Instruction on connecting to VPN for Linux. VPN Helper UG

Installing root certificates using a script

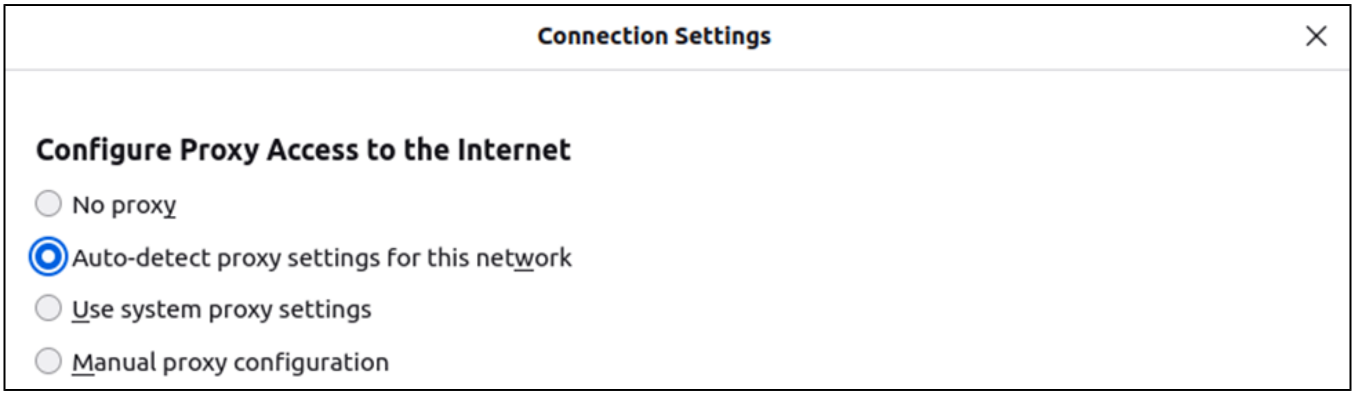
To install root certificates using a script, follow these steps:

1. Download the script from the link.
2. In the terminal, navigate to the directory where the script was downloaded. Run the following command:

```
sudo sh ./ca-certs.sh
```

Installing root certificates in manual mode

To access the Internet in FireFox, navigate to **Settings** → **General** → **Network Settings** → **Connection Settings** and select **Auto-detect proxy settings for this network**:



Connection Settings

Configure Proxy Access to the Internet

○ No proxy
● Auto-detect proxy settings for this network
○ Use system proxy settings
○ Manual proxy configuration

To install root certificates, follow these steps:

1. Download the archive with the certificates:

```
wget https://vpnhelp.kaspersky.com/Applications/certificates.zip
```

2. Unzip the archive and copy the contents to the destination folder:

```
unzip certificates.zip -d certificates
```

3. Navigate to the folder with the certificates:

```
cd certificates
```

4. Change the certificate format to a compatible one:

```
for f in *.cer; do mv "$f" "${f%.cer}.crt"; done
```

5. Copy the resulting files to the system folder, set access rights to them and start the process of updating system certificates:

```
sudo cp * /usr/local/share/ca-certificates/
sudo chmod 664 /usr/local/share/ca-certificates/*.*

sudo update-ca-certificates
```

Installing and configuring tokens using a script

To install and set up eToken/ruToken using a script, follow these steps:

1. Depending on the OS version and token type, download the required version of the script:
   - SafeNet for eToken Ubuntu 20.04
   - SafeNet for eToken Ubuntu 22.04

    - Minidriver for ruToken (Any OS version)
2. Insert the hardware token into the device.
3. Unzip the downloaded archive.
4. In the terminal, navigate to the unzipped directory.
5. Depending on which version of the script was downloaded, run one of the following commands:
    - For **SafeNet** for **eToken Ubuntu 20.04**:

      ```
      sudo sh ./SafeNet_20.04.sh
      ```
    - For **SafeNet** for **eToken Ubuntu 22.04**:

      ```
      sudo sh ./SafeNet_22.04_2.sh
      ```
    - For **Minidriver** for **ruToken**:

      ```
      sudo sh ./ruToken.sh
      ```

Installing and configuring tokens in manual mode

To enable tokens of any type to work in the system, run the following command:

```
sudo apt install gnutls-bin libengine-pkcs11-openssl opensc
```

