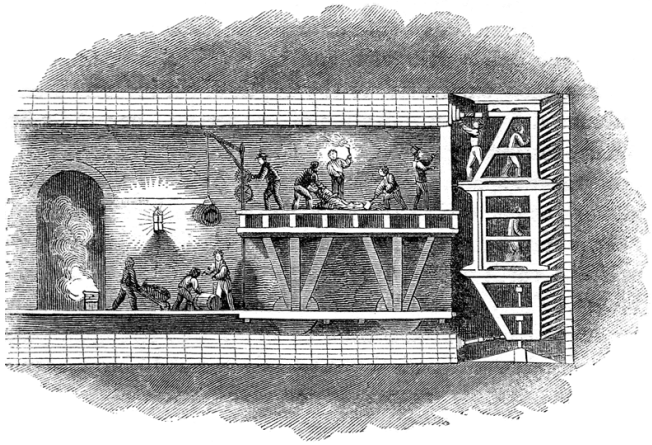
UvA-VPN for Linux

UvA ICTS



UvA-VPN is a device to establish a shielded connection between your personal computer residing outside the UvA and the internal network of the UvA, enabling you to access restricted university facilities (e.g. file servers, UNIX hosts, Zelfbediening, etc.) as if the remote computer were physically part of the UvA network. Additionally a few services require access through UvA-VPN even for hosts already connected to a UvA network. The following text explains how to set up UvA-VPN on a modern Linux computer, either Redhat RPM- or Debian-based.

OpenConnect vs. Juniper's proprietary software

To set up UvA-VPN on your Linux computer one can choose to either use Juniper's proprietary VPN software or utilize the Juniper/Pulse capability of OpenConnect, an open-source VPN program used by NetworkManager—the network control package used by most Linux distributions. We will limit ourselves to discussing the latter since the OpenConnect solution is more straightforward and better integrated into the Linux system.

Step by step instuction

1. If necessary install OpenConnect. Depending on your Linux distro you might need to install the OpenConnect software. Fedora 39 comes with it out of the box, while a bare Ubuntu 18 installation lacks the binaries.

   On rpm-based systems (Redhat EL, CentOS, SuSE) you would proceed as follows:

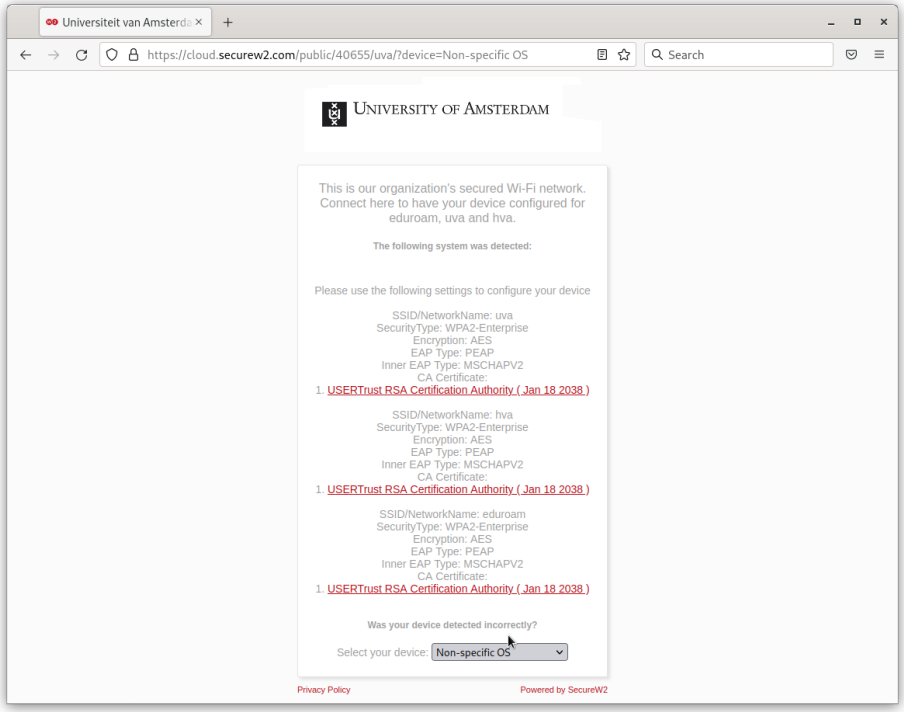
```
$ sudo yum -y install NetworkManager-openconnect-gnome
    (....)
$ sudo systemctl restart NetworkManager.service
```

