Руководство
по использованию
VDI клиента

Оглавление

1. Настройка VDI клиента

VDI клиент устанавливается в каталог /**usr**/**share**/**vdi-client**.

Для работы клиента с вашей средой виртуализации необходимо в каталог /**usr**/**share**/**vdi-client**/**pki** поместить сертификат удостоверяющего центра виртуализации. Он находится на машине управления виртуализацией по пути /**etc**/**pki**/**ovirt-engine**/**ca.pem**.

Далее настройте конфигурационный файл VDI клиента.

Синтаксис конфигурационного файла - «опция = значение». Комментарии в строке с опцией не допускаются.

Обязательные к настройке опции.

- Опция **url**. Укажите url для доступа к вашей среде виртуализации. Например:

```
url = https://redvirt-hostedengine.rs/ovirt-engine/api
```

Если DNS сервер в сети не разрешает этот адрес, укажите A запись в /**etc**/**hosts**, пример:

```
10.10.10.10 redvirt-hostedengine.rs
```

- Секция **[домены]**. Впишите имена доменов, пользователи которого будут осуществлять вход. Каждый новый домен перечисляется на новой строке с порядковым числом. Первая запись будет первой записью в списке выбора домена и не будет требовать выбора. Следующие записи будет необходимо выбирать в списке доменов. Пример:

```
[domains]
domain1 = samba.redos
domain2 = internal
```

Домен internal является доменом по умолчанию.

- Опция **ca_path** содержит путь к файлу сертификата вашей среды виртуализации. По умолчанию **/pki/ca.pem**. Это относительный путь от каталога **/usr/share/vdi-client**.

Необязательные опции:

- опция **use_spice_proxy** имеет два значения - yes и no. Она определяет, используется ли подключение к консоли виртуальных машин через Spice прокси-сервер или нет;
- опция **smartcard_slot** имеет два значения - pki и gost. Она определяет, в каком слоте на токене JaCarta искать ключевую пару логина и пароля;
- опция **pool_run_timeout** определяет время, необходимое для ожидания выделения из пула виртуальной машины и начала ее запуска. Для каждой инфраструктуры оно может быть разное и подбирается опытным путем;
- опция **logs_path** определяет абсолютный путь до каталога, в который будет сохраняться лог-файл. Лог-файл логирует только работу клиента и нужен для его отладки. Сохранять его необязательно. По этой причине он по умолчанию сохраняется в **/tmp**;
- опция **use_rdp** имеет два значения - yes и no. Она определяет протокол, используемый для подключения к консоли виртуальных машин. Значение по умолчанию - no, используется протокол SPICE. Если установлено значение yes, то для подключения к консоли виртуальной машины используется протокол RDP;
- опция **debug** имеет два значения - yes и no. Она определяет, добавляется ли в лог отладочная информация.

2. Авторизация

Авторизация в VDI клиенте возможна двумя способами.

Вы можете вручную ввести логин и пароль пользователя, выбрать домен и нажать кнопку «Войти» (Рисунок 1).

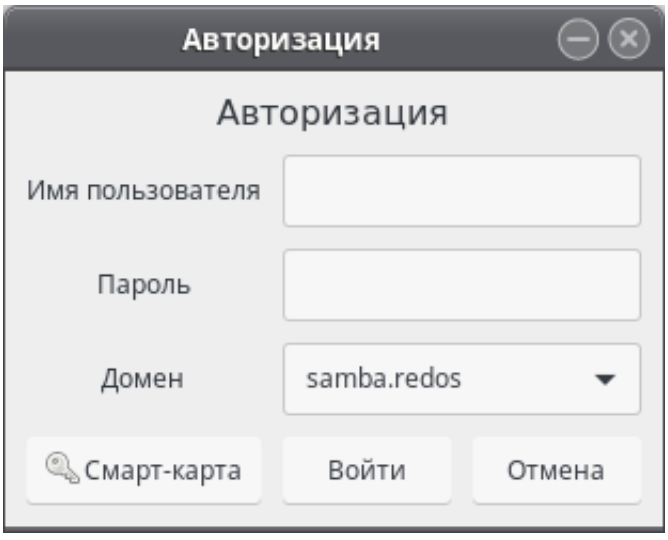

Рисунок 1 - Авторизация

Также возможно авторизоваться с помощью смарт-карты. Для этого подключите смарт-карту к компьютеру и нажмите кнопку «Смарт-карта». Выбирать имя домена из выпадающего списка не нужно, оно должно быть записано на смарт-карте. Откроется окно для ввода PIN-кода. Введите PIN-код и нажмите кнопку «Войти» (Рисунок 2). Будет произведен вход.