Installing and configuring eToken

1. Depending on Ubuntu version, download the driver for the eToken:
    - eToken driver for Ubuntu 20.04
    - eToken driver for Ubuntu 22.04
2. Unzip the downloaded archive.
3. Depending on Ubuntu version, run one of the following commands:
    - For **Ubuntu 20.04**:

      ```
      sudo dpkg –i safenetauthenticationclient_10.8.28_amd64.deb
      ```
    - For **Ubuntu 22.04**:

      ```
      sudo dpkg –i safenetauthenticationclient_10.8.1050_amd64.deb
      ```
4. Run the following commands:

   ```
   sudo mkdir -p /etc/pkcs11/modules/

   echo 'module: /usr/lib/libeTPkcs11.so' | sudo tee -a /etc/pkcs11/modules/eToken.module
   ```
5. To allow the **p11tool** utility to access the token module, specify the path to the token module:

   ```
    echo 'load=/usr/lib/libeTPkcs11.so' | sudo tee -a /etc/gnutls/pkcs11.conf
   ```
6. If the **gnutls** folder and the **pkcs11.conf** file have not been created, create them manually:

   ```
   sudo mkdir -p /etc/gnutls/

   sudo touch /etc/gnutls/pkcs11.conf
   ```

Installing and configuring ruToken

1. Download the latest version of the driver for ruToken from the link.
2. In the terminal, navigate to the folder with the driver and run the following command:

   ```
   sudo dpkg -i librtpkcs11ecp_{{ version }}_amd64.deb
   ```
3. Run the following commands:

   ```
   sudo mkdir -p /etc/pkcs11/modules/
   echo 'module: /usr/lib/librtpkcs11ecp.so' | sudo tee -a /etc/pkcs11/modules/ruToken.module
   ```
4. To allow the **p11tool** utility to access the token module, specify the path to the token module by running the following command:

```
echo 'load=/usr/lib/librtpkcs11ecp.so' | sudo tee -a /etc/gnutls/pkcs11.conf
```

Configuring a VPN connection using a script

To configure a VPN connection using a script, follow these steps:

1. Download the VPN connection setup script from the link.
2. Insert the hardware token into the device.
3. In the terminal, navigate to the directory where the script was downloaded. Run the following command:

   ```
   sudo sh ./KLCiscoVPN.sh
   ```

Configuring a VPN connection in manual mode

To configure a VPN connection, follow these steps:

1. Set up the **OpenConnect** client:

   ```
   sudo apt install network-manager-openconnect-gnome
   ```
2. Get your real UUID:

   ```
   awk '/^UUID/ {print $1;}' /etc/fstab | awk '{print substr( $0,6 )}' | sed '2d'
   ```
3. Get a URL for a user certificate and a key:

   ```
   p11tool --list-tokens | grep  "pkcs11" | grep -v "MultiToken" | grep -v "p11-kit" | grep -v "/usr/lib" |
   sed "s|.*: ||g"
   ```

   Or

   ```
   p11tool --list-token-urls
   ```

   Copy the string that contains the last and first name.

   > **Example**
   >
   > ```
   > pkcs11:model=eToken;manufacturer=SafeNet%2c%20Inc.;serial=11111111;token=token=<Employee name>%
   > 20<Employee Surname>'
   > ```

4. Get a user certificate:

   ```
   p11tool --login --list-all <Result of the previous command from step 3> | grep  "pkcs11" | grep
   "type=cert" | sed "s|.*: ||g" | grep -v "MultiToken"| sed "s|.*: ||g"
   ```

   Or

   ```
   p11tool --login --list-all <Result of the previous command from step 3>
   ```

   > **Example**
   >
   > ```
   > p11tool --login --list-all 'pkcs11:model=eToken;manufacturer=SafeNet%2c%20Inc.;serial=11111111;
   > token=token=<Employee name>%20<Employee Surname>'
   > ```

5. Get the Private Key of the token:

   ```
   p11tool --login --list-privkeys <Result of the previous command from step 3> | grep  "pkcs11" | grep
   "type=private" | sed "s|.*: ||g" | grep -v "MultiToken"| sed "s|.*: ||g"
   ```

Or

```
p11tool --login --list-privkeys <Result of the previous command from step 3>
```

Example

```
p11tool --login --list-privkeys 'pkcs11:model=eToken;manufacturer=SafeNet%2c%20Inc.;serial=11111111;
token=token=<Employee name>%20<Employee Surname>'
```

