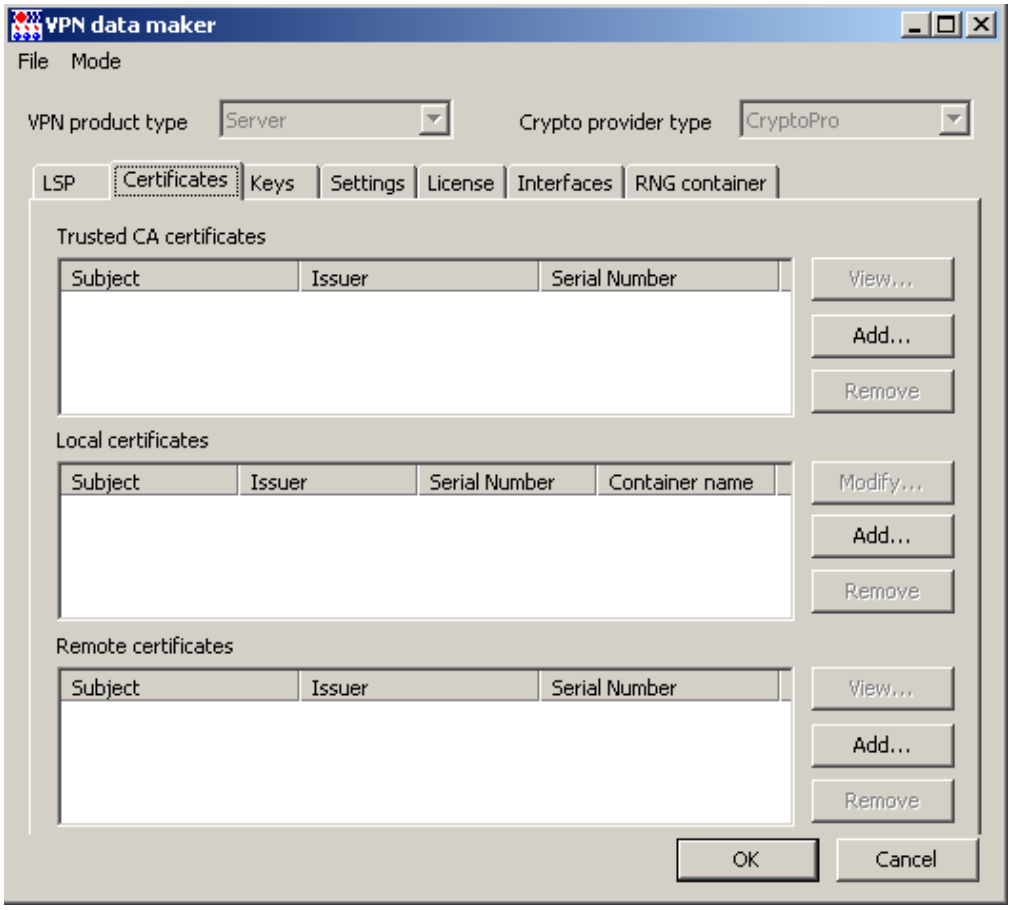

Рисунок 95

В разделе Local certificates нажмите кнопку Add и укажите файл с новым локальным сертификатом для клиента server01 (Рисунок 96).

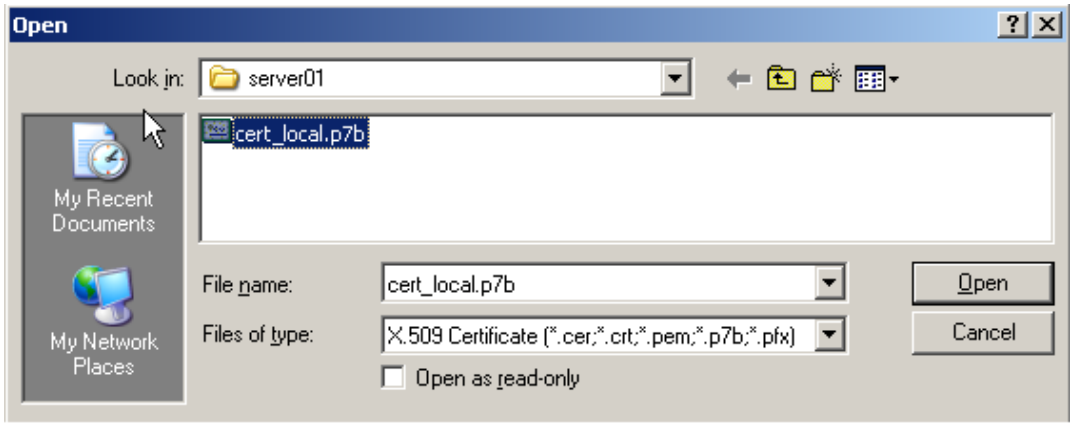

Рисунок 96

Из файла с сертификатами выберите нужный сертификат и нажмите ОК (Рисунок 97).

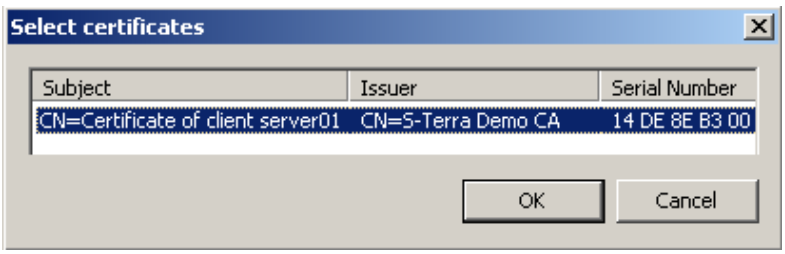

Рисунок 97

Выбранный сертификат добавится в раздел с локальными сертификатами данного клиента на Сервере обновления.

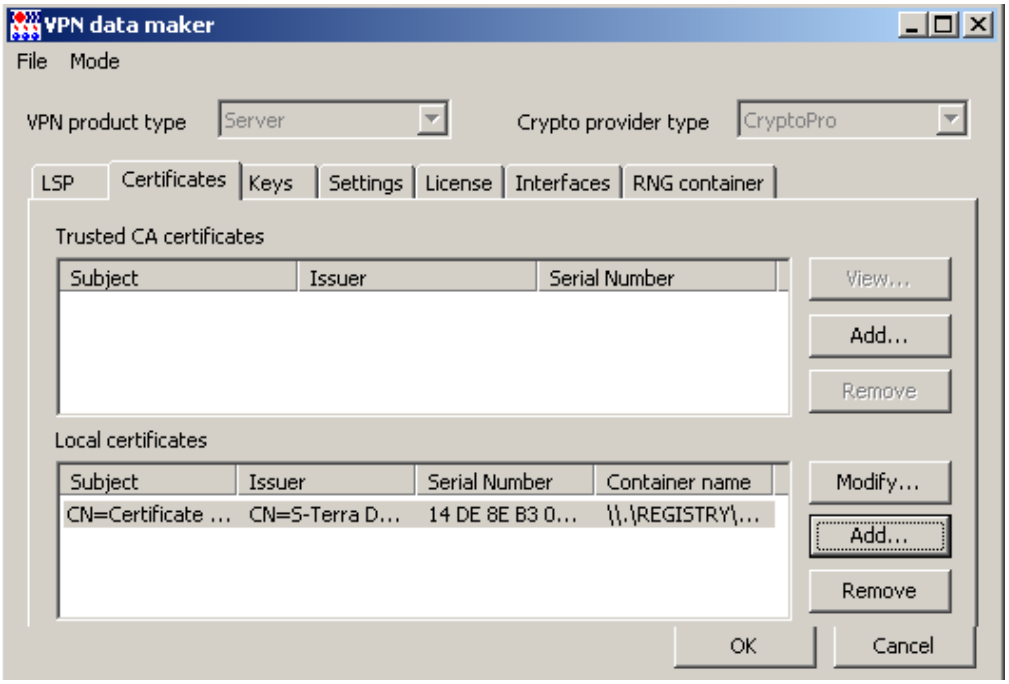

Рисунок 98

Если имя контейнера с секретным ключом и его пароль для нового сертификата не будут найдены, то появится окно для ввода имени контейнера и пароля (Рисунок 99).

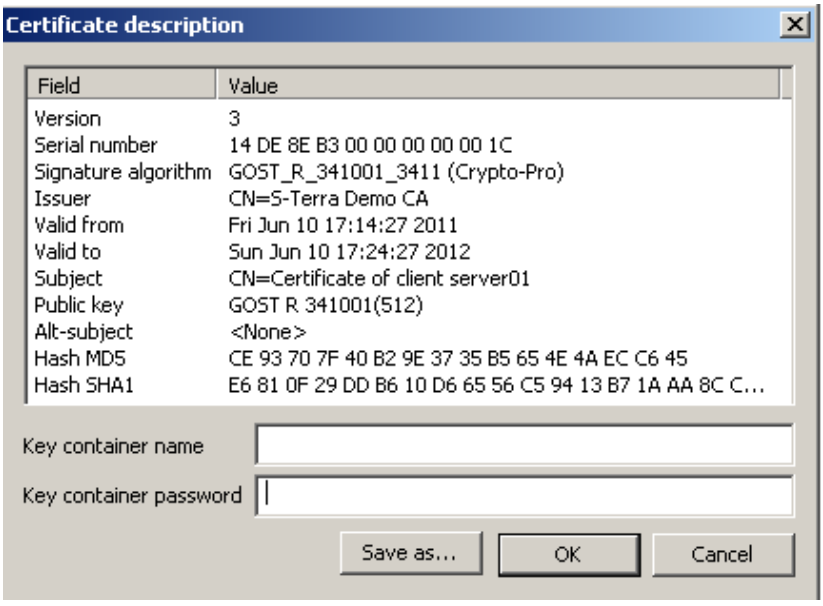

Рисунок 99

После указания локального сертификата нажмите кнопку OK в окне VPN data maker (Рисунок 98), создался новый файл с данными продукта CSP VPN Server – поле Product package (Рисунок 100).

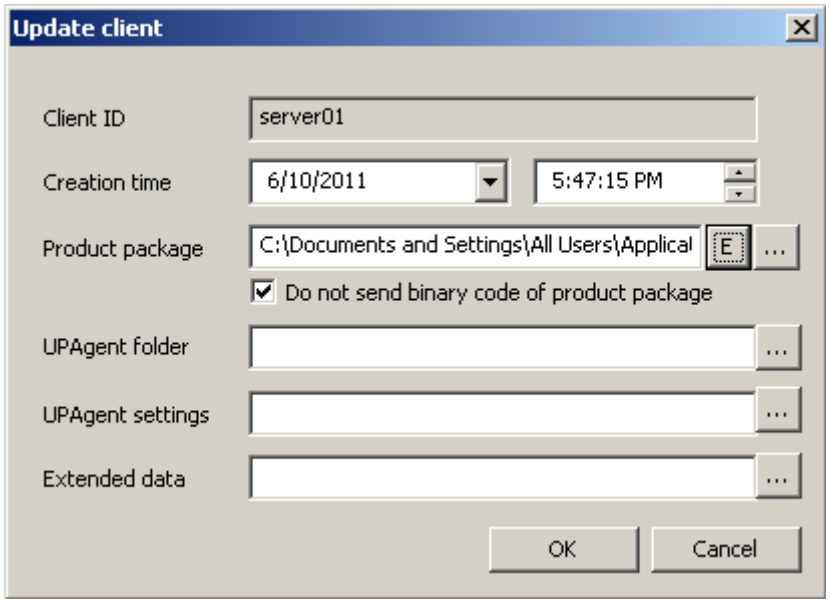

Рисунок 100

При нажатии кнопки OK появится новое обновление для server01 в таблице клиентов.

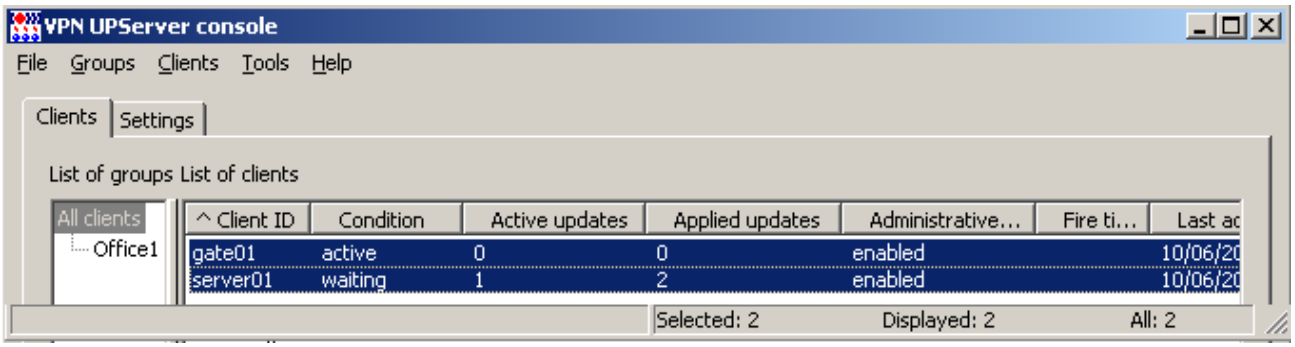

Рисунок 101

После применения обновления на клиенте вызовите Show в контекстном меню (Рисунок 102).