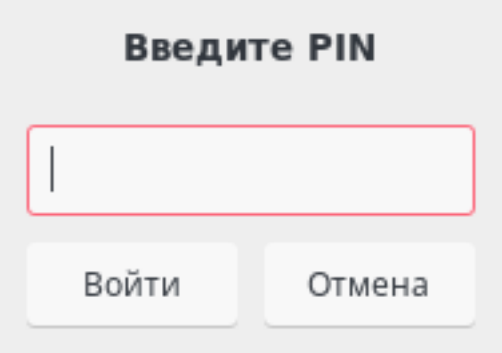

Рисунок 2 – Ввод PIN–кода

Для работы авторизации с помощью смарт-карты на клиентскую систему нужно установить библиотеку для работы со смарт-картой jcpkcs11-2_2.7.0.411_x64.rpm.

3. Работа с ВМ и пулами

После авторизации возможны два варианта.

Если вашей учетной записи делегирована только одна виртуальная машина или один пул, то после некоторого времени ожидания открывается spice-консоль.

Если виртуальная машина была выключена, она автоматически запускается.

Если виртуальная машина в пуле была не выделена, она выделится и запустится.

После запуска виртуальной машины консоль будет запущена в полноэкранном режиме и масштабирована под разрешение экрана, при условии установки гостевых дополнений и драйверов.

Если вашей учетной записи делегировано несколько виртуальных машин или пулов, то откроется окно управления (Рисунок 3).

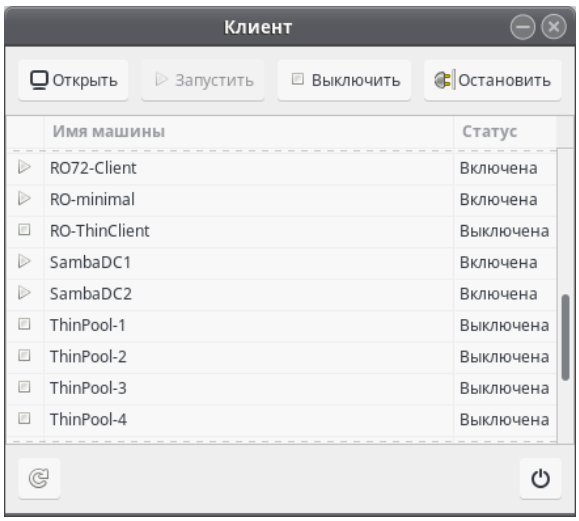

Рисунок 3 – Окно управления

Пулы отображаются вверху списка, затем идут виртуальные машины. Отличить пулы можно по статусу «Доступен».

В зависимости от выбранной виртуальной машины будут активны те или иные кнопки управления:

- при нажатии на кнопку «Открыть» открывается spice консоль виртуальной машины;
- при нажатии на кнопку «Запустить» происходит запуск виртуальной машины. Если это пул, то происходит выделение из пула виртуальной машины и ее последующий запуск;
- при нажатии на кнопку «Выключить» виртуальной машине передается сигнал выключения. Это рекомендованный способ выключения виртуальных машин;
- при нажатии на кнопку «Остановить» происходит аварийная остановка виртуальной машины. Это аналогично отключению питания на реальной машине;
- при нажатии на кнопку с иконкой круговой стрелки происходит обновление списка виртуальных машин и пулов;
- при нажатии на кнопку с иконкой выключения в правом нижнем углу VDI клиент завершает работу.

4. Работа в SPICE консоли

При работе в spice консоли можно пробрасывать USB-устройства с реальной на виртуальную машину. Для этого в консоли в верхнем меню нажмите «Файл» - «USB device selection» и выберите необходимое устройство (рис. 4).

