T-FLEX PLM

РОССИЙСКИЙ ПРОГРАММНЫЙ КОМПЛЕКС

Активация и обновление ключей на ОС Linux

ТОП СИСТЕМЫ

Авторские права

Содержание

Общие сведения

В данной инструкции описана работа с ключами защиты продуктов программного комплекса T-FLEX PLM на компьютерах под управлением ОС Linux.

Команды, выполняемые в окне терминала ОС, обозначены в данном документе следующим образом:

```
Текст команды, который необходимо ввести в терминал.
```

Вместо ввода команды вручную, можно скопировать её в буфер обмена из текущего документа, а затем вставить в терминал.

После ввода текста команды в терминал нажмите **Enter** для её выполнения.

Информация об электронных ключах защиты

Для защиты продуктов комплекса T-FLEX PLM от несанкционированного использования применяются ключи защиты, созданные по технологии **Sentinel HASP**. Существует два типа ключей защиты – аппаратный и программный. Ключи обладают собственной памятью, в которой содержатся сведения о доступных пользователю лицензиях.

Ключ аппаратной защиты записан на физическое устройство, которое подключается в USB-порт компьютера.

Для защиты продуктов комплекса T-FLEX PLM используются ключи аппаратной защиты HASP серии Sentinel HL версии 4.25 и выше. Более ранние версии ключей не поддерживаются.

Ключ программной защиты не требует наличия физического устройства. Он связан с конкретным компьютером, но при необходимости может быть перенесён на другой.

Лицензии в ключах защиты могут быть сетевыми и локальными.

Локальная лицензия работает только на одном компьютере. На этом компьютере должен быть активирован ключ защиты.

Сетевая лицензия даёт право работать на нескольких компьютерах, при этом количество пользователей, работающих одновременно, не должно превышать количество купленных лицензий. При этом используется один ключ с сетевой лицензией, установленный на одном из компьютеров локальной сети.

Процедура активации ключа не зависит от типа лицензии.

Доступ к управлению лицензиями осуществляется через программу **Sentinel Admin Control Center**.

Если на компьютере доступно несколько лицензий, то используется та, у которой наивысший приоритет. Ниже перечислены лицензии в порядке уменьшения приоритета:

1. локальная лицензия ключа аппаратной защиты;
2. локальная лицензия ключа программной защиты;
3. сетевая лицензия ключа аппаратной защиты;
4. сетевая лицензия ключа программной защиты.

Установка HASP License Manager

Пользователь, выполняющий установку должен иметь права суперпользователя.

1. Сохраните следующий архив в каталоге **Загрузки** целевого компьютера:
   Prerequisites_T-FLEX_17_Linux.zip

   При отсутствии интернет-соединения на целевом компьютере загрузите архив на компьютере, имеющем доступ в Интернет, и перенесите на целевой компьютер с помощью физических носителей или локальной сети.

2. Смените рабочий каталог на **Загрузки**:

   ```
   cd ~/Загрузки
   ```

3. Распакуйте архив **Prerequisites_T-FLEX_17_Linux.zip:**

   ```
   unzip Prerequisites_T-FLEX_17_Linux.zip
   ```

4. Смените рабочий каталог на папку **aksusbd**, ранее извлечённую из архива **Prerequisites_T-FLEX_17_Linux.zip:**

   ```
   cd HASP_Linux/aksusbd/
   ```

5. Сделайте файл **aksusbd** исполняемым и установите пакет **aksusbd**:

   ```
   sudo chmod +x dinst
   sudo ./dinst
   ```

   После запуска команды система запрашивает пароль суперпользователя. Введите пароль в терминал и нажмите **Enter.**

6. Смените рабочий каталог на **HASP_Linux**:

   ```
   cd ~/Загрузки/HASP_Linux
   ```

7. Скопируйте в рабочую директорию HASP License Manager библиотеки **haspvlib_46113.so** и **haspvlib_x86_64_46113.so**:

   ```
   sudo cp haspvlib_46113.so /var/hasplm/haspvlib_46113.so

   sudo cp haspvlib_x86_64_46113.so /var/hasplm/haspvlib_x86_64_46113.so
   ```

8. Сделайте исполняемыми библиотеки, скопированные на предыдущем шаге:

   ```
   sudo chmod +x /var/hasplm/haspvlib_46113.so

   sudo chmod +x /var/hasplm/haspvlib_x86_64_46113.so
   ```

9. Перезапустите службу HASP License Manager:

   ```
   sudo systemctl restart hasplmd
   ```

Активация нового программного ключа

Для активации аппаратного ключа достаточно вставить его в компьютер и подождать, пока загорится индикатор.

