T·FLEX PLM

LICENSE KEY ACTIVATION AND UPDATE

on Linux OS

MDM

PM

RM

CAD CAE VR

PDM

CAPP CAM

Copyright

Table of Contents

Introduction

This document describes work with protection keys of T-FLEX PLM products on Linux operating systems.

Commands to be executed in terminal of operating system are marked as follows within this document:

```
The text to be typed into the terminal
```

Instead of typing commands, you can just copy them to clipboard from the current document and then paste into the terminal.

Upon inputting a command text, press **Enter** to execute the command.

Information about Protection Keys

Special protection keys created using **Sentinel HASP** technology are used to protect T-FLEX PLM products from an unauthorized usage. There are two types of protection keys - hardware and software. Keys have their own memory, which contains information about available customer licenses.

The hardware key is recorded on a physical device that plugs into a USB port on your computer.

> Hardware HASP keys of Sentinel HL series version 4.25 and above are used for protection of T-FLEX products. Older versions of keys are not supported.

Software key does not require the physical device. It is associated with a specific computer but can be moved to another computer if necessary.

The keys can store network or local licenses.

Local license works only on a single computer. Protection key should be activated on such computer.

Network license works on several computers. A number of users should not exceed the number of purchased licenses. Only one key with network license is used in this case. The key should be activated on one of the local network computers.

> Activation procedure for the protection keys does not depend on the license type.

Access to the licenses management is carried out via **Sentinel Admin Control Center** application.

If several licenses are available on a certain computer, the one with the highest priority is used. Here is the list of licenses in order of priority (from highest to lowest):

1. local license of a hardware key;
2. local license of a software key;
3. network license of a hardware key;
4. local license of a software key.

Installing HASP License Manager

The user performing the installation should have superuser rights.

1. Put the following archive into the **Downloads** directory of the target computer:
   T-FLEX_17_Linux_Components.zip

   If there is no internet connection on the target computer, download the archive on a computer connected to Internet and transfer it onto the target computer using physical media or local network connection.

2. Change working directory to **Downloads**:

   ```
   cd ~/Downloads
   ```

3. Unpack the **T-FLEX_17_Linux_Components.zip** archive:

   ```
   unzip T-FLEX_17_Linux_Components.zip
   ```

4. Change working directory to the **aksusbd** directory, previously unpacked from the **T-FLEX_17_Linux_Components.zip** archive:

   ```
   cd HASP_Linux/aksusbd/
   ```

5. Install the **aksusbd** package:

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

   Upon executing the command, the system asks for a root password. Type the password into the terminal and press **Enter**.