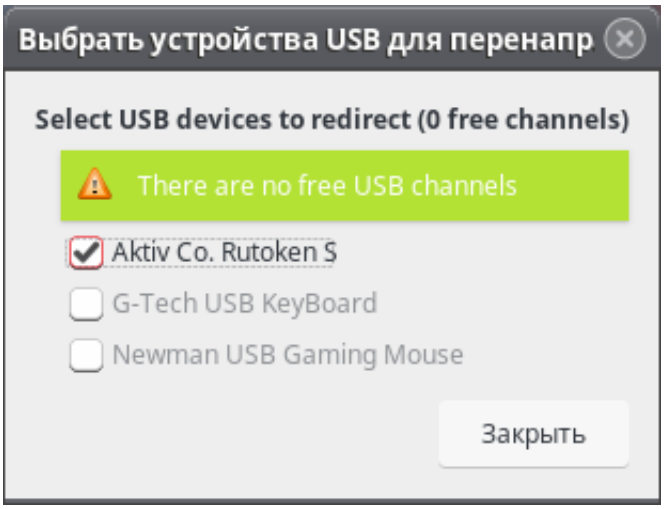

Рисунок 4 – Выбор USB устройства

Также можно выполнять сочетания клавиш, выбрав в верхнем меню «Отправить клавишу» (Рисунок 5).

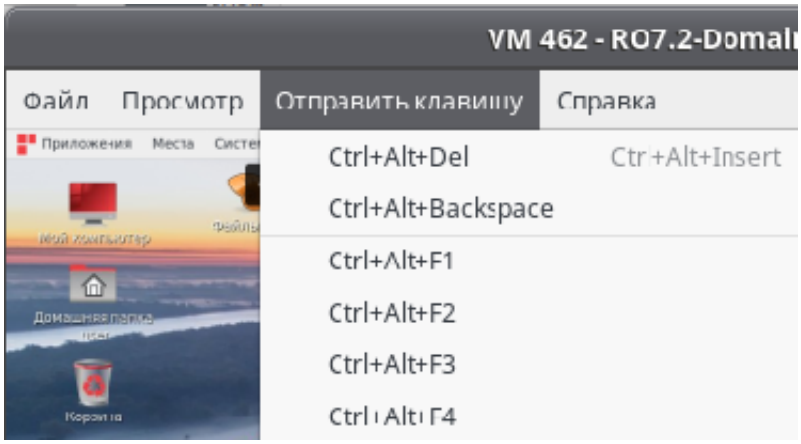

Рисунок 5 – Меню «Отправить клавишу»

Если на виртуальной машине не поддерживается автоматический захват устройств ввода, то отключить захваченные устройства можно сочетанием клавиш «Shift+F12».

В консоли spice работает двунаправленный буфер обмена между виртуальной машиной и хостовой системой.

5. Запись ключевой информации

Для записи ключевой информации на токен понадобится SecurLogon, если вы используете токены JaCarta.

Для записи ключевой информации на токен:

1. Вставьте токен в компьютер.

2. Запустите SecurLogon. При запуске понадобится ввести пароль для повышения привелегий. Нажмите кнопку «Далее» (Рисунок 6).

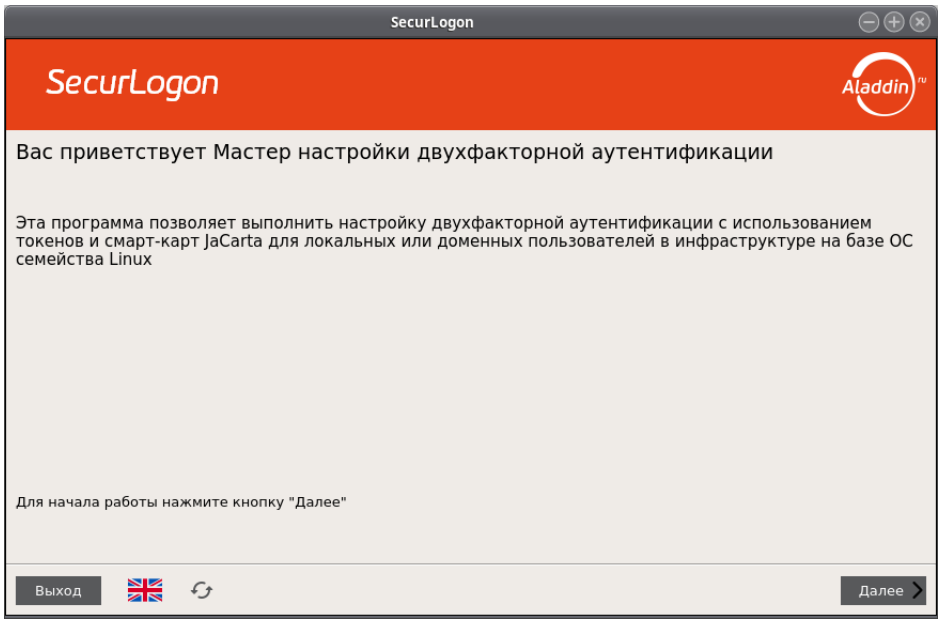

Рисунок 6 – Мастер настройки двухфакторной аутентификации

3. Выберите способ аутентификации «Сетевая» и нажмите кнопку «Далее»

(Рисунок 7).