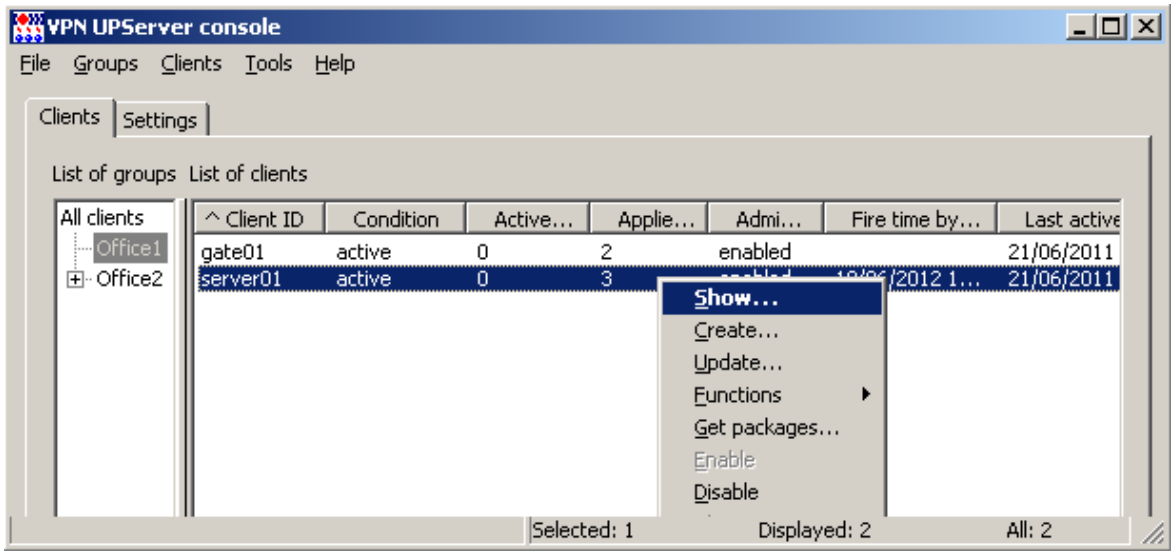

Рисунок 102

Во вкладке Certificates появился новый локальный сертификат, установленный на клиенте (Рисунок 103).

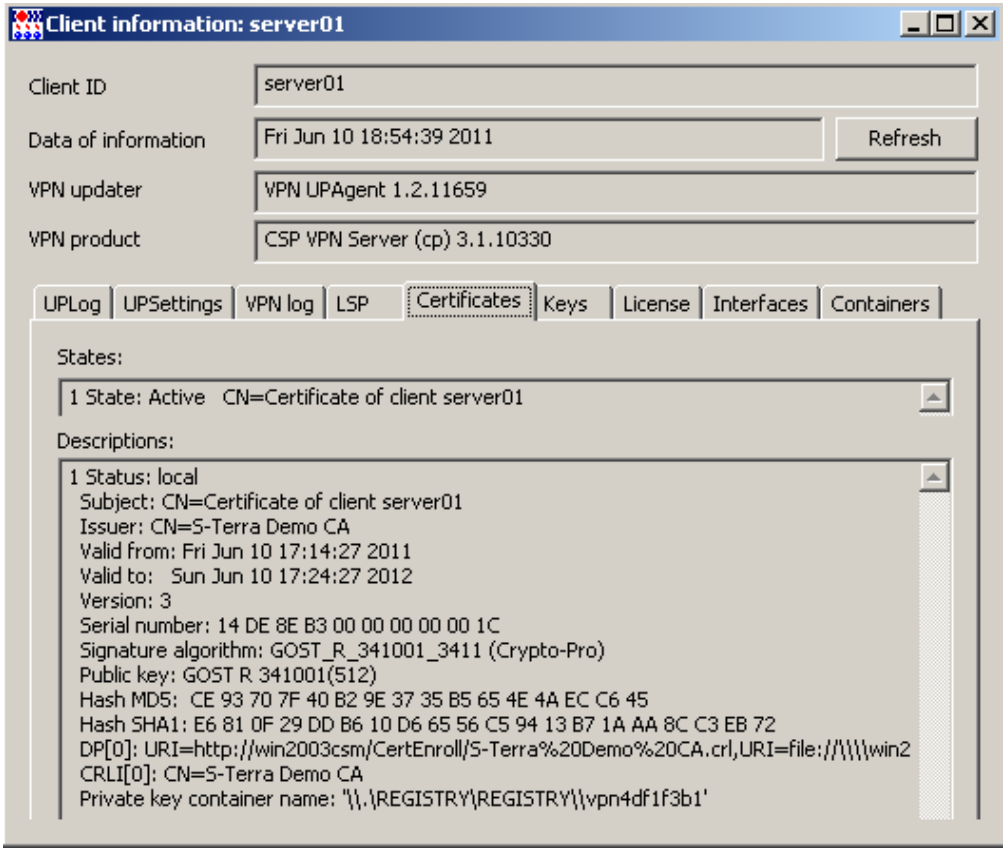

Рисунок 103

А во вкладке Containers у контейнера для данного сертификата появился статус TRUE (Рисунок 104).

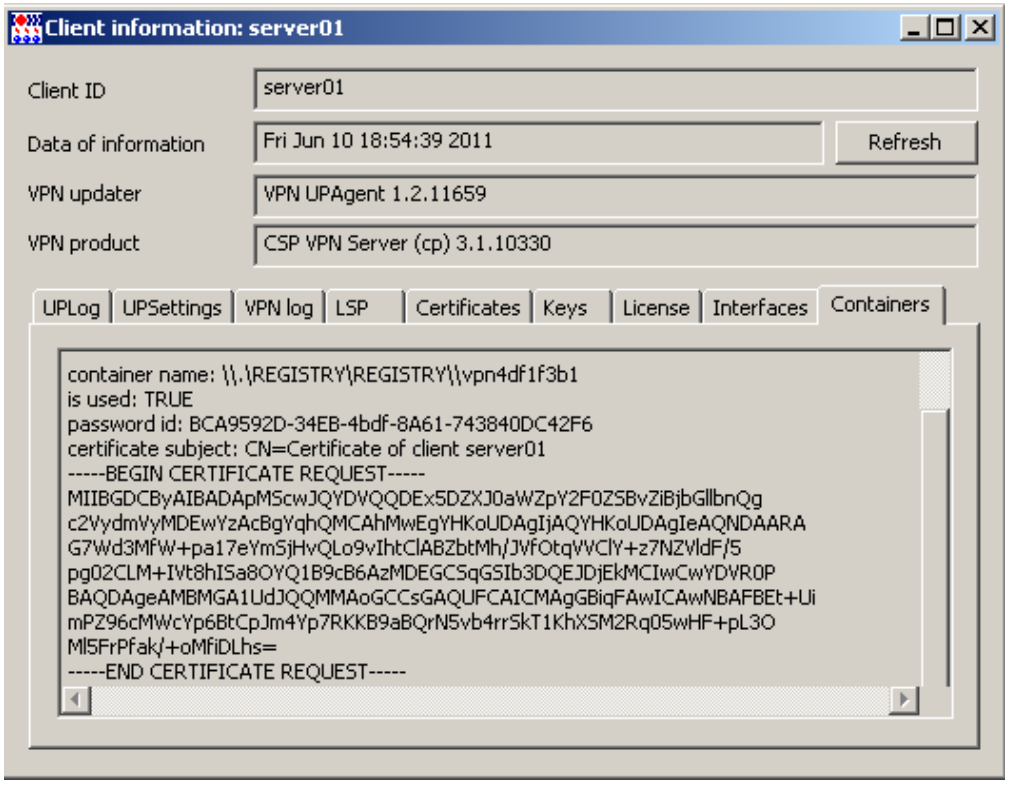

Рисунок 104

По такому сценарию можно создавать обновления с локальным сертификатом, CRL и сертификатами партнеров.


Note

Обратите внимание, что на момент замены сертификата на клиенте с CSP VPN Agent, другие vpn-устройства уже должны быть настроены на работу с новым сертификатом на CSP VPN Agent.

Групповые операции на Сервере обновления

В таблице клиентов Сервера обновления можно выделять несколько клиентов и применять к ним операции меню Clients, за исключением Create и Get package (Рисунок 105).

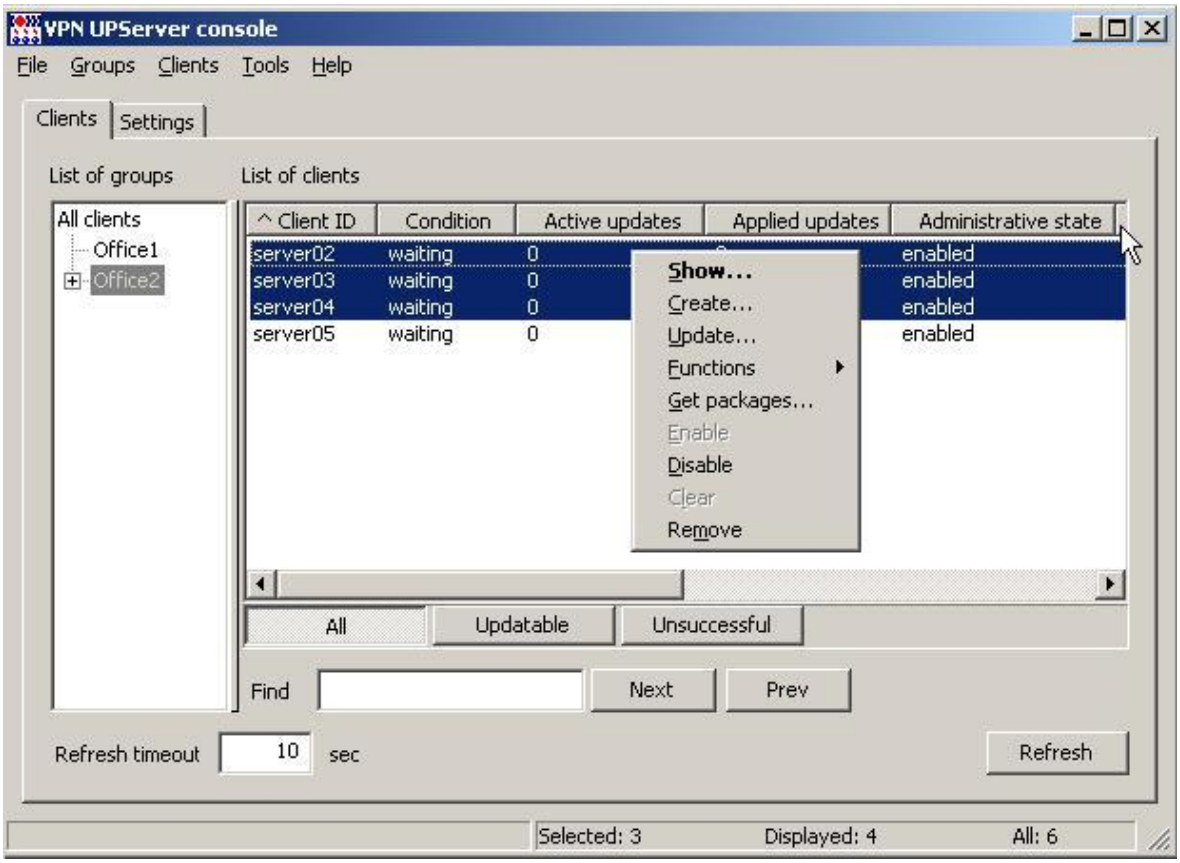

Рисунок 105

Каждый клиент на Сервере обновления создается отдельно и для каждого клиента дистрибутивы Клиента обновления и CSP VPN Agent также создаются отдельно.

Остальные операции могут применяться к любой выделенной группе клиентов.

Подробно операции меню Clients описаны в разделе «Меню Clients» главы «Описание меню Сервера обновления».

При выборе операции Update, для нескольких клиентов будут созданы одинаковые обновления. После применения этих обновлений клиенты будут иметь, например, одинаковую политику безопасности, один и тот же список предопределенных ключей, один и тот же список локальных сертификатов. Имея список локальных сертификатов, клиент не сможет создать соединение с партнером, так как будет использоваться первый сертификат списка. Чтобы избежать таких проблем с локальными сертификатами, используйте ***шаблон проекта***, при котором происходит отбор локального сертификата из списка для каждого клиента при обновлении.

Создание шаблона проекта

В меню Tools Сервера обновления выберите пункт меню VPN data maker (Рисунок 106).