Для получения нового программного ключа необходимо направить запрос в службу лицензирования компании «Топ Системы». Служба лицензирования обработает запрос и пришлёт письмо с файлом ключа. После получения файла его необходимо прикрепить к целевому компьютеру.

Процедура обновления является общей для программных и аппаратных ключей. Сначала направьте запрос обновления в службу лицензирования компании «Топ Системы». Служба лицензирования обработает запрос и пришлёт письмо с файлом обновления ключа. После получения файла его необходимо прикрепить к целевому компьютеру.

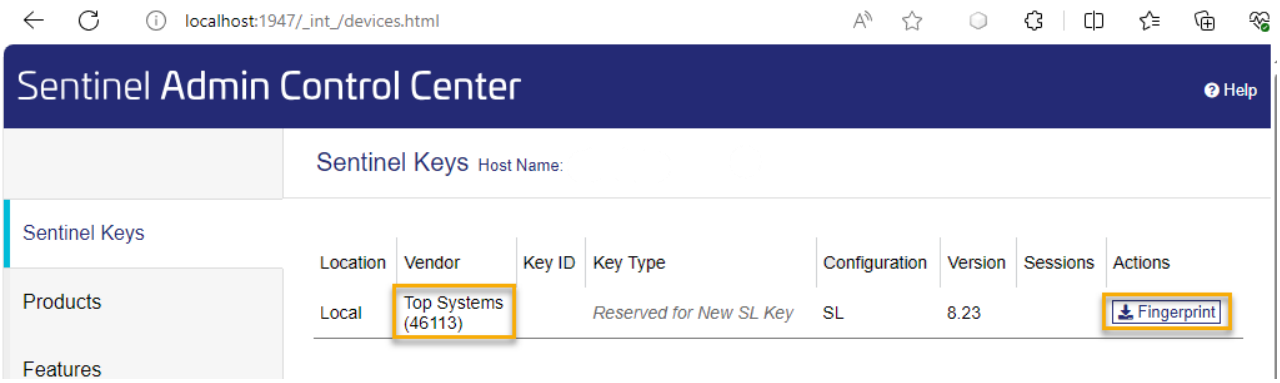
Запрос нового ключа или обновления для имеющегося ключа

1. Откройте Sentinel Admin Control Center, перейдя по ссылке http://localhost:1947.

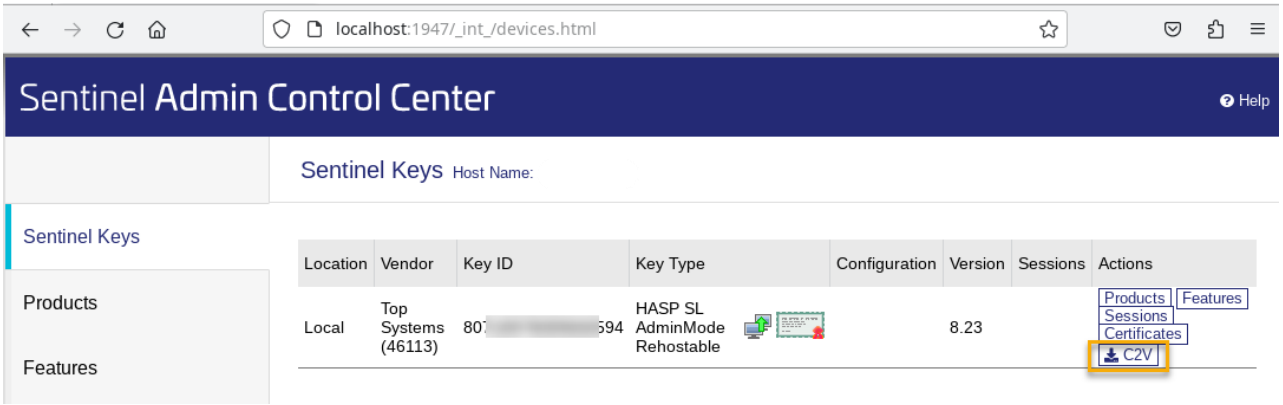
   Если необходим ключ или обновление ключа для компьютера с ОС Linux без графического интерфейса, то следует удаленно подключиться к Sentinel Admin Control Center с компьютера, имеющего графический интерфейс.