6. Create the **KLCVPN.nmconnection** file and place it in `/etc/NetworkManager/system-connections/`:

```
sudo nano /etc/NetworkManager/system-connections/KLCVPN.nmconnection
```

7. Instead of the specified variables, specify your data in this file:
   a. **UID** - result of the command from step 2
   b. **KLRCA_PATH** - path to **Kaspersky Root CA G3.crt** (default path when installing using the current instructions: `/usr/local/share/ca-certificates/Kaspersky_Root_CA_G3.crt`)
   c. **TOKEN_USR_CERT** - result of the command from step 4
   d. **TOKEN_PRIV_KEY** - result of the command from step 5

```
[connection]

id=KLCVPN

uuid=<UID>

type=vpn

permissions=



[vpn]

authtype=cert

autoconnect-flags=0

cacert=<KLRCA_PATH>

certsigs-flags=0

cookie-flags=2

enable_csd_trojan=no

gateway=cvpn.kaspersky.com

gateway-flags=2

gwcert-flags=2

lasthost-flags=0

pem_passphrase_fsid=no

usercert=<TOKEN_USR_CERT>

userkey=<TOKEN_PRIV_KEY>

xmlconfig-flags=0

service-type=org.freedesktop.NetworkManager.openconnect



[vpn-secrets]

lasthost=cvpn.kaspersky.com
```

```
xmlconfig=PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4NCjxBbnlDb25uZWN0UHJvZmlsZSB4bWxucz0ia
HR0cDovL3NjaGVtYXMueG1sc29hcC5vcmcvZW5jb2RpbmcvIiB4bWxuczp4c2k9Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvWE1M
U2NoZW1hLWluc3RhbmNlIiB4c2k6c2NoZW1hTG9jYXRpb249Imh0dHA6Ly9zY2hlbWFzLnhtbHNvYXAub3JnL2VuY29kaW5nLyB
BbnlDb25uZWN0UHJvZmlsZS54c2QiPg0KCTxDbGllbnRJbml0aWFsaXphdGlvbj4NCgkJPFVzZVN0YXJ0QmVmb3JlTG9nb24gVX
NlckNvbnRyb2xsYWJsZT0iZmFsc2UiPmZhbHNlPC9Vc2VTdGFydEJlZm9yZUxvZ29uPg0KCQk8QXV0b21hdGljQ2VydFNlbGVjd
GlvbiBVc2VyQ29udHJvbGxhYmxlPSJ0cnVlIj50cnVlPC9BdXRvbWF0aWNDZXJ0U2VsZWN0aW9uPg0KCQk8U2hvd1ByZUNvbm5l
Y3RNZXNzYWdlPmZhbHNlPC9TaG93UHJlQ29ubmVjdE1lc3NhZ2U+DQoJCTxDZXJ0aWZpY2F0ZVN0b3JlPlVzZXI8L0NlcnRpZml