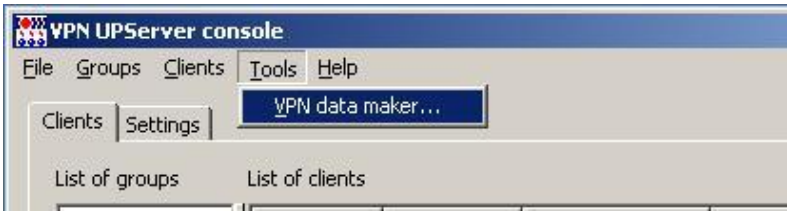

Рисунок 106

В открывшемся окне VPN data maker заполните необходимые вкладки для настройки продукта CSP VPN Agent (Рисунок 47). Во вкладке Cerificates можно создать список локальных сертификатов, для которых были созданы запросы на клиентах, список сертификатов партнеров, список удаленных сертификатов.

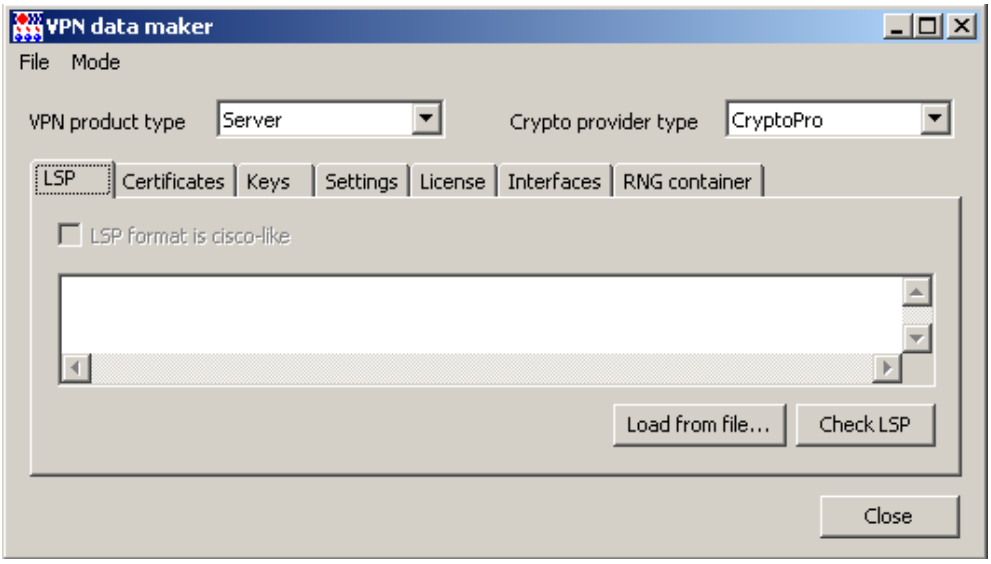

Рисунок 107

В окне VPN data maker перейдите в режим шаблона проекта, выбрав в меню `Mode` пункт `Enable template mode` (Рисунок 108).

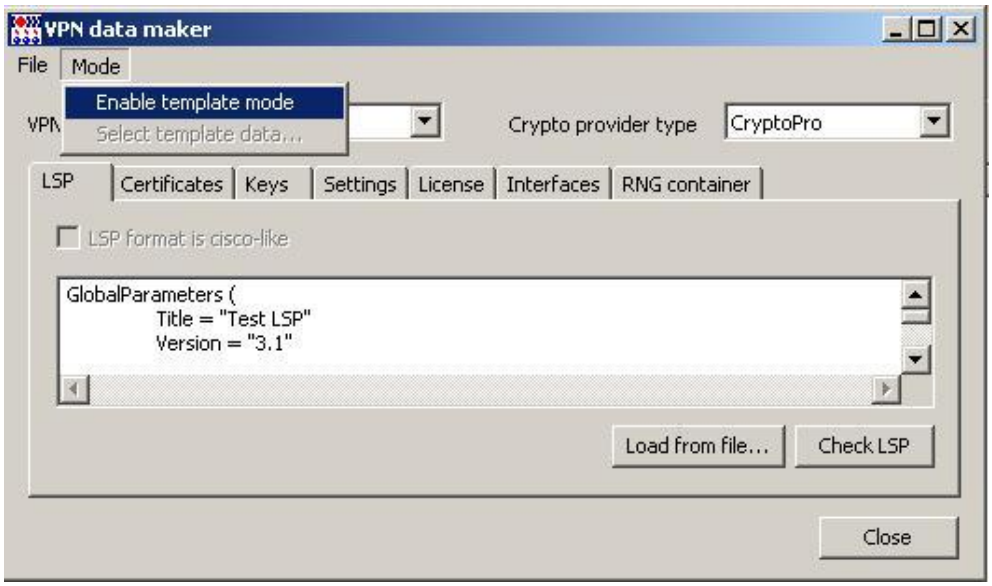

Рисунок 108

В режиме Mode выберите пункт Select template data (Рисунок 109).

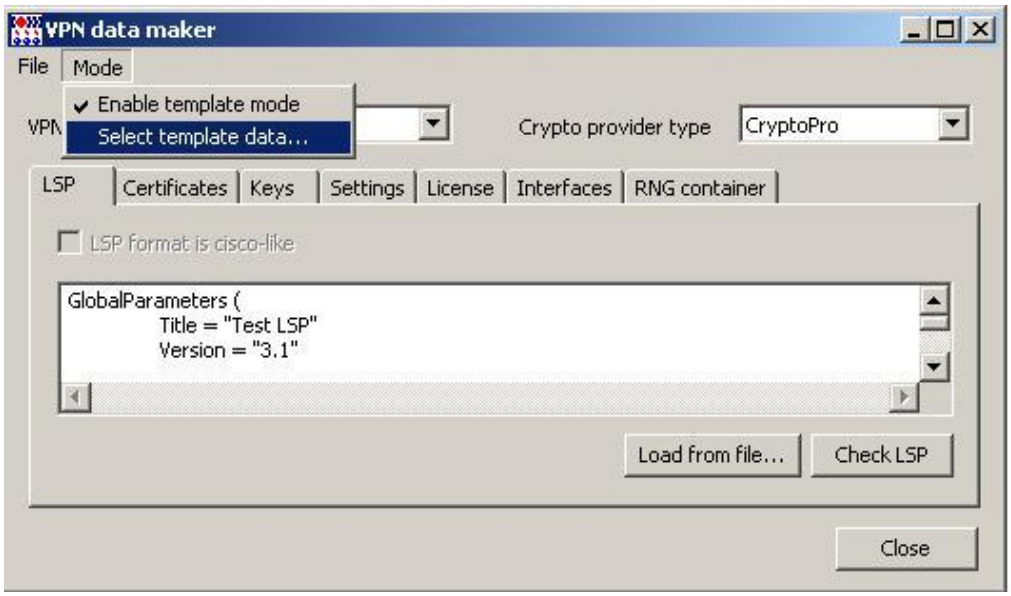

Рисунок 109

Появилось окно со списком данных, которые могут входить в шаблон проекта (Рисунок 110). Пометьте флажком данные, которые будут входить в шаблон. При применении обновления, созданного с использованием шаблона, только входящие в него данные будут изменяться на клиенте (см.описание в разделе «Меню Mode окна VPN data maker»).

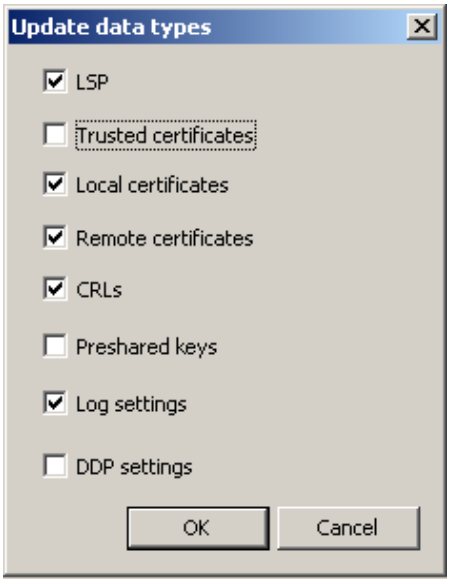

Рисунок 110

Нажмите кнопку OK. Сохраните созданный шаблон проекта в файл, выбрав пункт Save as… (Рисунок 111).

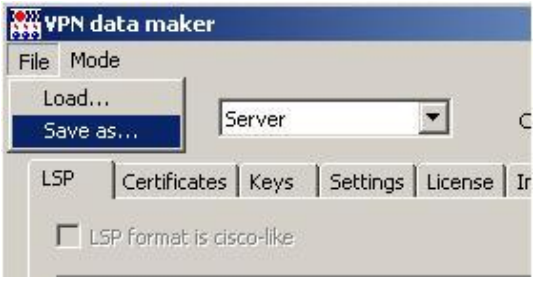

Рисунок 111

Использование шаблона проекта

Шаблон проекта удобно использовать при создании обновления сразу для нескольких клиентов. Для этого на Сервере обновления выделите в таблице несколько клиентов, в контекстном меню выберите предложение Update

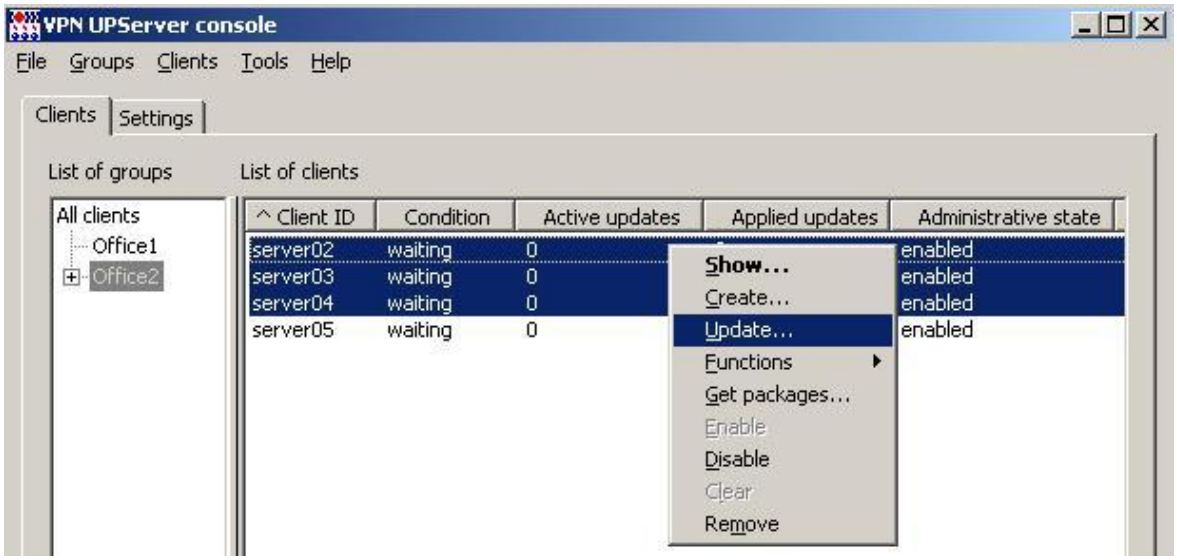

Рисунок 112

В открывшемся окне Update clients в поле Product package нажмите кнопку […] и в стандартном окне открытия файла укажите файл с шаблоном проекта (Рисунок 113).

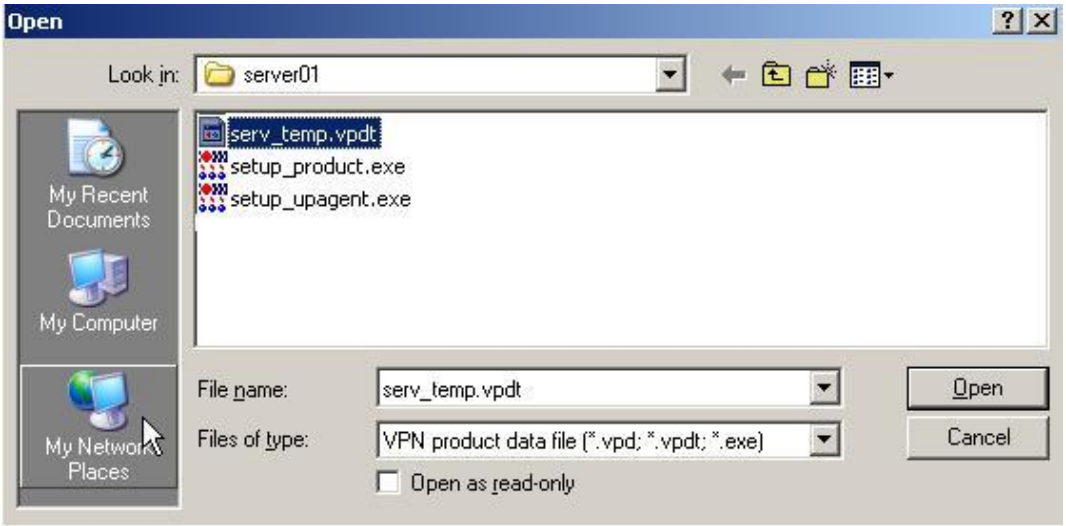

Рисунок 113

При применении обновлений, созданных с использованием шаблона проекта, только входящие в него данные будут изменяться на клиентах. Если в шаблон входит список локальных сертификатов, то при применении обновления каждый клиент будет отбирать для себя локальный сертификат из списка, выполняя проверку соответствия имеющегося у него запроса на сертификат и открытого ключа с информацией в сертификате. Такая проверка будет выполняться только при использовании шаблона. При отсутствии на клиенте запроса на его локальный сертификат такая проверка не выполняется и локальный сертификат на клиенте не обновляется.