2. В окне Sentinel Admin Control Center перейдите на вкладку **Sentinel Keys** и выполните следующие действия:

   - Если вы хотите запросить новый программный ключ, найдите запись поставщика **Top Systems (46113)** и нажмите кнопку **Fingerprint** в столбце **Actions**:

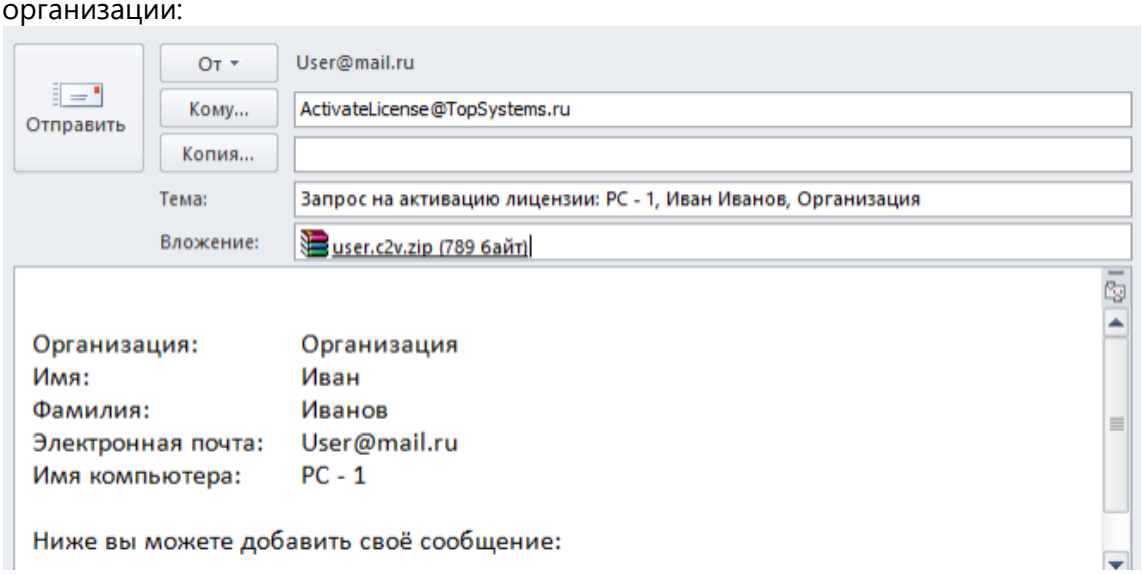


   - Если вы хотите запросить обновление для имеющегося программного или аппаратного ключа, найдите запись этого ключа и нажмите кнопку C2V в столбце Actions:



   В обоих случаях будет сформирован файл отпечатка компьютера в формате C2V, необходимый для генерации ключа. По умолчанию файл будет загружен в подкаталог **Загрузки** домашнего каталога пользователя. Файл отпечатка компьютера содержит только информацию об аппаратной части компьютера, и не содержит ваших личных данных.

3. Отправьте на адрес ActivateLicense@TopSystems.ru письмо с файлом C2V и данными об организации:



Прикрепление полученного файла

Служба лицензирования компании «Топ Системы» обработает запрос и пришлёт письмо с прикреплённым файлом. Файл содержит данные, необходимые для активации нового или обновления имеющегося ключа. Имя прикреплённого файла совпадает с номером ключа, формат файла – V2C.