jYXRlU3RvcmU+DQoJCTxDZXJ0aWZpY2F0ZVN0b3JlTWFjPkxvZ2luPC9DZXJ0aWZpY2F0ZVN0b3JlTWFjPg0KCQk8Q2VydGlmaW
NhdGVTdG9yZUxpbnV4PkFsbDwvQ2VydGlmaWNhdGVTdG9yZUxpbnV4Pg0KCQk8Q2VydGlmaWNhdGVTdG9yZU92ZXJyaWRlPmZhb
HNlPC9DZXJ0aWZpY2F0ZVN0b3JlT3ZlcnJpZGU+DQoJCTxQcm94eVNldHRpbmdzPk5hdGl2ZTwvUHJveHlTZXR0aW5ncz4NCgkJ
PEFsbG93TG9jYWxQcm94eUNvbm5lY3Rpb25zPnRydWU8L0FsbG93TG9jYWxQcm94eUNvbm5lY3Rpb25zPg0KCQk8QXV0aGVudGl
jYXRpb25UaW1lb3V0PjEyPC9BdXRoZW50aWNhdGlvblRpbWVvdXQ+DQoJCTxBdXRvQ29ubmVjdE9uU3RhcnQgVXNlckNvbnRyb2
xsYWJsZT0idHJ1ZSI+ZmFsc2U8L0F1dG9Db25uZWN0T25TdGFydD4NCgkJPE1pbmltaXplT25Db25uZWN0IFVzZXJDb250cm9sb
GFibGU9InRydWUiPnRydWU8L01pbmltaXplT25Db25uZWN0Pg0KCQk8TG9jYWxMYW5BY2Nlc3MgVXNlckNvbnRyb2xsYWJsZT0i
dHJ1ZSI+dHJ1ZTwvTG9jYWxMYW5BY2Nlc3M+DQoJCTxEaXNhYmxlQ2FwdGl2ZVBvcnRhbERldGVjdGlvbiBVc2VyQ29udHJvbGx
hYmxlPSJ0cnVlIj5mYWxzZTwvRGlzYWJsZUNhcHRpdmVQb3J0YWxEZXRlY3Rpb24+DQoJCTxDbGVhclNtYXJ0Y2FyZFBpbiBVc2
VyQ29udHJvbGxhYmxlPSJmYWxzZSI+dHJ1ZTwvQ2xlYXJTbWFydGNhcmRQaW4+DQoJCTxJUFByb3RvY29sU3VwcG9ydD5JUHY0P
C9JUFByb3RvY29sU3VwcG9ydD4NCgkJPEF1dG9SZWNvbm5lY3QgVXNlckNvbnRyb2xsYWJsZT0idHJ1ZSI+dHJ1ZQ0KCQkJPEF1
dG9SZWNvbm5lY3RCZWhhdmlvciBVc2VyQ29udHJvbGxhYmxlPSJmYWxzZSI+UmVjb25uZWN0QWZ0ZXJSZXN1bWU8L0F1dG9SZWN
vbm5lY3RCZWhhdmlvcj4NCgkJPC9BdXRvUmVjb25uZWN0Pg0KCQk8U3VzcGVuZE9uQ29ubmVjdGVkU3RhbmRieT5mYWxzZTwvU3
VzcGVuZE9uQ29ubmVjdGVkU3RhbmRieT4NCgkJPEF1dG9VcGRhdGUgVXNlckNvbnRyb2xsYWJsZT0iZmFsc2UiPnRydWU8L0F1d
G9VcGRhdGU+DQoJCTxSU0FTZWN1cklESW50ZWdyYXRpb24gVXNlckNvbnRyb2xsYWJsZT0iZmFsc2UiPkF1dG9tYXRpYzwvUlNB
U2VjdXJJREludGVncmF0aW9uPg0KCQk8V2luZG93c0xvZ29uRW5mb3JjZW1lbnQ+U2luZ2xlTG9jYWxMb2dvbjwvV2luZG93c0x
vZ29uRW5mb3JjZW1lbnQ+DQoJCTxMaW51eExvZ29uRW5mb3JjZW1lbnQ+U2luZ2xlTG9jYWxMb2dvbjwvTGludXhMb2dvbkVuZm
9yY2VtZW50Pg0KCQk8V2luZG93c1ZQTkVzdGFibGlzaG1lbnQ+QWxsb3dSZW1vdGVVc2VyczwvV2luZG93c1ZQTkVzdGFibGlza