Действия пользователя при обновлении

Сценарий обновления на управляемом vpn-устройстве зависит от настройки Режим запроса подтверждения у пользователя о начале обновления на Клиенте обновления. По умолчанию эта настройка имеет значение auto – для продукта CSP VPN Client всегда будет запрашиваться разрешение на применение обновления, для CSP VPN Server и CSP VPN Gate такое разрешение не запрашивается.

При получении обновления Клиент обновления проверяет тип установленного на компьютере VPN-продукта, и при наличии CSP VPN Client на панель состояния операционной системы выводится иконка в виде красного флажка и сообщение с просьбой запустить процесс обновления (Рисунок 114).

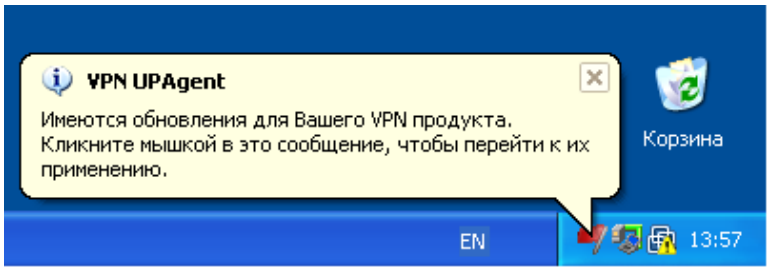

Рисунок 114

Двойное нажатие мышки на этой иконке или теле сообщения приводит к появлению окна с отображением процесса обновления (Рисунок 115). При нажатии кнопки Start процесс обновления запустится.

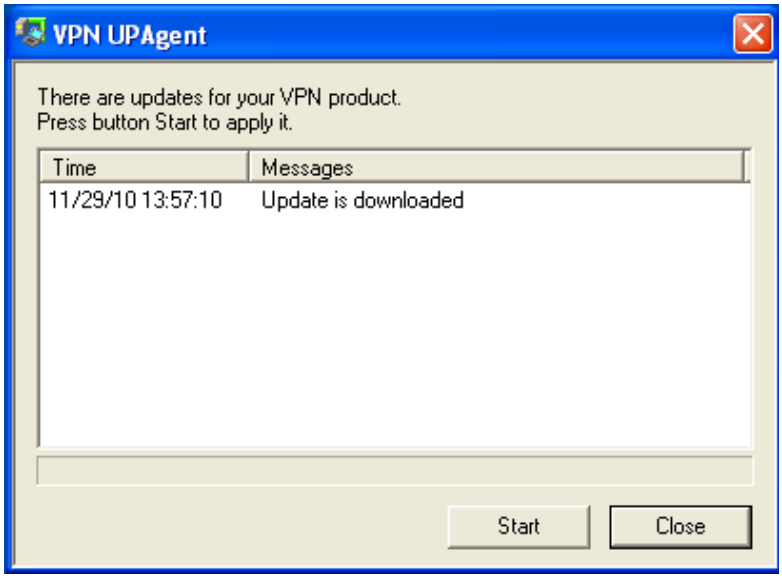

Рисунок 115

Если пароль логина в продукт CSP VPN Client не пустой, то в процессе обновления может запрашиваться пароль для изменения данных в базе продукта CSP VPN Client (Рисунок 116). Необходимо задать пароль и нажать кнопку OK. При отказе задать пароль - обновление будет считаться неуспешным (все данные будут возвращены в прежнее состояние, сообщение о неудачном обновлении будет отправлено администратору).

Рисунок 116

В окне VPN UPAgent отображаются все этапы обновления продукта. При удачном завершении процесса обновления будет выдана строка «Update is applied successfully» (Рисунок 117).

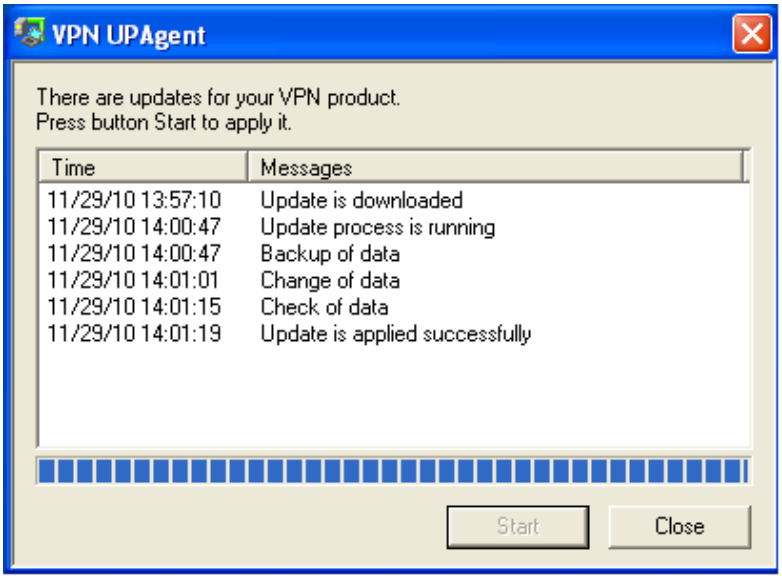

Рисунок 117

А над иконкой с красным флажком появится сообщение «Обновление применено» (Рисунок 118). Через некоторое время это сообщение и иконка исчезнут.

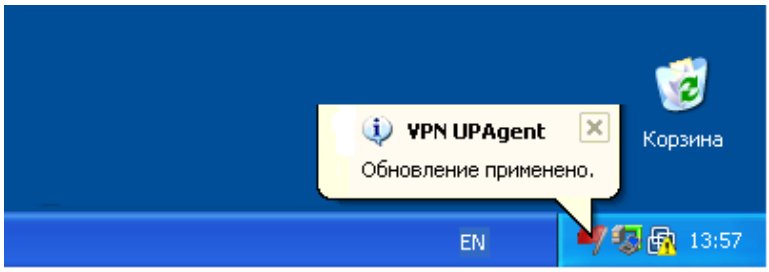

Рисунок 118

При неуспешном обновлении в окне VPN UPAgent появится строка «Update is not applied», а над красным флажком появится сообщение «Обновление не применено». Окно и сообщение через некоторое время исчезнут.

Описание меню Сервера обновления

Графический интерфейс приложения VPN UPServer console содержит следующие элементы (Рисунок 15).

Меню File

Меню File включает одно предложение:

Exit – завершает работу консоли управления (обслуживание клиентов при этом не завершается).

Меню Groups

Меню Groups содержит следующие элементы:

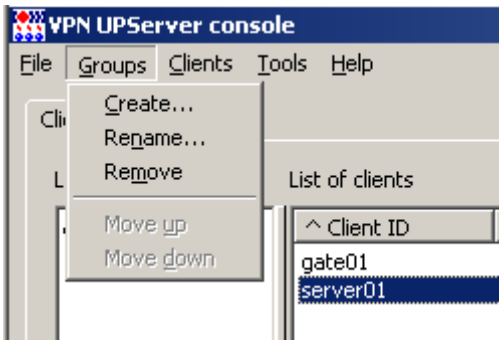

Рисунок 119

Create… - вызывает окно создания новой группы (группа создается как подгруппа выделенной группы), в котором надо задать имя группы (Рисунок 120).

`Parent group name` – имя группы, в которой создается подгруппа

`Group name` – имя создаваемой подгруппы.

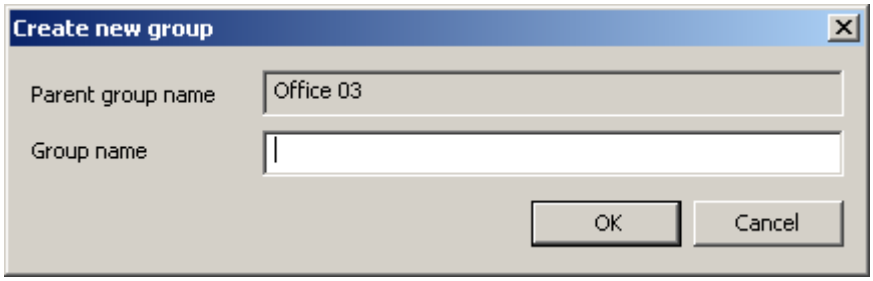

Рисунок 120

Rename… - вызывает окно переименования выделенной группы, в котором задается новое имя группы (Рисунок 121).

`Parent group name` – имя группы, в которой переименовывается подгруппа

`Group name` – новое имя подгруппы.

При переименовании группы все входящие в нее клиенты и группы сохраняются.

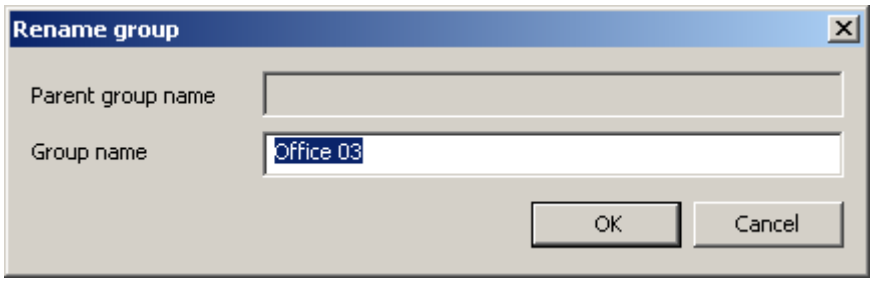

Рисунок 121

Remove – удаляет выделенную группу; при этом все клиенты и подгруппы, входящие в нее, перемещаются в группу уровнем выше

Move up – перемещает выделенную группу в списке вверх, сохраняя уровень группы в дереве

Move down – перемещает выделенную группу в списке вниз, сохраняя уровень группы в дереве.

Меню Clients

Меню Clients содержит следующие элементы:

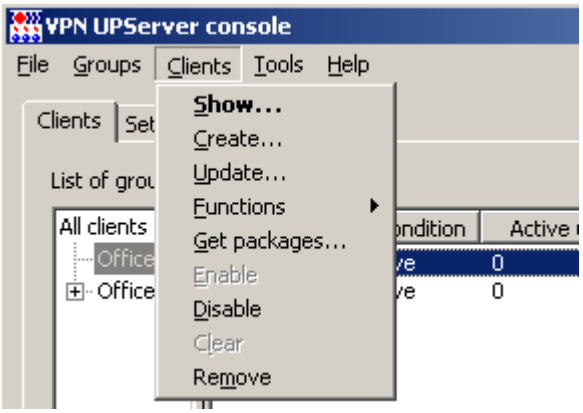

Рисунок 122

Show… – вызывает окно отображения параметров существующего клиента (Рисунок 52)

Create… – вызывает окно создания нового клиента (Рисунок 28)

Update… – вызывает окно создания обновления для существующего клиента (Рисунок 45)

Functions – вызывает подменю:

`Key pairs` – позволяет задать действия с ключевой парой на управляемом vpn-устройстве

`Log` – позволяет задать настройки протоколирования событий на управляемом vpn-устройстве

С ключевой парой возможны два действия (Рисунок 123):

`Generate…` - создание ключевой пары на управляемом vpn-устройстве

`Remove…` -удаление ключевой пары с управляемого vpn-устройства

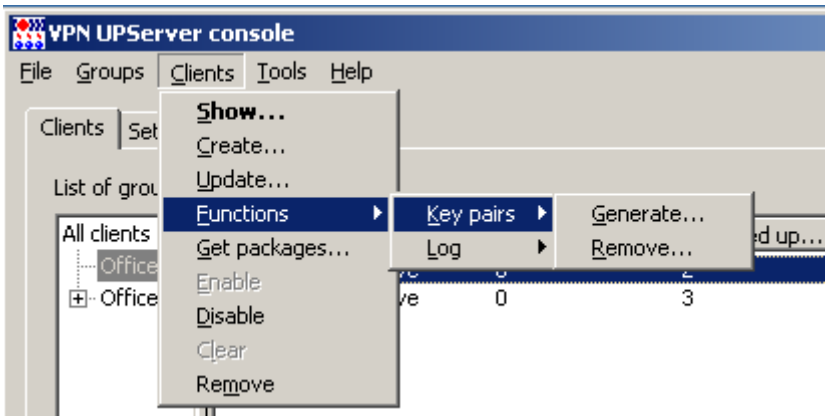

Рисунок 123

При выборе предложения `Generate` появляется окно Make key pair для задания параметров ключевой пары (см. Рисунок 86 и описание к нему)

При выборе предложения `Remove` появляется окно Remove container для задания параметров удаляемой ключевой пары (Рисунок 124):

`Creation time` – дата и время, когда Сервер обновления сделает доступным для скачивания Клиентом обновления пакет обновления, содержащий данные для удаления ключевой пары на управляемом vpn-устройстве. Если указанное время уже прошло, то пакет обновления будет открыт для скачивания сразу после его создания

`Container name` – имя контейнера на управляемом vpn-устройстве, который будет удален. Поле является обязательным для заполнения.
В выпадающем списке присутствуют имена существующих, но не используемых VPN-продуктом контейнеров

`Container password` – пароль контейнера, который будет использоваться при удалении. Если это поле не задано, то пароль считается пустым.