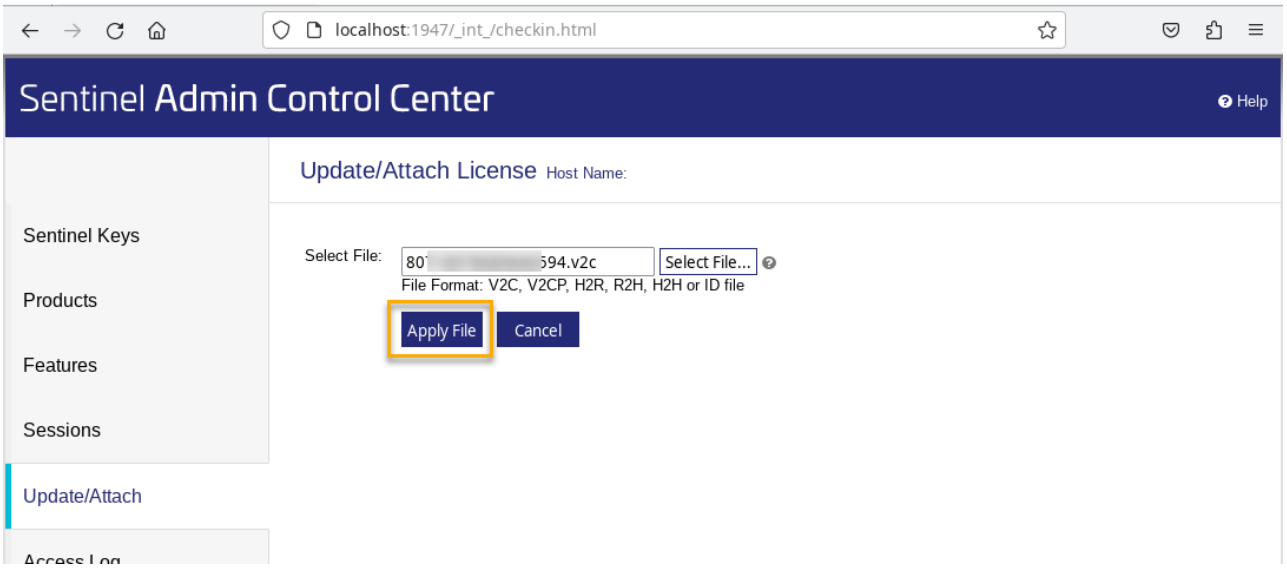
> Применение файла V2C следует производить строго на той машине, с которой был получен файл C2V. Файл C2V можно применить только один раз, повторное применение приведет к ошибке. Данная информация актуальна как для программных, так и для аппаратных ключей.

Для прикрепления файла ключа выполните следующие действия:

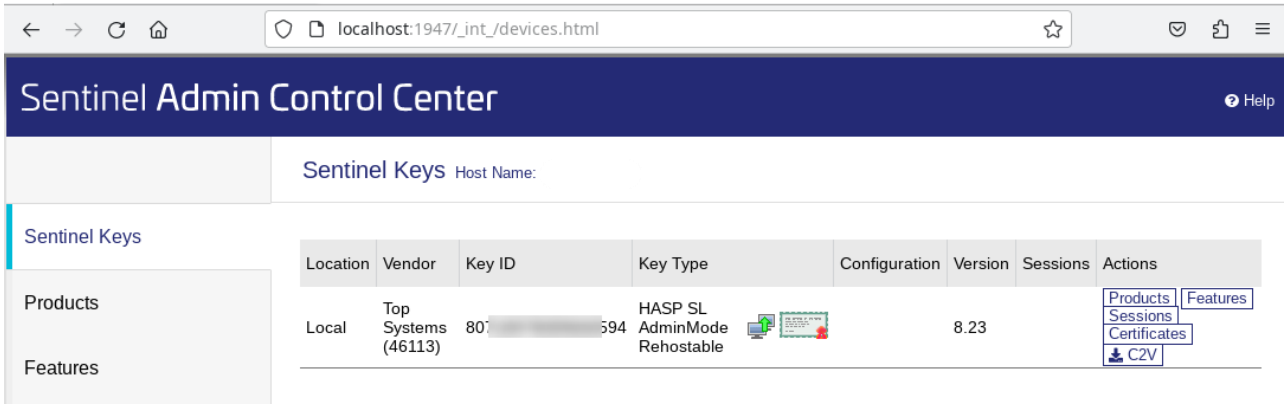
1. Сохраните полученный V2C файл в любую директорию на целевом компьютере.
2. Откройте Sentinel Admin Control Center, перейдя по ссылке http://localhost:1947

> Если необходимо прикрепить файл к компьютеру с ОС Linux без графического интерфейса, то следует удаленно подключиться к Sentinel Admin Control Center с компьютера, имеющего графический интерфейс.