G1lbnQ+DQoJCTxMaW51eFZQTkVzdGFibGlzaG1lbnQ+QWxsb3dSZW1vdGVVc2VyczwvTGludXhWUE5Fc3RhYmxpc2htZW50Pg0K
CQk8QXV0b21hdGljVlBOUG9saWN5PmZhbHNlPC9BdXRvbWF0aWNWUE5Qb2xpY3k+DQoJCTxQUFBFeGNsdXNpb24gVXNlckNvbnR
yb2xsYWJsZT0iZmFsc2UiPkF1dG9tYXRpYw0KCQkJPFBQUEV4Y2x1c2lvblNlcnZlcklQIFVzZXJDb250cm9sbGFibGU9ImZhbH
NlIj48L1BQUEV4Y2x1c2lvblNlcnZlcklQPg0KCQk8L1BQUEV4Y2x1c2lvbj4NCgkJPEVuYWJsZVNjcmlwdGluZyBVc2VyQ29ud
HJvbGxhYmxlPSJmYWxzZSI+ZmFsc2U8L0VuYWJsZVNjcmlwdGluZz4NCgkJPENlcnRpZmljYXRlUGlubmluZz50cnVlDQoJCQk8
Q2VydGlmaWNhdGVQaW5MaXN0Pg0KCQkJCTxQaW4gU3ViamVjdD0iQ049S2FzcGVyc2t5IFNlcnZlciBBdXRoZW50aWNhdGlvbiB
DQSBHMyxPPUthc3BlcnNreSxDPVJVIiBJc3N1ZXI9IkNOPUthc3BlcnNreSBSb290IENBIEczLE89S2FzcGVyc2t5LEM9UlUiPk
U3RTU4OUYxN0Q4MzQ5Mjg1QzA4NDI1M0RDMTg5RkYxRTgzMkJFNUNGRTI3QTY0NzUyOTc0ODcwRUI1ODAzNzQ1QkI3MDE4OTBEQ
jMxNzQ0RkE2NjAwNzQyQzkzMEY1Q0UyQzA0RjhBNThDNzQ4MkIzNzk4MDI3MEIxQkZGNkMxPC9QaW4+DQoJCQk8L0NlcnRpZmlj
YXRlUGluTGlzdD4NCgkJPC9DZXJ0aWZpY2F0ZVBpbm5pbmc+DQoJCTxDZXJ0aWZpY2F0ZU1hdGNoPg0KCQkJPE1hdGNoT25seUN
lcnRzV2l0aEVLVT50cnVlPC9NYXRjaE9ubHlDZXJ0c1dpdGhFS1U+DQoJCQk8TWF0Y2hPbmx5Q2VydHNXaXRoS1U+ZmFsc2U8L0
1hdGNoT25seUNlcnRzV2l0aEtVPg0KCQkJPEV4dGVuZGVkS2V5VXNhZ2U+DQoJCQkJPEV4dGVuZGVkTWF0Y2hLZXk+Q2xpZW50Q
XV0aDwvRXh0ZW5kZWRNYXRjaEtleT4NCgkJCQk8Q3VzdG9tRXh0ZW5kZWRNYXRjaEtleT4xLjMuNi4xLjQuMS4zMTEuMjAuMi4y
PC9DdXN0b21FeHRlbmRlZE1hdGNoS2V5Pg0KCQkJPC9FeHRlbmRlZEtleVVzYWdlPg0KCQkJPERpc3Rpbmd1aXNoZWROYW1lPg0
KCQkJCTxEaXN0aW5ndWlzaGVkTmFtZURlZmluaXRpb24gT3BlcmF0b3I9IkVxdWFsIiBXaWxkY2FyZD0iRW5hYmxlZCIgTWF0Y2
hDYXNlPSJFbmFibGVkIj4NCgkJCQkJPE5hbWU+SVNTVUVSLUNOPC9OYW1lPg0KCQkJCQk8UGF0dGVybj5LYXNwZXJza3k8L1Bhd
HRlcm4+DQoJCQkJPC9EaXN0aW5ndWlzaGVkTmFtZURlZmluaXRpb24+DQoJCQkJPERpc3Rpbmd1aXNoZWROYW1lRGVmaW5pdGlv
biBPcGVyYXRvcj0iTm90RXF1YWwiIFdpbGRjYXJkPSJFbmFibGVkIiBNYXRjaENhc2U9IkVuYWJsZWQiPg0KCQkJCQk8TmFtZT5
JU1NVRVItQ048L05hbWU+DQoJCQkJCTxQYXR0ZXJuPkNBIEVDQzwvUGF0dGVybj4NCgkJCQk8L0Rpc3Rpbmd1aXNoZWROYW1lRG