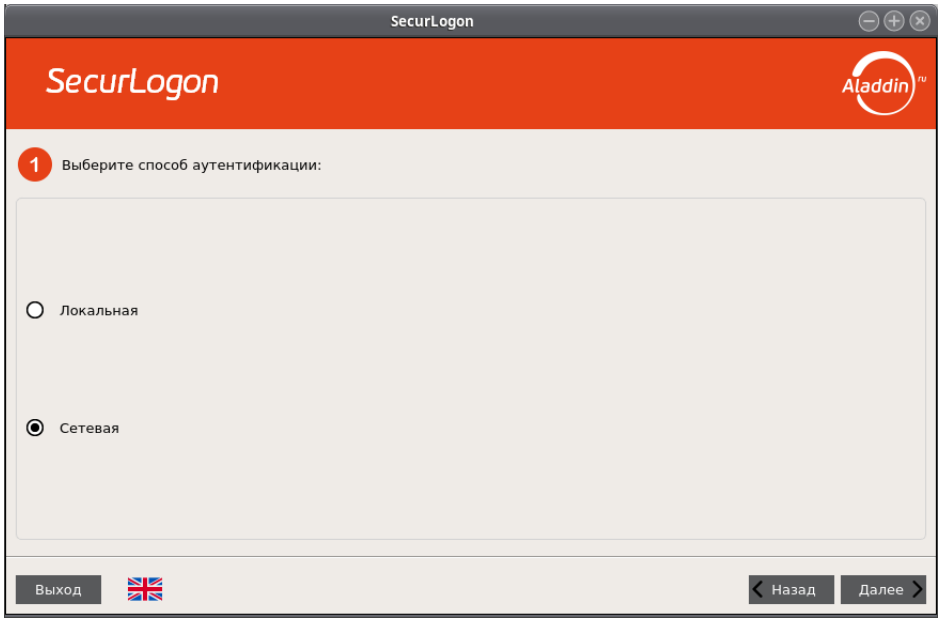

Рисунок 7 – Выбор способа аутентификации

4. Выберите тип домена в зависимости от того, какой у вас используется. Нажмите кнопку «OK» (Рисунок 8).

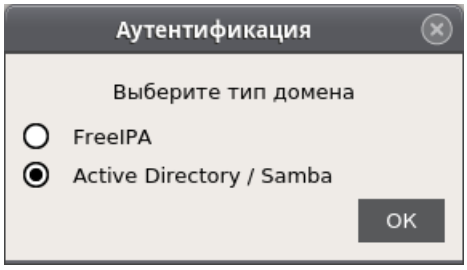

Рисунок 8 – Выбор типа домена

5. Выберите «Настроить двухфакторную аутентификацию при входе в систему» и нажмите кнопку «Далее».

6. Выберите электронный ключ (слот) для записи на него ключевой информации. Нажмите кнопку «Далее» (Рисунок 9).