For Debian-based systems (Debian, Ubuntu, etc.) issue the following commands:

```
$ sudo apt-get install network-manager-openconnect network-manager-openconnect-gnome
    (....)
$ sudo systemctl restart network-manager
$ sudo systemctl daemon-reload
```

Beware that this instruction is based on version 9.12 of OpenConnect and may not work on older versions.

2. Open https://cloud.securew2.com/public/40655/uva/?device=Non-specific OS in a web browser or alternatively go to `http://wifiportal.uva.nl` and under “Select your device:” choose “Non-specific OS” (obs. *not* “Linux”!). You should then see the following web page:



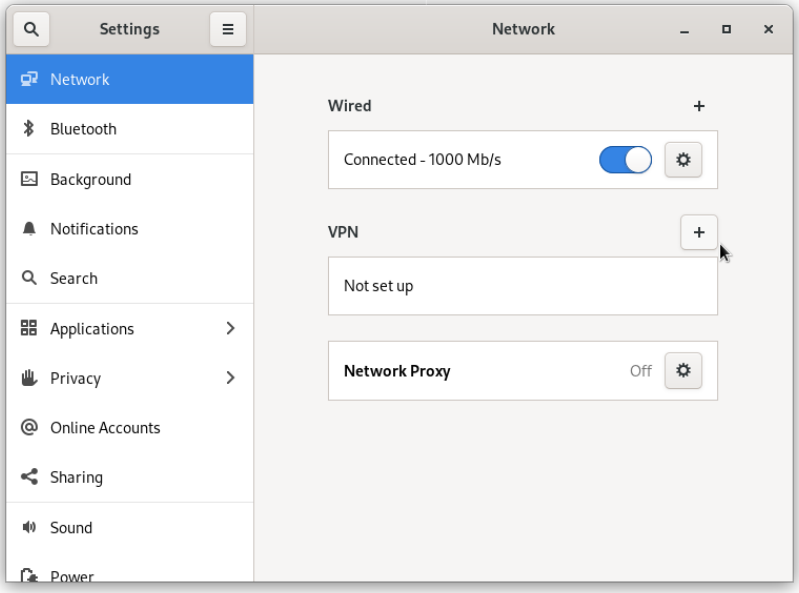
3. Download the file `usertrustrsaca [jdk].cer` under the top hyperlink USERTrust RSA Certification Authority (Jan 18 2038). Actually it does not matter which of the three displayed hyperlinks you choose as they all point to the same file.

4. Install the UvA root certificate in your computer's so-called "trust store". With Redhat-based systems, this goes as follows:

```
$ sudo cp usertrustrsaca\ [jdk].cer /etc/pki/ca-trust/source/anchors/
$ sudo update-ca-trust extract
```

On Debian-based systems the procedure is slightly different, notably the certificate first requires conversion.

```
$ openssl x509 -in usertrustrsaca\ \[jdk\].cer -out usertrustrsaca\ \[jdk\].crt
$ sudo cp usertrustrsaca\ [jdk].crt /usr/local/share/ca-certificates/
$ sudo update-ca-certificates
```



5. Open the network configuration panel from the system menu.

6. On the **VPN** row click on "**+**" to create a new VPN configuration.

   This will open a new window titled **Add VPN** and featuring a list of options.