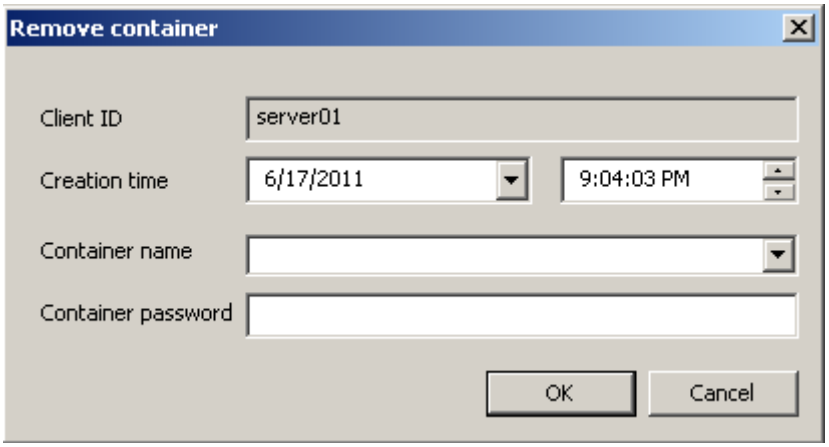

Рисунок 124

С настройками протоколирования возможны два действия (Рисунок 125):

`Setup…` - задание параметров протоколирования на управляемом vpn-устройстве

`Request…` - запрос данных из системы протоколирования на управляемом vpn-устройстве

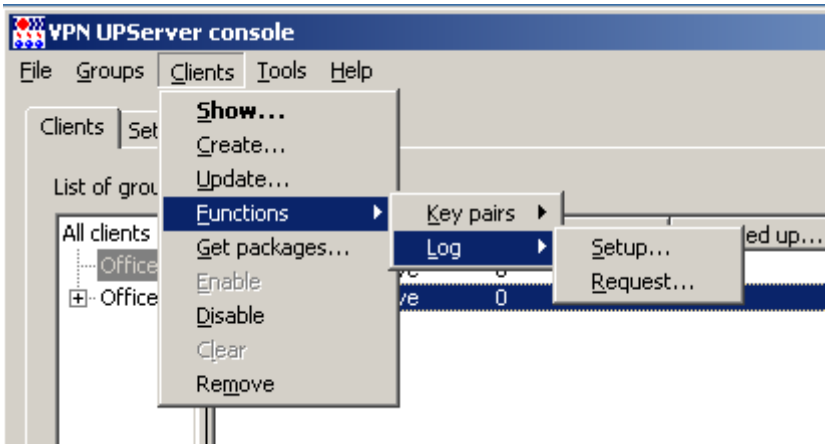

Рисунок 125

При выборе предложения `Setup` появляется окно `Setup log` для задания параметров (Рисунок 126):

`Creation time` – дата и время, когда Сервер обновления сделает доступным для скачивания пакет обновления, содержащий данные для настройки протоколирования на управляемом vpn-устройстве. Если указанное время уже прошло, то пакет обновления будет открыт для скачивания сразу после его создания

`State` – состояние системы протоколирования:

ON – включить пересылку syslog сообщений в стандартную систему протоколирования операционной системы Windows

OFF – выключить пересылку syslog сообщений в стандартную систему протоколирования операционной системы Windows

Эта настройка работает только для управляемых vpn-устройств с ОС Windows. Для устройств с ОС Unix эта настройка не применяется, журналирование на таких устройствах включено по умолчанию и не может быть отключено.

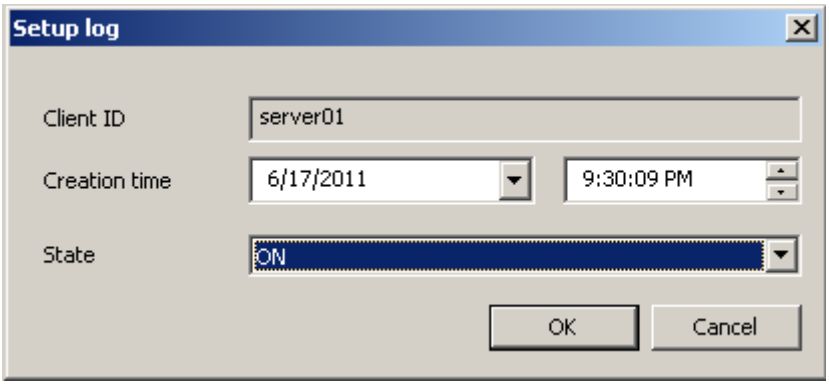

Рисунок 126

При выборе предложения `Request` появляется окно `Request log` для запроса данных из системы протоколирования управляемого vpn-устройства (Рисунок 127):

`Creation time` – дата и время, когда Сервер обновления сделает доступным для скачивания пакет обновления, содержащий данные для запроса данных протоколирования syslog канала. Если указанное время уже прошло, то пакет обновления будет открыт для скачивания сразу после его создания.

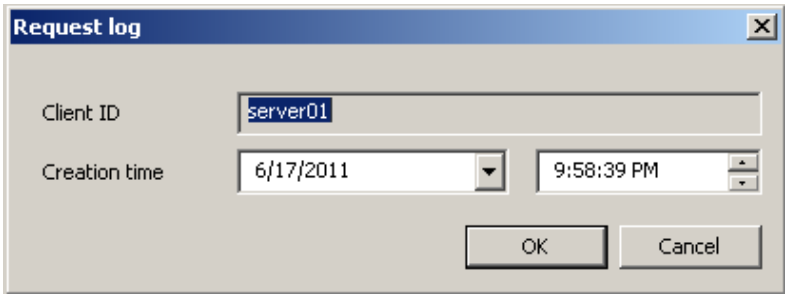

Рисунок 127

Get packages… – вызывает окно запроса каталога, в который будут сохранены инициализационные дистрибутивы для управляемого vpn-устройства

Enable – включает механизм обмена данными с клиентом

Disable – выключает механизм обмена данными с клиентом

Clear – удаляет все неприменённые обновления для клиента (предназначено для отмены неудачных обновлений)

Remove – удаляет информацию о клиенте с Сервера обновления.

Меню Tools

Меню Tools содержит одно предложение VPN data marker (Рисунок 128):

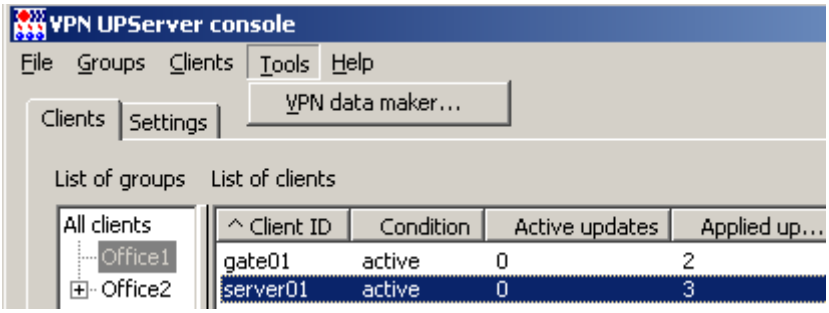

Рисунок 128

VPN data maker - вызывает одноименное окно для создания нового проекта с настройками (данными) продукта CSP VPN Agent (Рисунок 129), никак несвязанного с имеющимися клиентами в таблице, если даже выделить клиента. Созданный проект можно сохранить в файл и использовать при создании обновления для клиента (предложение Update) - в поле Product package (Рисунок 46) указать созданный файл, нажав кнопку `[…]`. Элементы окна VPN data maker:

`VPN product type` – тип CSP VPN Agent, для которого задаются данные:

`Client` – продукт CSP VPN Client 3.1

`Gate` – продукт CSP VPN Gate 3.1

`Server` – продукт CSP VPN Server 3.1

`Crypto provider type` – тип криптопровайдера, используемого продуктом CSP VPN Agent:

`CryptoPro` – КриптоПро

`SignalCOM` – СигналКом

Вкладки предназначены для создания настроек продукта CSP VPN Agent:

`LSP` – вкладка для задания локальной политики безопасности продукта CSP VPN Agent, предписанной управляемому vpn-устройству (Рисунок 129).

LSP format is cisco-like – установка этого флажка говорит о том, что локальная политика безопасности задана в формате cisco-like

Load from file… - вызывает окно для загрузки LSP из файла

Check LSP – запускает процесс проверки синтаксиса LSP. В этой версии продукта проверка синтаксиса LSP в виде cisco-like формата не производится.

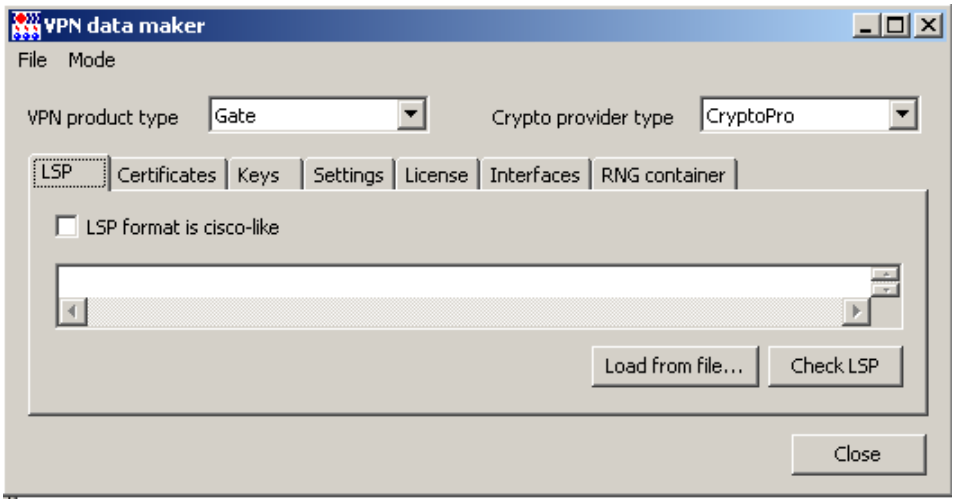

Рисунок 129

`Certificates` – вкладка для задания CA, локальных, партнерских сертификатов и списков отозванных сертификатов для продукта CSP VPN Agent (Рисунок 130).

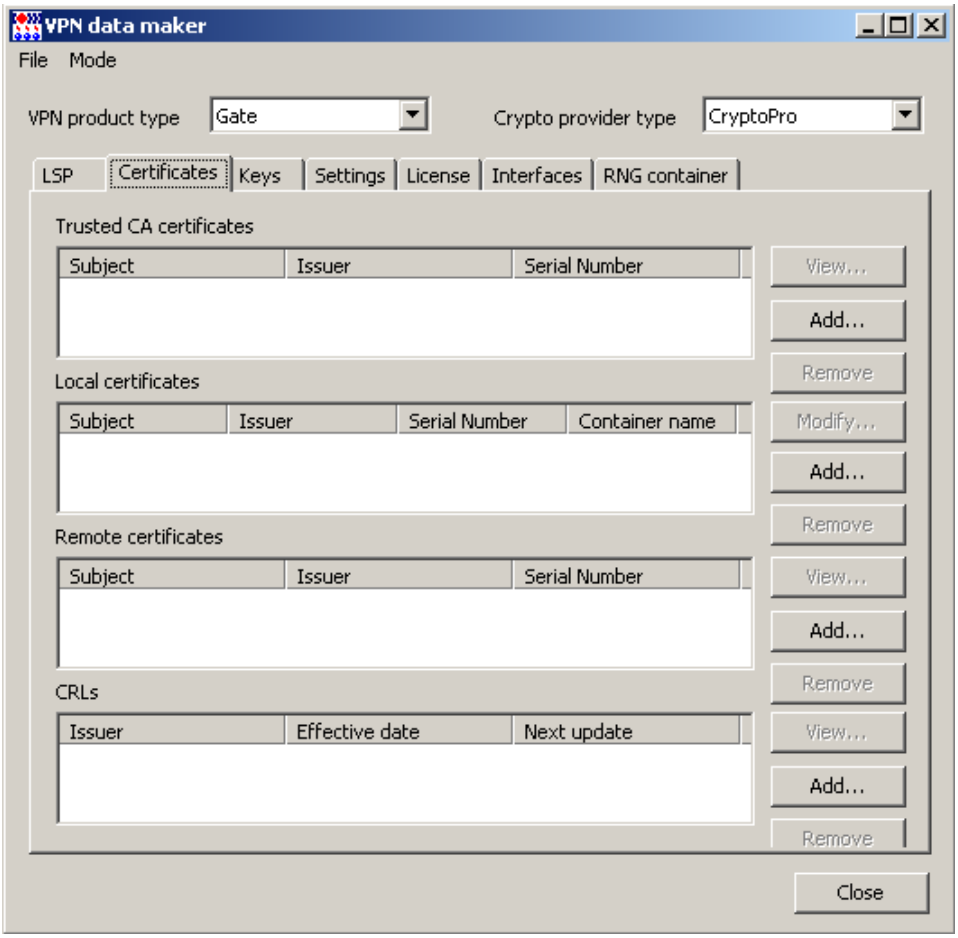

Рисунок 130

`Keys` – вкладка для задания предопределенных ключей продукта CSP VPN Agent для работы с партнерами (Рисунок 131).