VmaW5pdGlvbj4NCgkJCQk8RGlzdGluZ3Vpc2hlZE5hbWVEZWZpbml0aW9uIE9wZXJhdG9yPSJOb3RFcXVhbCIgV2lsZGNhcmQ9I
kVuYWJsZWQiIE1hdGNoQ2FzZT0iRW5hYmxlZCI+DQoJCQkJCTxOYW1lPklTU1VFUi1DTjwvTmFtZT4NCgkJCQkJPFBhdHRlcm4+
RXh0ZXJuYWwgU2VydmljZXM8L1BhdHRlcm4+DQoJCQkJPC9EaXN0aW5ndWlzaGVkTmFtZURlZmluaXRpb24+DQoJCQk8L0Rpc3R
pbmd1aXNoZWROYW1lPg0KCQk8L0NlcnRpZmljYXRlTWF0Y2g+DQoJCTxFbmFibGVBdXRvbWF0aWNTZXJ2ZXJTZWxlY3Rpb24gVX
NlckNvbnRyb2xsYWJsZT0idHJ1ZSI+dHJ1ZQ0KCQkJPEF1dG9TZXJ2ZXJTZWxlY3Rpb25JbXByb3ZlbWVudD4yMDwvQXV0b1Nlc
nZlclNlbGVjdGlvbkltcHJvdmVtZW50Pg0KCQkJPEF1dG9TZXJ2ZXJTZWxlY3Rpb25TdXNwZW5kVGltZT40PC9BdXRvU2VydmVy
U2VsZWN0aW9uU3VzcGVuZFRpbWU+DQoJCTwvRW5hYmxlQXV0b21hdGljU2VydmVyU2VsZWN0aW9uPg0KCQk8UmV0YWluVnBuT25
Mb2dvZmY+ZmFsc2UNCgkJPC9SZXRhaW5WcG5PbkxvZ29mZj4NCgkJPENhcHRpdmVQb3J0YWxSZW1lZGlhdGlvbkJyb3dzZXJGYW
lsb3Zlcj5mYWxzZTwvQ2FwdGl2ZVBvcnRhbFJlbWVkaWF0aW9uQnJvd3NlckZhaWxvdmVyPg0KCQk8QWxsb3dNYW51YWxIb3N0S
W5wdXQ+ZmFsc2U8L0FsbG93TWFudWFsSG9zdElucHV0Pg0KCTwvQ2xpZW50SW5pdGlhbGl6YXRpb24+DQoJPFNlcnZlckxpc3Q+
DQoJCTxIb3N0RW50cnk+DQoJCQk8SG9zdE5hbWU+QVBBQzwvSG9zdE5hbWU+DQoJCQk8SG9zdEFkZHJlc3M+Y3Zwbi5hcGFjLmt
hc3BlcnNreS5jb208L0hvc3RBZGRyZXNzPg0KCQkJPEJhY2t1cFNlcnZlckxpc3Q+DQoJCQkJPEhvc3RBZGRyZXNzPmN2cG4uY2
5iai5rYXNwZXJza3kuY29tPC9Ib3N0QWRkcmVzcz4NCgkJCTwvQmFja3VwU2VydmVyTGlzdD4NCgkJPC9Ib3N0RW50cnk+DQoJC
TxIb3N0RW50cnk+DQoJCQk8SG9zdE5hbWU+Q05CSjwvSG9zdE5hbWU+DQoJCQk8SG9zdEFkZHJlc3M+Y3Zwbi5jbmJqLmthc3Bl
cnNreS5jb208L0hvc3RBZGRyZXNzPg0KCQkJPEJhY2t1cFNlcnZlckxpc3Q+DQoJCQkJPEhvc3RBZGRyZXNzPmN2cG4uYXBhYy5
rYXNwZXJza3kuY29tPC9Ib3N0QWRkcmVzcz4NCgkJCTwvQmFja3VwU2VydmVyTGlzdD4NCgkJPC9Ib3N0RW50cnk+DQoJCTxIb3
N0RW50cnk+DQoJCQk8SG9zdE5hbWU+RVU8L0hvc3ROYW1lPg0KCQkJPEhvc3RBZGRyZXNzPmN2cG4uZXUua2FzcGVyc2t5LmNvb
TwvSG9zdEFkZHJlc3M+DQoJCQk8QmFja3VwU2VydmVyTGlzdD4NCgkJCQk8SG9zdEFkZHJlc3M+Y3Zwbi5zZGMua2FzcGVyc2t5