7. Click option **Multi-protocol VPN client (openconnect)**.

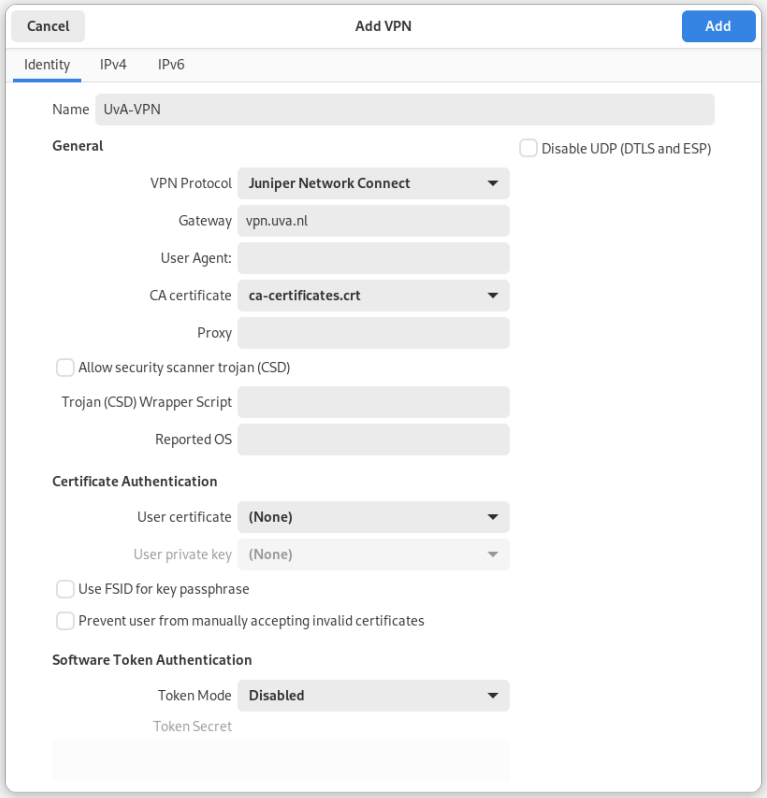
   This will open the configuration panel. The tab labled **Identity** will be displayed.

8. In the **Name** text box enter an appropriate name for the VPN configuration such as "`UvA-VPN`"

9. In the pop-up button labled **VPN Protocol** choose option **Juniper Network Connect**.

10. In the **Gateway** text box enter: `vpn.uva.nl`

11. In the pop-up button labled **CA certificate** choose option **Select from file...** to open the file selector.



12. Click **+ Other Locations** → **Computer** and browse the file system to the bundled CA certificate file. On Redhat-based systems follow the path `/etc/pki/ca-trust/extracted/pem/directory-hash` and select the file `ca-certificates.crt`. On Debian-based systems the same file is found under `/etc/ssl/certs`. All the remaining fields should be left unchanged.

13. Click the **Add** button at the top-right side of the window to save the new configuration.

    In the network configuration panel under **VPN** we will see a box symbolizing to the newly created configuration **UvA-VPN** (or whatever name you choose to give it).

14. In the **UvA-VPN** box toggle the switch to **ON**.

    This will open the login frame **Connect to VPN "UvA-VPN"**.

15. Enter your UvAnetID (in lowercase letters) and associated password.

16. Press Enter or click the **Login** button (*not* the **Connect** or **Close** button).

    Briefly the login frame will display **Connecting to host** and, if all went well, disappear uncovering the network configuration panel. The slide button for **UvA-VPN** will be set to **ON** indicating that your VPN connection to the UvA is up and running. An active VPN is also indicated by a padlock ( ) in the top bar.

17. This about sums it up for setting-up UvA VPN. You may now close the network configuration panel.

Usage

Disconnecting and reconnecting is done through the system menu (i.e. **VPN Off** → **Connect** and **UvA-VPN** → **Turn Off**). For each time you start UvA-VPN you will be presented the **Connect to VPN "UvA-VPN"** window asking you to enter your UvA password.
To make adjustments to the existing VPN configuration, or either to delete it, open the network configuration panel (NetworkManager) through the system menu and under **VPN** click the "cog" button (⚙) in the **UvA-VPN** box. The rest should be self-explanatory.