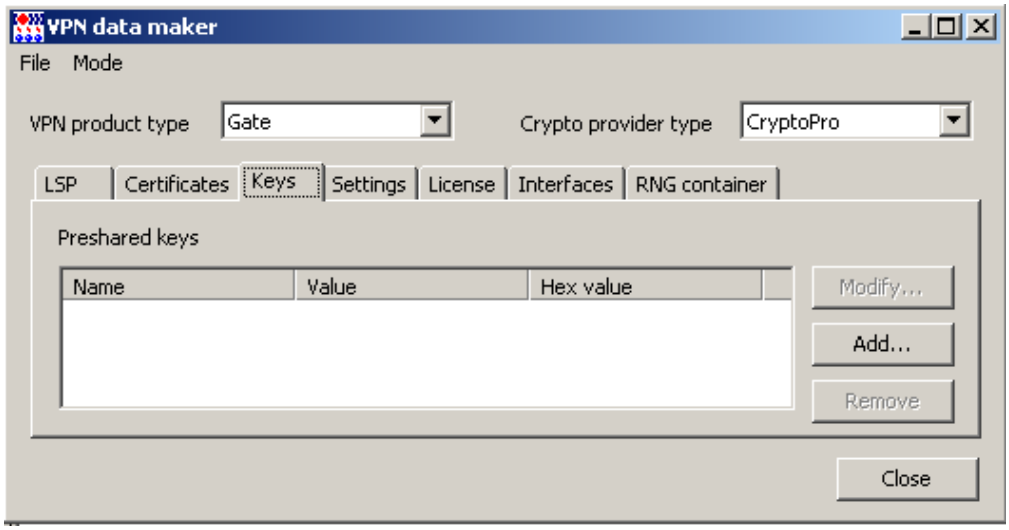

Рисунок 131

`Settings` – вкладка для задания локальных настроек продукта CSP VPN Agent (Рисунок 132).

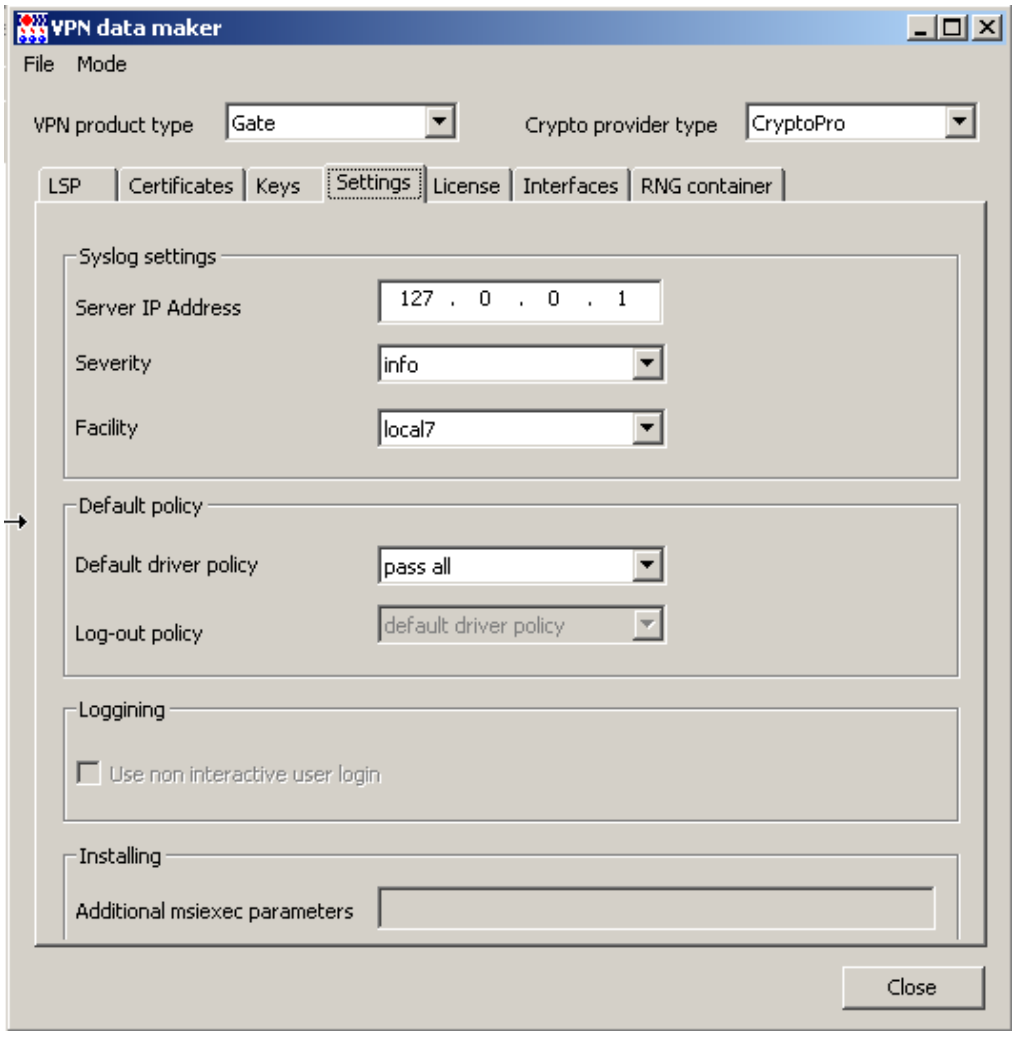

Рисунок 132

`License` – вкладка для ввода данных лицензии на продукт CSP VPN Agent.

`Interfaces` – вкладка для задания настроек сетевых интерфейсов продукта CSP VPN Server/CSP VPN Gate (Рисунок 133).

`Network interfaces` – установка этого флажка позволяет добавлять, модифицировать и удалять логические и физические имена сетевых интерфейсов

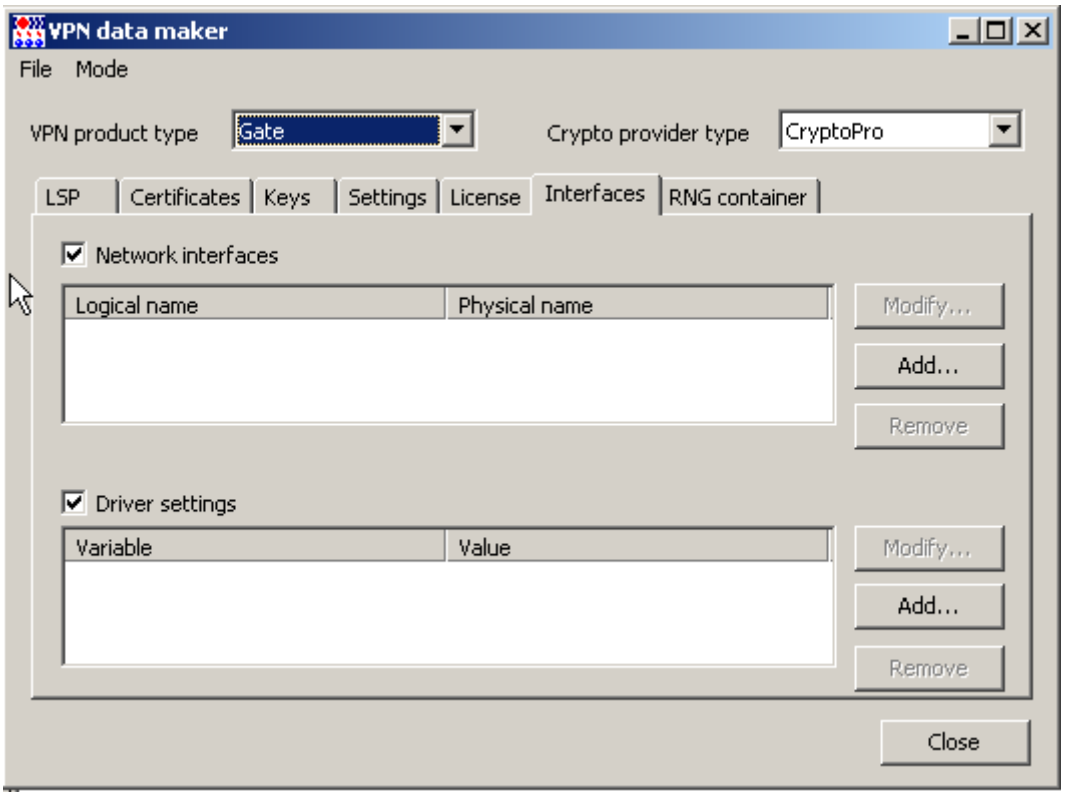

Рисунок 133

`Driver settings` – установка этого флажка позволяет изменить настройки IPsec драйвера, установленные по умолчанию (Рисунок 134). Эти настройки имеются только у продукта CSP VPN Gate и в командной строке изменяются при помощи утилиты drv_mgr. Поэтому см. описание настроек в описании утилиты drv_mgr в документе «Специализированные команды», входящем в состав «Руководства администратора Программный комплекс CSP VPN Gate».

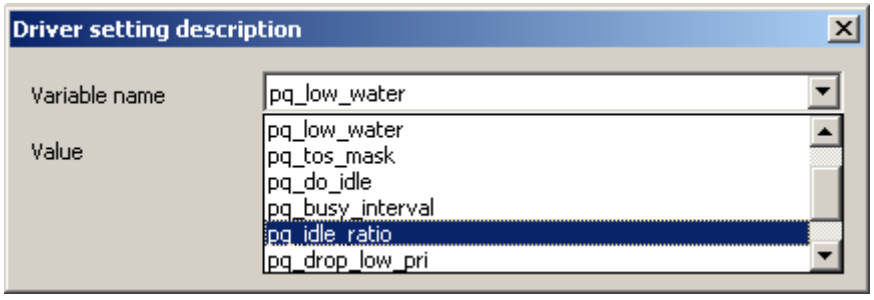

Рисунок 134

`RNG container` – вкладка задания местоположения криптографического (RNG) контейнера, содержащего инициализационные данные для датчика случайных чисел (ДСЧ). RNG контейнер представляет собой каталог, поэтому имя контейнера – имя каталога (Рисунок 135). Используется только для криптопровайдера SignalCOM.

При создании дистрибутива продукта `CSP VPN Client/CSP VPN Server` надо указать имя каталога для нового контейнера, если указанного каталога нет - он будет создан. При создании обновления для этих продуктов указывается уже существующий RNG контейнер. Для продукта CSP VPN Gate процедура инициализации выполняется только один раз, поэтому в этой вкладке указывается уже существующий RNG контейнер, как при создании дистрибутива, так и при создании обновления.

В этой вкладке может использоваться подстановка %INSTALLDIR%, которая означает каталог, в который установлен CSP VPN Agent. Значения по умолчанию – каталоги CSP VPN Client, CSP VPN Server, CSP VPN Gate.