6. Change working directory to **HASP_Linux**:

   ```
   cd ~/Downloads/HASP_Linux
   ```

7. Copy **haspvlib_46113.so** and **haspvlib_x86_64_46113.so** libraries into the HASP License Manager directory:

   ```
   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. Make libraries copied on the previous step executable:

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

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

9. Restart HASP License Manager service:

   ```
   sudo systemctl restart hasplmd
   ```

Activating or updating a key

In order to activate a hardware key, just plug it into the target computer and wait for indicator to light up.

In order to receive a new software key, you should request it from the Top Systems Licensing Service. The Licensing Service will process the request and send a message with a key file. Upon receiving the file, you need to attach it to the target computer.

Updating procedure is same for software and hardware keys. First, request an update from the Top Systems Licensing Service. The Licensing Service will process the request and send a message with an updated key file. Upon receiving the file, you need to attach it to the target computer.

Requesting a new key or an update for an existing key

1. Open the Sentinel Admin Control Center, using this link: http://localhost:1947.

    If you need a key for a computer without graphical interface, you should access Sentinel Admin Control Center remotely from a computer with graphical interface.

2. In the Sentinel Admin Control Center switch to the **Sentinel Keys** tab and perform following actions:

    - If you want to request a new software key, find the record of the**Top Systems (46113)** vendor and press the **Fingerprint** button in the **Actions** column:
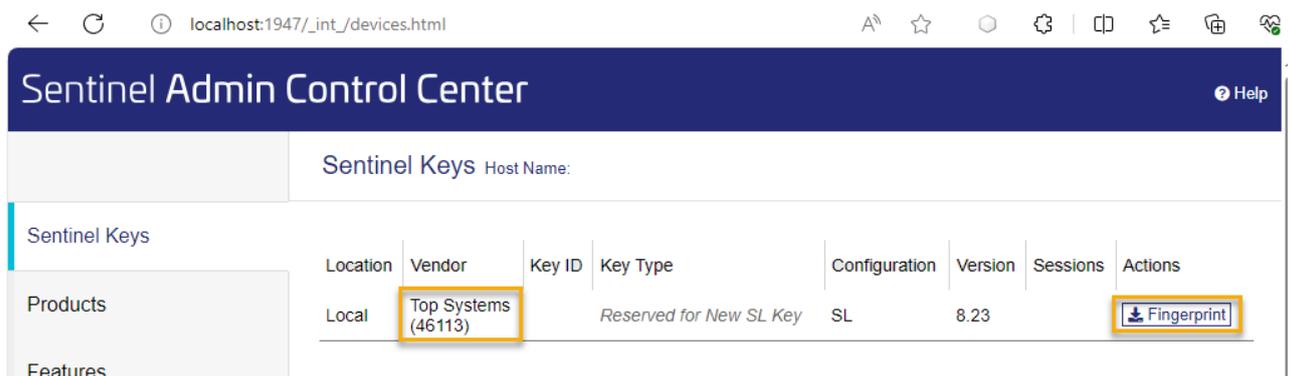