LmNvbTwvSG9zdEFkZHJlc3M+DQoJCQkJPEhvc3RBZGRyZXNzPmN2cG4ub2RjLmthc3BlcnNreS5jb208L0hvc3RBZGRyZXNzPg0
KCQkJCTxIb3N0QWRkcmVzcz5jdnBuLmxkYy5rYXNwZXJza3kuY29tPC9Ib3N0QWRkcmVzcz4NCgkJCTwvQmFja3VwU2VydmVyTG
lzdD4NCgkJPC9Ib3N0RW50cnk+DQoJCTxIb3N0RW50cnk+DQoJCQk8SG9zdE5hbWU+SFEtTDwvSG9zdE5hbWU+DQoJCQk8SG9zd
EFkZHJlc3M+Y3Zwbi5sZGMua2FzcGVyc2t5LmNvbTwvSG9zdEFkZHJlc3M+DQoJCQk8QmFja3VwU2VydmVyTGlzdD4NCgkJCQk8
SG9zdEFkZHJlc3M+Y3Zwbi5vZGMua2FzcGVyc2t5LmNvbTwvSG9zdEFkZHJlc3M+DQoJCQkJPEhvc3RBZGRyZXNzPmN2cG4uc2R
```

```
jLmthc3BlcnNreS5jb208L0hvc3RBZGRyZXNzPg0KCQkJPC9CYWNrdXBTZXJ2ZXJMaXN0Pg0KCQk8L0hvc3RFbnRyeT4NCgkJPE
hvc3RFbnRyeT4NCgkJCTxIb3N0TmFtZT5IUS1PPC9Ib3N0TmFtZT4NCgkJCTxIb3N0QWRkcmVzcz5jdnBuLm9kYy5rYXNwZXJza
3kuY29tPC9Ib3N0QWRkcmVzcz4NCgkJCTxCYWNrdXBTZXJ2ZXJMaXN0Pg0KCQkJCTxIb3N0QWRkcmVzcz5jdnBuLmxkYy5rYXNw
ZXJza3kuY29tPC9Ib3N0QWRkcmVzcz4NCgkJCQk8SG9zdEFkZHJlc3M+Y3Zwbi5zZGMua2FzcGVyc2t5LmNvbTwvSG9zdEFkZHJ
lc3M+DQoJCQk8L0JhY2t1cFNlcnZlckxpc3Q+DQoJCTwvSG9zdEVudHJ5Pg0KCQk8SG9zdEVudHJ5Pg0KCQkJPEhvc3ROYW1lPk
hRLVM8L0hvc3ROYW1lPg0KCQkJPEhvc3RBZGRyZXNzPmN2cG4uc2RjLmthc3BlcnNreS5jb208L0hvc3RBZGRyZXNzPg0KCQkJP
EJhY2t1cFNlcnZlckxpc3Q+DQoJCQkJPEhvc3RBZGRyZXNzPmN2cG4ubGRjLmthc3BlcnNreS5jb208L0hvc3RBZGRyZXNzPg0K
CQkJCTxIb3N0QWRkcmVzcz5jdnBuLm9kYy5rYXNwZXJza3kuY29tPC9Ib3N0QWRkcmVzcz4NCgkJCTwvQmFja3VwU2VydmVyTGl
zdD4NCgkJPC9Ib3N0RW50cnk+DQoJCTxIb3N0RW50cnk+DQoJCQk8SG9zdE5hbWU+VVM8L0hvc3ROYW1lPg0KCQkJPEhvc3RBZG
RyZXNzPmN2cG4udXMua2FzcGVyc2t5LmNvbTwvSG9zdEFkZHJlc3M+DQoJCQk8QmFja3VwU2VydmVyTGlzdD4NCgkJCQk8SG9zd
EFkZHJlc3M+Y3Zwbi5ldS5rYXNwZXJza3kuY29tPC9Ib3N0QWRkcmVzcz4NCgkJCTwvQmFja3VwU2VydmVyTGlzdD4NCgkJPC9I
b3N0RW50cnk+DQoJPC9TZXJ2ZXJMaXN0Pg0KPC9BbnlDb25uZWN0UHJvZmlsZT4NCg==



[ipv4]

dns-search=

method=auto


[ipv6]

addr-gen-mode=stable-privacy

dns-search=

ip6-privacy=0

method=auto


[proxy]
```