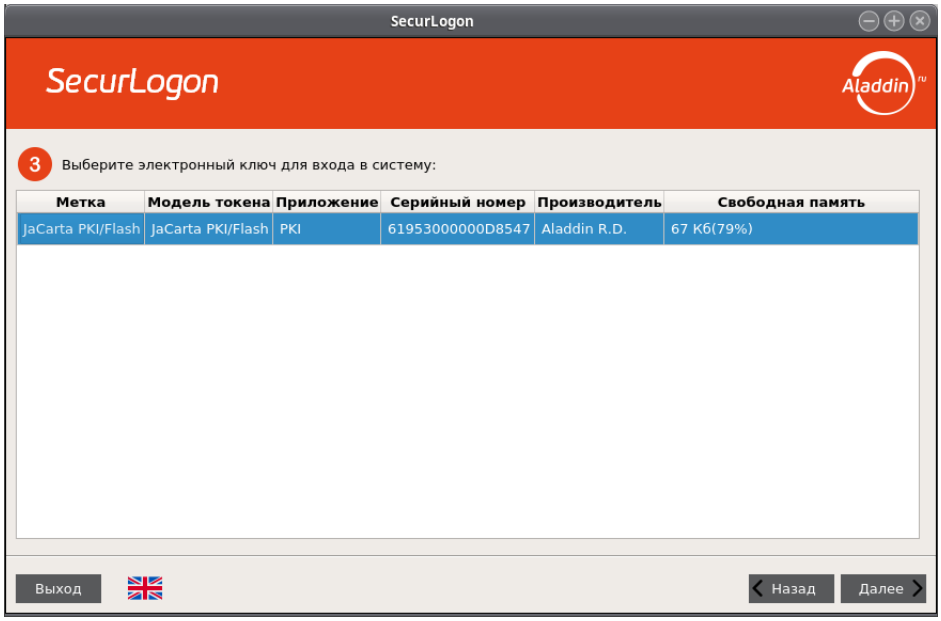

Рисунок 9 – Выбор электронного ключа

7. Выберите «Без использования PKI». Нажмите кнопку «Далее» (Рисунок 10).

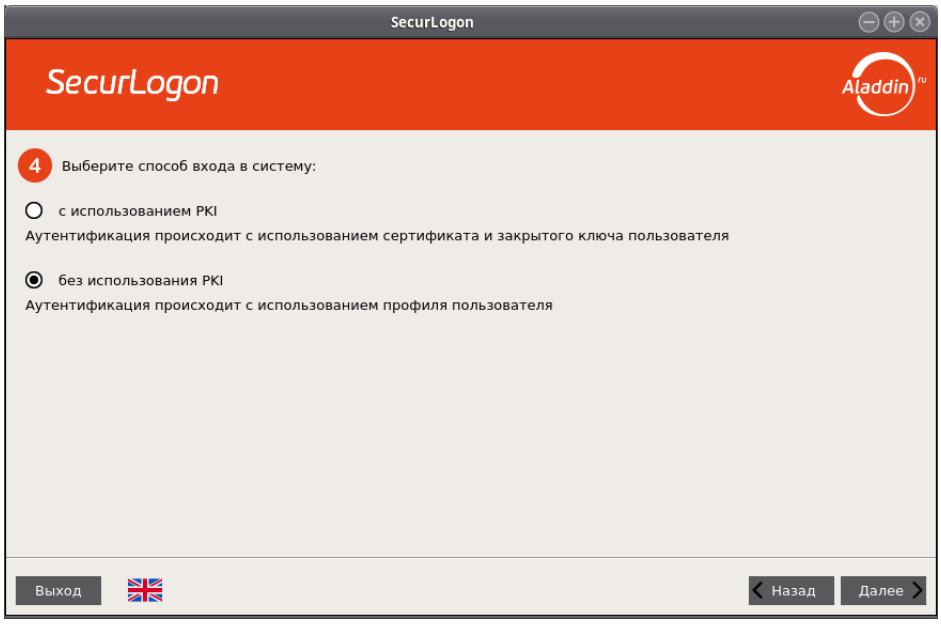

Рисунок 10 – Выбор способа входа в систему

8. Введите PIN-код пользователя и нажмите кнопку «OK» (Рисунок 11).

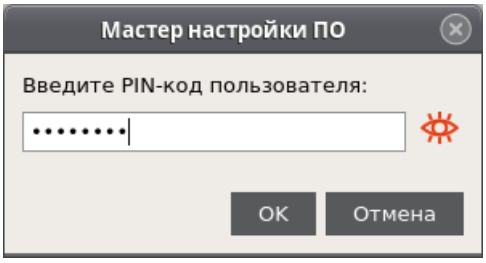

Рисунок 11 – Ввод PIN-кода пользователя

9. Нажмите на иконку токена для его форматирования. Откроется окно «Управление токеном». В нем перейдите на вкладку «Форматирование», введите PIN-код администратора и два раза PIN-код пользователя. Нажмите кнопку «Выполнить» (Рисунок 12).