    - If you want to request an update for an existing software or hardware key, find the record of such key and press the **C2V** button in the **Actions** column:
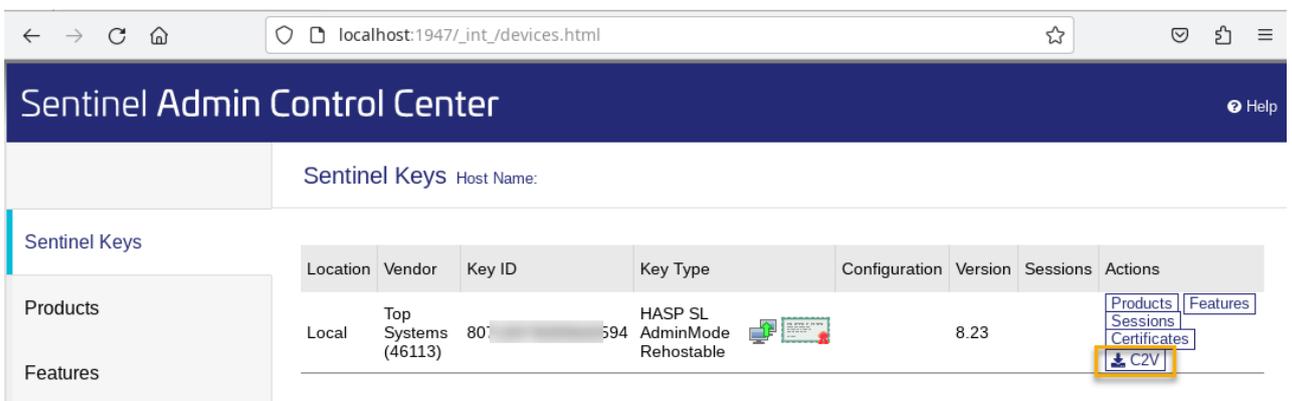
    In both cases, a fingerprint file in C2V format will be generated. It is required for generating a key. By default, the file is put into the **Downloads** subdirectory of user's home directory. Fingerprint file is unique for each computer. It contains information about your hardware components and doesn't contain any personal data

3. Send an e-mail to ActivateLicense@TopSystems.ru, attach the C2V file generated on the previous step and provide information about the company requesting the key:
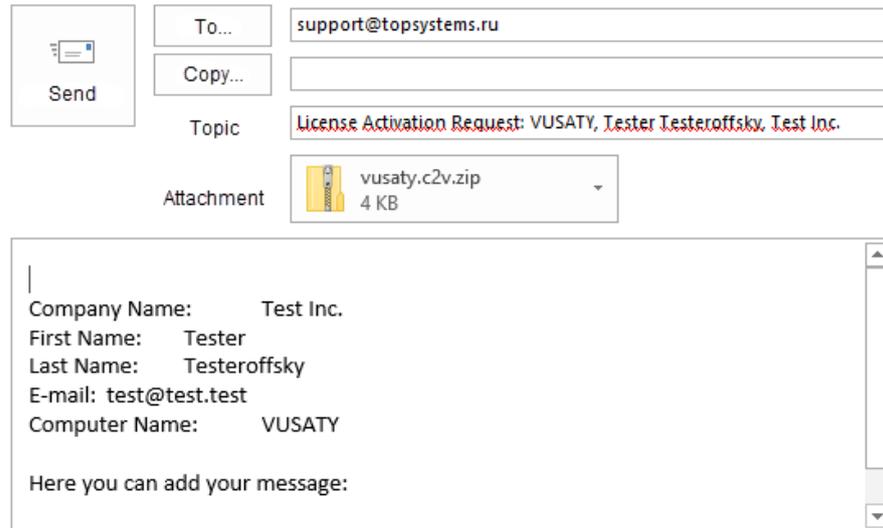
Attaching a received file

After processing your request, the Licensing Service will send you a message with the attached file. The file contains data for a new key activation or an update for the existing key. A name of the attached file is a number of the key. The file format is V2C.
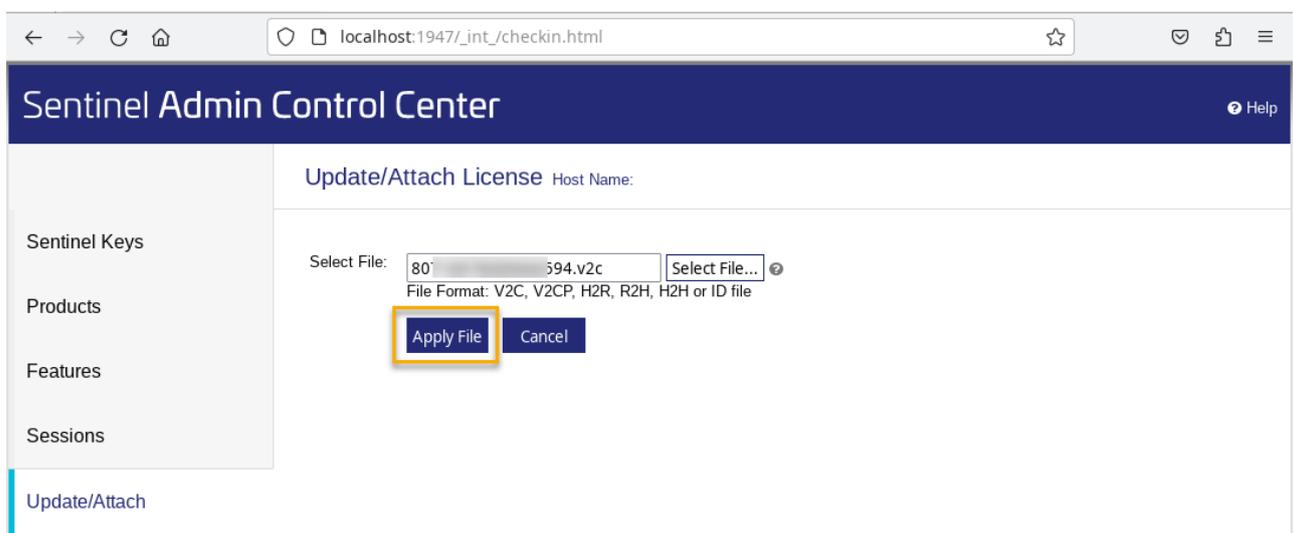
> A V2C can be attached only to those computer, where the C2V file sent in the request was generated. A key can only be activated once; further activation attempts cause errors.

In order to attach a file, perform following actions:

1. Save the received V2C file into any directory of the target computer.

2. Open Sentinel Admin Control Center, using this link: http://localhost:1947

> If you need to attach a file to a computer without graphical interface, you should access Sentinel Admin Control Center remotely from a computer with graphical interface.
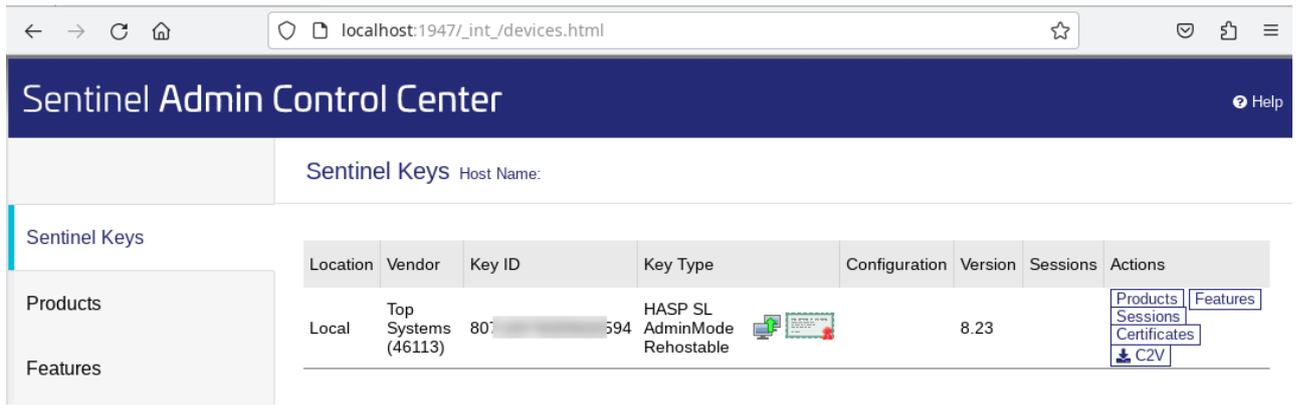
3. In the Sentinel Admin Control Center switch to the **Update/Attach** tab, press the **Select File** button, specify path to the received V2C file and press the **Apply File** button:

Activated key will be displayed in the **Sentinel Keys** tab:

Remote access to Sentinel Admin Control Center

If a key needs to be activated or updated on a computer that uses Linux OS without graphical user interface, you should allow the remote access to Sentinel Admin Control Center and open it remotely from a computer that uses OS with graphical user interface.

Remote access to Sentinel Admin Control Center is prohibited by default. In order to allow it, perform following actions:

1. Open the **/etc/hasplm/hasplm.ini** file:

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

You need superuser rights to perform this action. Upon executing the command, the system asks for a root password. Type the password into the terminal and press **Enter**.

2. Depending on whether the file exists, perform one of the following actions:
   - If the file already exists, it contains various parameters of HASP License Manager. In such case, find the `accremote` parameter in the `[SERVER]` section and change its value from `0` to `1`.
   - If the file doesn't exist, the empty draft will be opened. In such case, fill it with the following text:

```
[SERVER]
name = <COMPUTER_NAME>
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}
```

> Replace **COMPUTER_NAME** in the second line with actual name of the current computer.

3. Close the file by pressing **Ctrl+X** and confirm changes by typing **Y** and pressing **Enter**.

4. Restart the HASP License Manager service:

```
systemctl restart hasplmd.service
```

Upon allowing the remote access, you can open the Sentinel Admin Control Center from a different computer using by opening the following page in any internet-browser:

`http://servername:1947`

where **servername** should be replaced by the name or IP-address of the target computer.