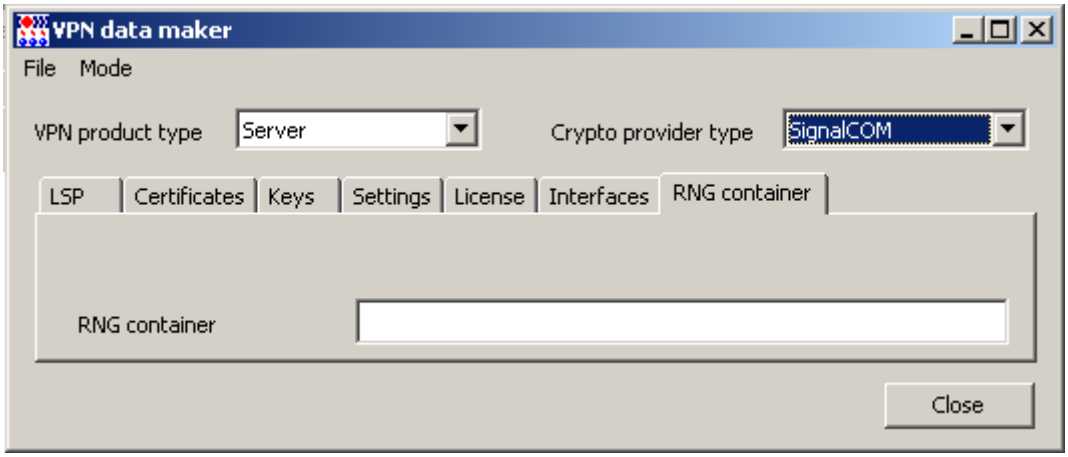

Рисунок 135

Меню File окна VPN data maker

Меню ***File*** окна VPN data maker содержит два предложения:

`Load` – загружает данные из файла данных продукта CSP VPN Agent

`Save as` – сохраняет данные продукта CSP VPN Agent в файл, отраженные во вкладках окна VPN data maker

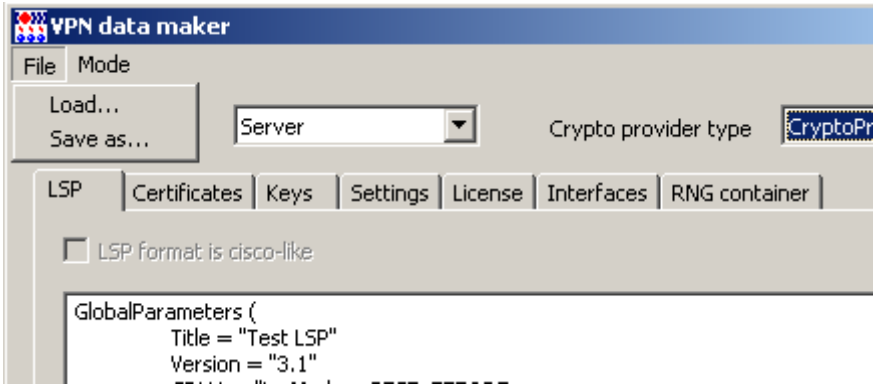

Рисунок 136

Меню Mode окна VPN data maker

Меню ***Mode*** окна VPN data maker содержит два предложения (Рисунок 137):

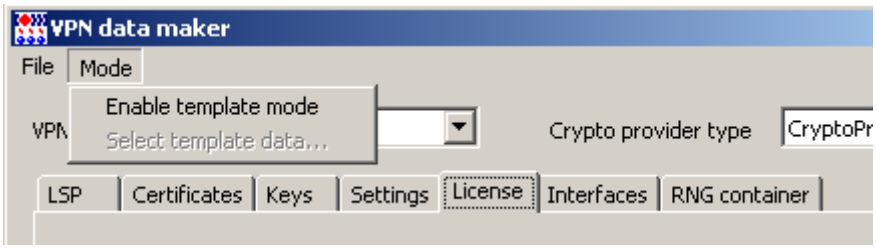

Рисунок 137

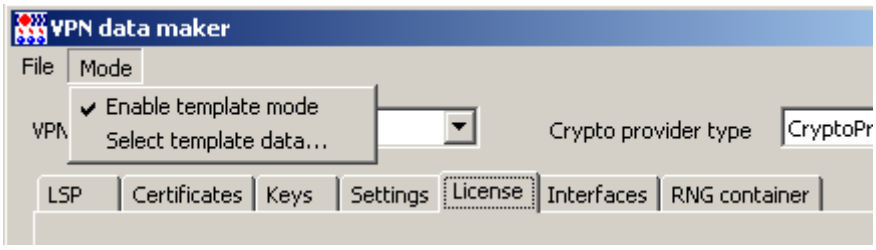

Рисунок 138

`Enable template mode` – при выборе этого предложения окно VPN data maker переходит в режим создания ***шаблона проекта***

`Select template data` – это предложение становится доступным только в режиме шаблона проекта и при его выборе открывается окно со списком данных, которые могут входить в шаблон проекта (Рисунок 139).

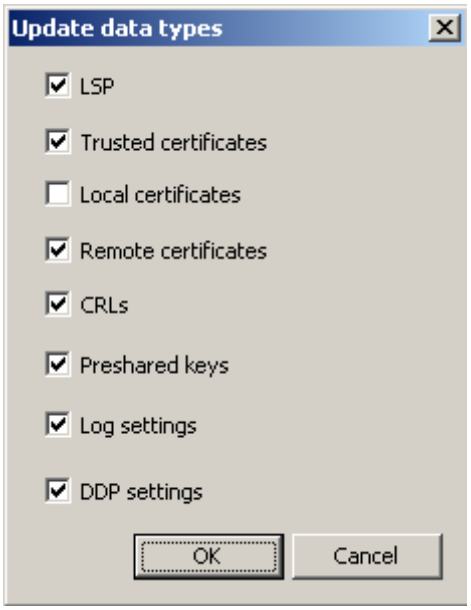

Рисунок 139

В окне Update data types флажком помечаются данные, которые будут входить в шаблон проекта. При применении обновления, созданного с использованием шаблона, только входящие в него данные будут изменяться на клиенте. Состав окна:

LSP – при установке флажка локальная политика безопасности, указанная во вкладке LSP, будет входить в состав шаблона проекта

Trusted certificates – при установке флажка все доверенные CA-сертификаты, указанные во вкладке Certificates, будут входить в шаблон проекта

Local certificates – при установке флажка все локальные сертификаты, указанные во вкладке Cerificates в разделе Local certificates, будут входить в шаблон проекта

Remote certificate – при установке флажка все сертификаты партнеров, указанные во вкладке Cerificates в разделе Remote certificates, будут входить в шаблон проекта

CRLs – при установке флажка все списки отозванных сертификатов, указанные во вкладке Cerificates в разделе CRLs, будут входить в шаблон проекта

Preshared keys – при установке флажка все предопределенные ключи, указанные во вкладке Keys, будут входить в состав шаблона проекта

Log settings – при установке флажка настройки протоколирования, указанные во вкладке Settings, будут входить в шаблон проекта

DDP settings - при установке флажка политика DDP, указанная во вкладке Settings, будет входить в шаблон проекта.

Выбрав данные, которые будут входить в шаблон, и заполнив вкладки для этих данных, сохраните созданный шаблон в файл, используя предложение Save as меню File.

Меню Help

Меню Helps содержит одно предложение About VPN UPServer console, по которому выводится окно с версией Сервера обновления (Рисунок 140):

Рисунок 140

Настройки Сервера обновления

Настройки Сервера обновления содержатся в реестре и в файле, расположение которого зависит от операционной системы:

`C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

или `C:\ProgramData\UPServer\ssettings.txt` (начиная с ОС Vista)

.

Администратор Сервера обновления может задавать следующие настройки.

Режим работы создаваемых Клиентов обновления

Задается через ключ реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UPServer`

Переменная `ClientMode`

Значение:

- `windowless` – безоконный режим работы ***Клиента обновления*** (значение по умолчанию);
- `<пустая строка>` – оконный режим работы ***Клиента обновления*** (для отладки и тестирования).

Режим запроса подтверждения у пользователя о начале обновления, устанавливаемый в пакете Клиента обновления

Задается через ключ реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UPServer`

Переменная `ClientUserAskMode`

Значение:

- `auto` – необходимость запроса определяется на основе типа VPN-продукта (подтверждение запрашивается, если на компьютере установлен продукт CSP VPN Client);
- `never` – подтверждение никогда не запрашивается, несмотря на тип VPN-продукта;
- `always` – подтверждение запрашивается всегда, несмотря на тип VPN-продукта.

Если переменная содержит другое значение, то оно трактуется как `auto`.

Сетевой адрес для взаимодействия с сервисом продукта FileZilla Server

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[FtpServer]`

Переменная `Address`

Значение: локальный IP-адрес сервера FileZilla Server (значение по умолчанию 127.0.0.1).

Сетевой порт для взаимодействия с сервисом продукта FileZilla Server

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[FtpServer]`

Переменная `Port`

Значение: порт сервиса FileZilla Server (значение по умолчанию 14147).

Пароль для взаимодействия с сервисом продукта FileZilla Server

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[FtpServer]`

Переменная `Password`

Значение: строка, представляющая из себя пароль сервиса FileZilla Server (значение по умолчанию <ПУСТАЯ СТРОКА>).

Размер файла протоколирования

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[Log]`

Переменная `FileMaxSize`

Значение: максимальный размер файла протоколирования в килобайтах (`C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log`). Минимальное значение 10. Если переменная отсутствует или некорректна – используется значение по умолчанию - 10200 килобайт.

При достижении заданного значения, данные копируются в файл `в upserver.log.bak`, а файл `upserver.log` очищается.

Пример файла протоколирования:

```
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44 Log file name:
C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44 Log setting FileMaxSize:
5120
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44 Log setting SyslogEnable:
false
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44 Log setting SyslogSrvAddr:
127.0.0.1
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44 Log setting
SyslogFacility: log_local7
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44 Settings is read from file
C:\Documents and Settings\All Users\Application
Data\UPServer\ssettings.txt
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44 UPSRV:WorkThreadCount: 2
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44
UPSRV:MaxCountOfStorableUpdates: 0
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44 UPSRV:DoNotCreateWorkCert:
false
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44
UPSRV:DoNotClearOldPasswords: false
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44 ClientInfo:MaxVPNLogSize:
256 KB
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44 ClientInfo:MaxFTPLogSize:
51200 KB
Fri May 13 20:57:26 2011 INFO    upsrv 00001c44
ClientInfo:FTPLogReadPeriod: 5 min
Fri May 13 20:57:26 2011 NOTICE  upsrv 00001c44 Module 1.2.11603 is
started
Fri May 13 20:57:36 2011 INFO    upcns 00001cc4 Log file name:
C:\Documents and Settings\All Users\Application Data\UPServer\upserver.log
```

```
Fri May 13 20:57:36 2011 INFO    upcns 00001cc4 Log setting FileMaxSize:
5120
Fri May 13 20:57:36 2011 INFO    upcns 00001cc4 Log setting SyslogEnable:
false
Fri May 13 20:57:36 2011 INFO    upcns 00001cc4 Log setting SyslogSrvAddr:
127.0.0.1
Fri May 13 20:57:36 2011 INFO    upcns 00001cc4 Log setting
SyslogFacility: log_local7
Fri May 13 20:57:36 2011 INFO    upcns 00001cc4 Settings is read from file
C:\Documents and Settings\All Users\Application
Data\UPServer\ssettings.txt
Fri May 13 20:57:36 2011 INFO    upcns 00001cc4
Notifications:MaxNoActiveTime: 24 hours
Fri May 13 20:57:36 2011 INFO    upcns 00001cc4
Notifications:MinCertificateFireTime: 30 days
Fri May 13 20:57:36 2011 NOTICE  upcns 00001cc4 Module 1.2.11603 is
started
Fri May 13 21:07:05 2011 NOTICE  upcns 00001cc4 CA certificate is created
(Hash SHA1: 69f11c5ccd557693728478b10ba15ceb567421f4)
Fri May 13 21:10:19 2011 NOTICE  upcns 00001cc4 Work certificate is
created (Hash SHA1: d268140c96cba27b793ea339c50d580c988b2bcf)
```

Флаг включения syslog протоколирования

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[Log]`

Переменная `SyslogEnable`

Значение: `true` - включено протоколирование, `false` - выключено (значение по умолчанию – `false`).

Адрес Syslog-сервера

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[Log]`

Переменная `SyslogSrvAddr`

Значение: любой корректный IP-адрес (значение по умолчанию – 127.0.0.1)

Адрес Syslog-facility (адрес источника сообщений)

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[Log]`

Переменная `SyslogFacility`

Значение: строка (значение по умолчанию – `log_local7`)

Количество рабочих ниток в сервисе подготовки обновлений

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[UPSRV]`

Переменная `WorkThreadCount`

Значение: десятичное число от 1 до 10 (значение по умолчанию 2). Рекомендуемое значение - количество процессоров на компьютере + 1.

Максимальное количество хранимых примененных обновлений для каждого клиента

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[UPSRV]`

Переменная `MaxCountOfStorableUpdates`

Значение: десятичное число от 0 до 4294967295, значение 0 – обновления не удаляются (значение по умолчанию 0).

Флаг отключения автоматического пересоздания рабочего сертификата

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[UPSRV]`

Переменная `DoNotCreateWorkCert`

Значение: `false` – отключено автоматическое пересоздание, `true` – включено автоматическое пересоздание (значение по умолчанию `false`).