8. Set **600** permissions on the `/etc/NetworkManager/system-connections/KLCVPN.nmconnection` file:

   ```
   sudo chmod 0600 /etc/NetworkManager/system-connections/KLCVPN.nmconnection
   ```

9. Upload the file to Network Manager:

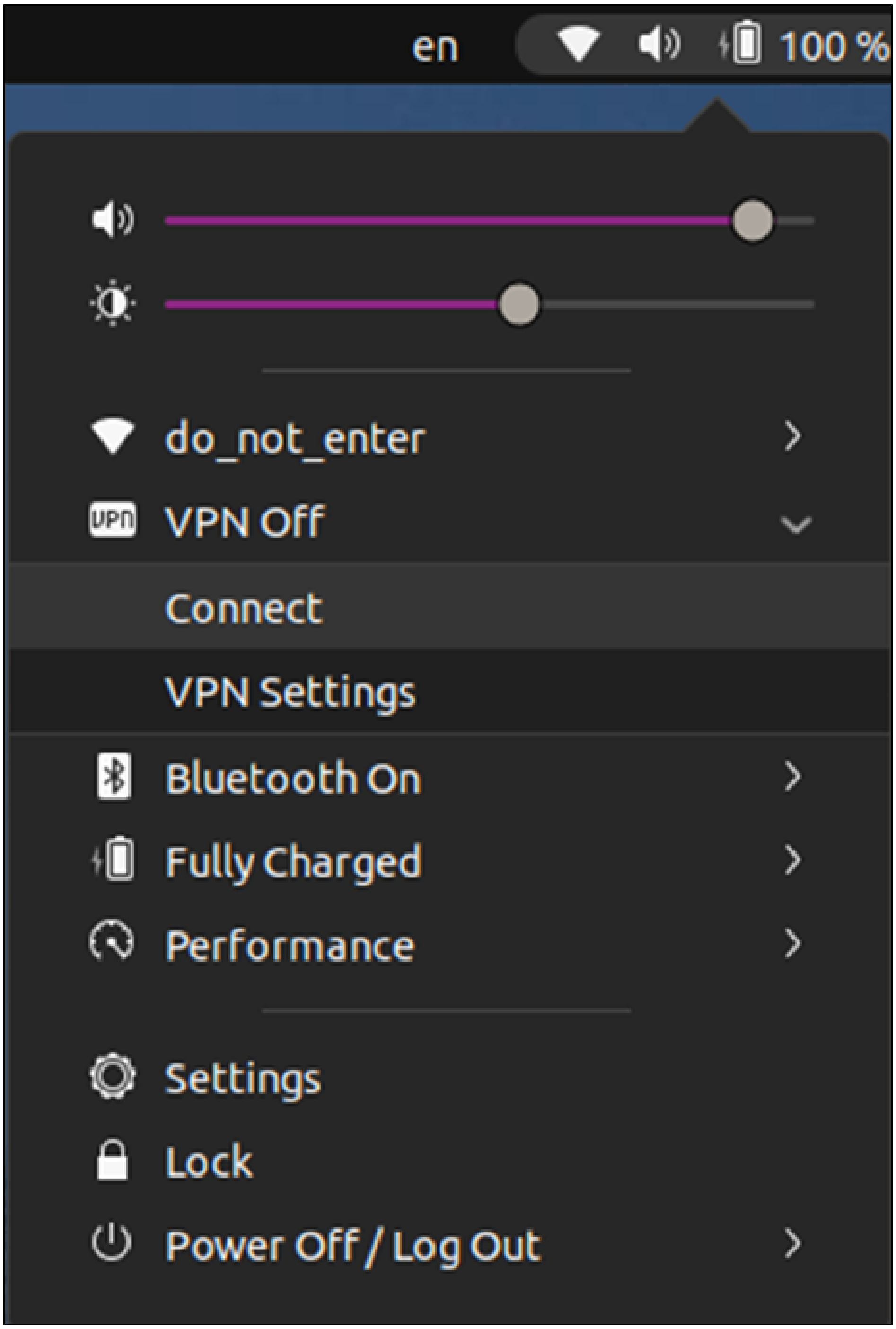
   ```
   sudo nmcli connection load /etc/NetworkManager/system-connections/KLCVPN.nmconnection

   sudo nmcli connection reload /etc/NetworkManager/system-connections/KLCVPN.nmconnection
   ```

10. Restart Network Manger:

    ```
    sudo systemctl restart NetworkManager
    ```

11. Establish the connection:



12. In the window that opens, click **Connect.**
13. When connecting, enter the password for the token and select the **Save Passwords** checkbox.

> **Note**
>
> For the first connection, the selection of VPN node will not be available, on subsequent connections you will be able to select the desired node yourself.

[OPTIONAL] To disable the **sudo** password request when connecting to the VPN from other accounts, follow these steps:

1. Use the **policykit** integrated tools:

```
echo """
```

```
[Let all users modify system settings for network]

Identity=unix-user:*

Action=org.freedesktop.NetworkManager.settings.modify.system

ResultAny=no

ResultInactive=no

ResultActive=yes

""" | sudo tee /etc/polkit-1/localauthority/50-local.d/10-network-manager.pkla
```

2. Restart Network Manger:

   ```
   sudo systemctl restart NetworkManager
   ```