3. В окне Sentinel Admin Control Center перейдите на вкладку **Update/Attach**, нажмите кнопку **Select File**, выберите полученный V2C файл и нажмите кнопку **Apply File**:



После успешной загрузки на вкладке **Sentinel Keys** должен отобразиться активированный ключ:



Удалённый доступ к Sentinel Admin Control Center

Если программный ключ требуется установить на компьютер с ОС Linux без графического интерфейса, то следует разрешить удаленный доступ к Sentinel Admin Control Center и подключиться к нему удаленно с компьютера, имеющего графический интерфейс.

По умолчанию удаленный доступ к Sentinel Admin Control Center запрещен. Чтобы разрешить удаленный доступ, выполните следующие действия:

1. Откройте файл **/etc/hasplm/hasplm.ini**

   ```
   sudo nano /etc/hasplm/hasplm.ini
   ```

Для данного действия требуются права суперпользователя. После запуска команды система запрашивает пароль суперпользователя. Введите пароль в терминал и нажмите **Enter**.

2. В зависимости от того, существует ли указанный файл, выполните одно из следующих действий:
   - Если файл существует, в нём уже будут прописаны различные параметры менеджера лицензий. В таком случае, найдите параметр **`accremote = 0`** в разделе **`[SERVER]`** и измените его значение с **`0`** на **`1`**.
   - Если файл не существует, откроется пустой черновик. В таком случае, вставьте туда следующий текст:

```
[SERVER]
name = <имя компьютера>
certificate =
privatekey =
identity_storage_encrypt = no
pagerefresh = 3
linesperpage = 12
accremote = 1
adminremote = 0
enablehaspc2v = 0
old_files_delete_days = 90

enabledetach = 0
enableautodetach = 0
autodetachhours = 2
reservedseats = 0
reservedpercent = 0
detachmaxdays = 14
commuter_delete_days = 7
disable_um = 0
idle_session_timeout_mins = 720

requestlog = 0
loglocal = 0
logremote = 0
logadmin = 0
errorlog = 1
rotatelogs = 0
access_log_maxsize = 0 ;kB
error_log_maxsize = 0 ;kB
zip_logs_days = 0
delete_logs_days = 0
pidfile = 0
passacc = 0

accessfromremote = anyone
accesstoremote = 1
bind_local_only = 0   ; 0=all adapters, 1=localhost only
```

```
id_public_addr =
proxy = 0
proxy_host =
proxy_port = 8080
proxy_username =
proxy_password =


[REMOTE]
broadcastsearch = 1
aggressive = 0
serversearchinterval = 30
serveraddr = S1


[ACCESS]


[USERS]


[VENDORS]


[EMS]
emsurl = http://localhost:8080
emsurl = http://127.0.0.1:8080


[TRUST]


[LOGPARAMETERS]
text = {timestamp} {clientaddr}:{clientport} {clientid} {method} {url}
{function}({functionparams}) result({statuscode}){newline}
```

Замените **имя компьютера** во второй строке фактическим именем целевого компьютера.

3. Нажмите **Ctrl+X,** чтобы закрыть файл, затем введите **Y** и нажмите **Enter** для сохранения внесённых изменений.
4. Перезапустите службу HASP License Manager:

```
systemctl restart hasplmd.service
```

После разрешения удалённого доступа можно подключиться к Sentinel Admin Control Center с другой компьютера, открыв в интернет-браузере следующую страницу:

```
http://servername:1947
```

где вместо **servername** следует указать либо имя целевого компьютера, либо его IP-адрес.