Флаг удаления старых паролей к клиентским ключевым контейнерам

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[UPSRV]`

Переменная `DoNotClearOldPassword`

Значение: `false` – удаляются автоматически старые пароли, `true` – не удаляются автоматически старые пароли (значение по умолчанию `false`).

Максимальный размер данных лог сообщений VPN-продукта, хранящихся для каждого Клиента обновления

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[ClientInfo]`

Переменная `MaxVPNLogSize`

Значение: десятичное число от 1 до 102400 килобайт (значение по умолчанию 256).

Максимальный размер данных лог сообщений FTP-сервера

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[ClientInfo]`

Переменная `MaxFTPLogSize`

Значение: десятичное число от 1024 до 921600 килобайт (значение по умолчанию 51200).

Период анализа сообщений FTP-сервера

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[ClientInfo]`

Переменная `FTPLogReadPeriod`

Значение: десятичное число от 1 до 60 минут (значение по умолчанию 5).

Максимальное время неактивности клиента

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[Notifications]`

Переменная `MaxNoActiveTime`

Значение: десятичное число от 0 до 4294967295 часов, значение 0 – отключает отслеживание максимального времени неактивности клиентов (значение по умолчанию 24).

Минимальное время перед окончанием срока действия сертификата vpn-устройства клиента

Задается в файле `C:\Documents and Settings\All Users\Application Data\UPServer\ssettings.txt`

Секция `[Notifications]`

Переменная `MinCertificateFireTime`

Значение: десятичное число от 0 до 4294967295 суток, значение 0 – отключает отслеживание минимального времени перед окончанием срока действия сертификатов vpn-устройства клиентов (значение по умолчанию 30).

Настройки Клиента обновления

Настройки Клиента обновления по умолчанию содержатся в файле, расположение которого зависит от операционной системы:

`C:\Documents and Settings\All Users\Application Data\UPServer\csettings.txt`

или `C:\ProgramData\UPServer\csettings.txt` (начиная с ОС Vista).

Эти настройки можно изменить, описание настроек и возможных значений представлено ниже.

Размер файла протоколирования событий

Секция `[Log]`

Переменная `FileMaxSize`

Значение: максимальный размер файла протоколирования в килобайтах

(для ОС Windows - `C:\Program Files\UPAgent\upagent.log`,

для ОС Unix – `/var/log/upagent/upagent.log`).

Минимальное значение - 10. Если строка отсутствует или некорректна – используется значение по умолчанию - 5120 килобайт.

При достижении заданного значения данные копируются в файл `upagent.log.bak`, а файл `upagent.log` очищается.

Флаг включения syslog протоколирования

Секция `[Log]` Переменная `SyslogEnable`

Значение: `true` - включено протоколирование, `false` - выключено (значение по умолчанию – `false`).

Адрес Syslog-сервера

Секция `[Log]`

Переменная `SyslogSrvAddr`

Значение: любой корректный IP-адрес (значение по умолчанию – 127.0.0.1)

Адрес Syslog-facility (адрес источника сообщений)

Секция `[Log]`

Переменная `SyslogFacility`

Значение: строка (значение по умолчанию – `log_local7`)

Период проверки новых обновлений на Сервере обновления

Секция `[Update]`

Переменная `CheckingPeriod`

Значение: от 60 до 86400 секунд (значение по умолчанию 3600).

Ограничение скорости скачивания обновлений с Сервера обновления

Секция [FTPServer]

Переменная SpeedLimit

Значение: от 512 до 4294967295 байт/секунду или 0 (0 – ограничения нет, значение по умолчанию).

Максимальное количество попыток скачать/получить данные с/на FTP сервер(а)

Секция `[FTPServer]`

Переменная `MaxTryCount`

Значение: десятичное число от 1 до 10 (значение по умолчанию 3).

Период между попытками скачать/получить данные с/на FTP сервер(а)

Секция `[FTPServer]`

Переменная `TryPeriod`

Значение: десятичное число от 0 до 300 секунд (значение по умолчанию 120).

Максимальное время отсутствия трафика между Клиентом обновления и FTP-сервером, по истечении которого считается, что соединение разорвано

Секция `[FTPServer]`

Переменная `MaxTrafficTimeout`

Значение: десятичное число от 30 до 3600 секунд (значение по умолчанию 180).

Адреса FTP сервера

Секция `[FTPServer]`

Переменная `AddressX`, где X любое десятичное число (0,1,2..)

Количество таких переменных может быть больше одного, они будут использоваться в том порядке, в котором заданы. Числа должны быть уникальные в пределах секции.

Значение: IP-адрес или DNS-имя, которое будет транслироваться в IP-адрес в момент создания соединения.

Максимальный размер сообщений продукта CSP VPN Agent, пересылаемых на Сервер обновления

Секция `[Info]`

Переменная `MaxVPNLogSize`

Значение: десятичное число от 1 до 102400 килобайт (значение по умолчанию 16).

Режим работы Клиента обновления

Задается через ключ реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UPAgent`

Переменная `Mode`

Значение:

- windowless – безоконный режим работы Клиента обновления (значение по умолчанию);
- <пустая строка> – оконный режим работы Клиента обновления (для отладки и тестирования).

Режим запроса подтверждения у пользователя о начале обновления

Задается через ключ реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UPAgent`

Переменная `UserAskMode`

Значение:

- `auto` – необходимость запроса определяется на основе типа VPN-продукта (подтверждение запрашивается, если на компьютере установлен продукт CSP VPN Client) (значение по умолчанию)
- `never` – подтверждение никогда не запрашивается, не смотря на тип VPN-продукта
- `always` – подтверждение запрашивается всегда, не смотря на тип VPN-продукта.

Если переменная содержит другое значение, то оно трактуется как `auto`.

Создание обновлений с помощью командной строки

Для автоматизации процесса управления клиентами удобно использовать интерфейс командной строки. Для этого в состав продукта ***VPN UPServer*** входит командно-строчная утилита `upmgr.exe`. Она размещена в каталоге продукта – `C:\Program Files\UPServer\upmgr.exe`.

При успешном завершении команды - код возврата равен 0, а при неуспешном - отличен от 0.

Команды утилиты `upmgr.exe`:

```
upmgr show [-i CLIENT_ID [-s SECTION_NAME]]

upmgr create -i CLIENT_ID -p PRODUCT_PKG [-g CLIENT_GROUP] [-a AGENT_PKG] [-s AGENT_SETTINGS]

upmgr remove -i CLIENT_ID

upmgr get -i CLIENT_ID -d PRODUCT_DIR

upmgr update -i CLIENT_ID [-p[d] PRODUCT_PKG] [-a AGENT_PKG] [-s AGENT_SETTINGS] [-e EXTENDED_DATA] [-date CREATION_DATE] [-time CREATION_TIME]

upmgr clear -i CLIENT_ID

upmgr disable -i CLIENT_ID

upmgr enable -i CLIENT_ID

upmgr set_group -g CLIENT_GROUP {-i CLIENT_ID|-go OLD_CLIENT_GROUP}

upmgr show_cert

upmgr renew_cert [-expired_only]
```

где:

`CLIENT_ID`	уникальный идентификатор клиента, может состоять из любых символов, за исключением следующих: \?/:">*<|, не должен начинаться или заканчиваться символами пробел, табуляция или точка, и не должен быть равен “NUL” или “CON” или “COMx”, где x [0..9];
`SECTION_NAME`	имя секции данных о клиенте. `Например, ”---VPN PRODUCT----”, ”---LSP---”, ”---LICENSE---” и т.п.`
`PRODUCT_PKG`	имя файла, содержащего VPN данные, который был создан с помощью окна консоли управления VPN data maker, или имя файла дистрибутива продукта CSP VPN Server/CSP VPN Client, который был создан с помощью продукта CSP VPN Server/Client AdminTool
`CLIENT_GROUP`	имя группы, к которой принадлежит клиент (формат SUB1/SUB2/NAME);
`AGENT_PKG`	каталог, в котором размещен дистрибутив Клиента обновления (указывается, если получена новая версия Клиента обновления от разработчика, текущая версия размещена в каталоге upagent);
`AGENT_SETTINGS`	имя файла, содержащего настройки Клиента обновления;

PRODUCT_DIR	каталог, в который будут сохранены дистрибутивы для Клиента обновления;
EXTENDED_DATA	каталог, в котором расположены расширенные данные и скрипты обновления;
CREATION_DATE	формат: dd/mm/yy
CREATION_TIME	формат: hh:mm. Дата и время, когда Сервер обновления сформирует пакет обновления и сделает его доступным для скачивания Клиентом обновления. Если указанное время уже прошло, то пакет обновления будет сформирован и открыт для скачивания Клиентом обновления сразу после создания обновления (если параметры не указаны, то используются текущая дата и время);
OLD_CLIENT_GROUP	имя группы, которая должна быть заменена на CLIENT_GROUP (формат PARENT0/PARENT1[/NAME][*]);
-expired_only	рабочий сертификат Сервера обновления пересоздается, если у него истек срок действия.

Команда ***show*** выводит информацию, аналогичную таблице клиентов (Рисунок 24). Если не указывать ключ -i – краткая информация обо всех клиентах, при указании ключа -i - выводится расширенная информация для указанного клиента.

```
upmgr show [-i CLIENT_ID]
```

```
upmgr.exe show
00000001      active  0     3     enabled 14/05/2012 00:21:38     16/05/20
11 18:20:49     40.0.0.101      none
```

Команда ***create*** позволяет создать нового клиента на Сервере обновления.

```
upmgr create -i CLIENT_ID -p PRODUCT_PKG [-a AGENT_PKG]
[-s AGENT_SETTINGS]
```

Создание нового клиента с идентификатором "00000002" и с именем дистрибутива продукта CSP VPN Server "e:\share\test_pkg.exe":

```
upmgr.exe create -i 0000002 -p e:\share\test_pkg.exe
```

Команда ***remove*** позволяет удалить клиента из таблицы клиентов на Сервере обновления.

```
upmgr remove -i CLIENT_ID
```

Удаление клиента с идентификатором "00000002":

```
upmgr.exe remove -i 0000002
```

Команда ***get*** позволяет получить инициализационные дистрибутивы для управляемого vpn-устройства в указанный каталог.

```
upmgr get -i CLIENT_ID -d PRODUCT_DIR
```

Получение дистрибутивов для клиента с идентификатором "00000002" и с записью их в каталог "e:\share\#init\00000002":

```
upmgr.exe get -i 0000002 -d e:\share\#init\00000002
```

Команда ***update*** позволяет создать обновление на Сервере обновления для клиента.

```
upmgr update -i CLIENT_ID [-p[d] PRODUCT_PKG] [-a AGENT_PKG]
[-s AGENT_SETTINGS] [-e EXTENDED_DATA] [-date CREATION_DATE] [-time
CREATION_TIME]
```

Создание для клиента с идентификатором "00000002" обновления данных продукта CSP VPN Agent, находящихся в дистрибутиве этого продукта "e:\share\test_pkg.exe":

```
upmgr.exe update -i 0000002 -p e:\share\test_pkg.exe
```

Если вместо ключа -p указать ключ -pd, то Клиенту обновления будут пересылаться только данные, без бинарных кодов продукта CSP VPN Agent.

Команда ***clear*** позволяет отменить все неприменённые обновления для клиента.

```
upmgr clear -i CLIENT_ID
```

Удаление всех неприменённых обновлений для клиента с идентификатором "00000002":

```
upmgr.exe clear -i 0000002
```

Команда ***disable*** блокирует все сетевые обмены Сервера обновления с клиентом.

```
upmgr disable -i CLIENT_ID
```

Запрет всех сетевых обменов с клиентом с идентификатором "00000002":

```
upmgr.exe disable -i 0000002
```

Команда ***enable*** разрешает Серверу обновления сетевые обмены с клиентом.

```
upmgr enable -i CLIENT_ID
```

Разрешение сетевых обменов с клиентом с идентификатором "00000002":

```
upmgr.exe enable -i 0000002
```

Команда ***set_group*** изменяет группу у заданных клиентов.

```
upmgr set_group -g CLIENT_GROUP {-i CLIENT_ID|-go OLD_CLIENT_GROUP}
```

Включает клиента "00000002" в группу "Moscow/Office01":

```
upmgr.exe set_group -g Moscow/Office01 -i 00000002
```

Команда ***show_cert*** запускает стандартную GUI программу операционной системы для отображения рабочего сертификата Сервера обновления.

```
upmgr show_cert
```

Показать рабочий сертификат Сервера обновления:

```
upmgr.exe show_cert
```

Команда ***renew_cert*** запускает перевыпуск рабочего сертификата Сервера обновления (начало срока действия сертификата за день до текущей даты, время жизни сертификата 1 месяц).

```
upmgr renew_cert [-expired_only]
```

Пересоздать рабочий сертификат Сервера обновления в том случае, если у него истек срок действия:

```
upmgr.exe renew_cert -expired_only
```