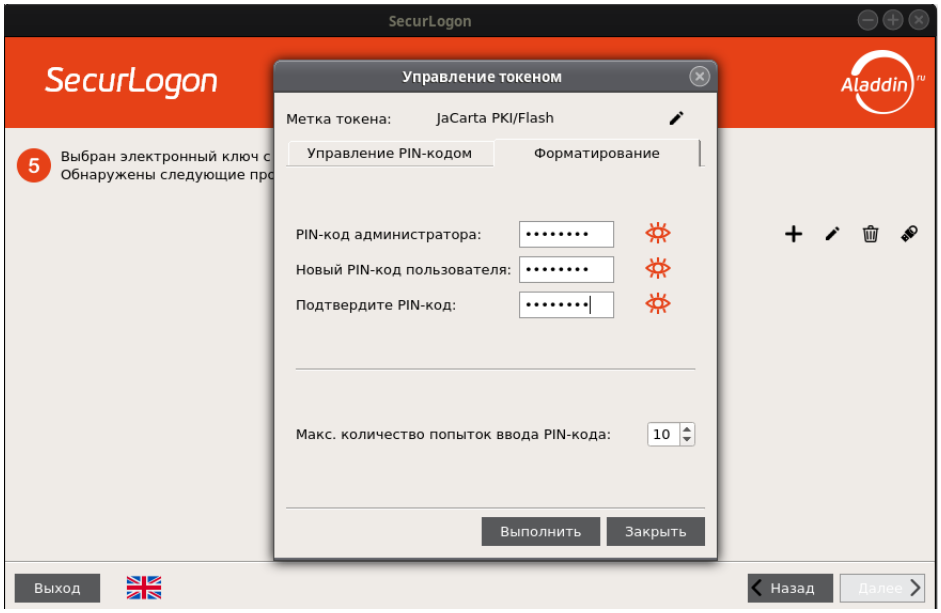

Рисунок 12 – Управление токенами

10. В информационном окне, сообщающем об успешности форматирования, нажмите «OK» (Рисунок 13).

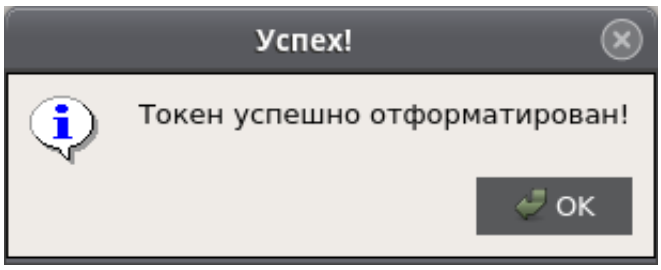

Рисунок 13 - Информационное окно

11. В основном окне программы нажмите на кнопку с иконкой плюса.

12. Введите имя пользователя, домен и пароль пользователя в соответствующие поля. Нажмите кнопку «Создать» (Рисунок 14).

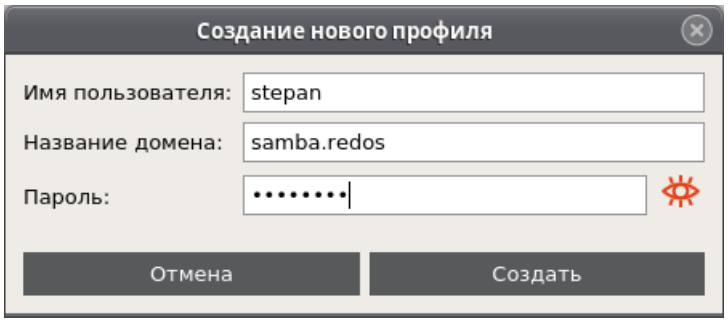

Рисунок 14 – Создание нового профиля

13. После успешного создания профиля появится соответствующее сообщение. Нажмите кнопку «OK» (Рисунок 15).

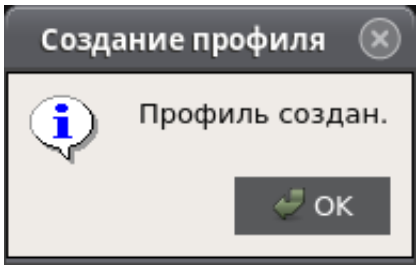

Рисунок 15 - Информационное окно

В основном окне SecurLogon могут не отображаться созданные профили, если компьютер, на котором он запущен, не введен в домен. Это нормально, ключевая информация на токен все равно записана.

На этом запись токена завершена. Можете закрыть SecurLogon.