

Connecting Linux to the Secure UvA Networks (Wi-Fi and wired)

This instruction is intended for employees and students wishing to access the internet with their Linux computer through the secure networks of the University of Amsterdam (UvA). Section 1 explains connecting to the WiFi networks 'uva' and 'eduroam' and in section 2 the wired "Zelfsupport" network is discussed as well as the wired UvA congress LAN.

1 Setting up a connection to UvA Wi-Fi networks 'uva' and 'eduroam'

Throughout all of its buildings the University of Amsterdam offers employees and students access to two wireless (Wi-Fi) networks, designated 'uva' and 'eduroam', both accessible with a UvA account (UvAnetID or UvA student account). The eduroam Wi-Fi can also be unlocked with a non-UvA educational account or through the so-called Eduroam Visitor Access (eVA) which involves creating a efemeral guest account using your celular phone. In addition sometimes a publicly accessible Wi-Fi network is available named 'UvA Open Wi-Fi' save at Science Park where it is called 'Amsterdam Science Park'. The public network does not require authentication, but lacks security, is slow and does not give direct access to UvA's intranet. For this and other reasons UvA is gradually dismantling the public Wi-Fi in favor of eVA.

Aside from the network identifier (i.e. the SSID) the steps required to connect to uva and eduroam are identical. We recommend using the uva network since it is slightly less prone to failures than eduroam.

1.1 WPA Supplicant

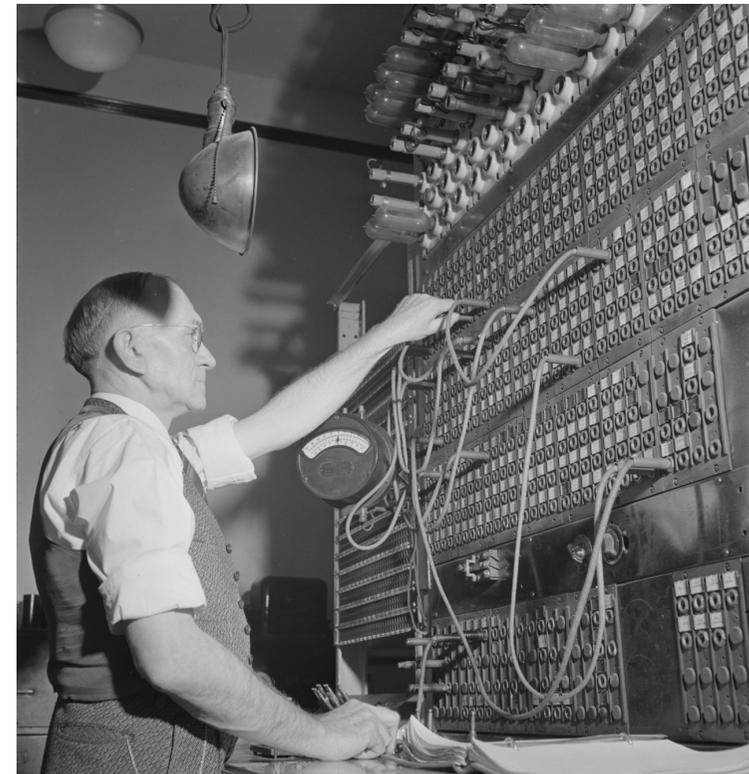
First make sure your computer has the package `wpa_supplicant` installed. On a RPM-based system (Redhat, SuSE, etc.) you would issue the following command in a terminal:

```
$ rpm -q wpa_supplicant
```

On APT-based systems (Debian, Ubuntu, etc.) the instruction would be:

```
$ dpkg -l wpasupplicant
```

If lacking please consult the documentation of your Linux distribution on how to install the software.



1.2 Parameters

All parameters needed by the network manager software to configure a connection to UvA's Wi-Fi networks are summed up in the following table.

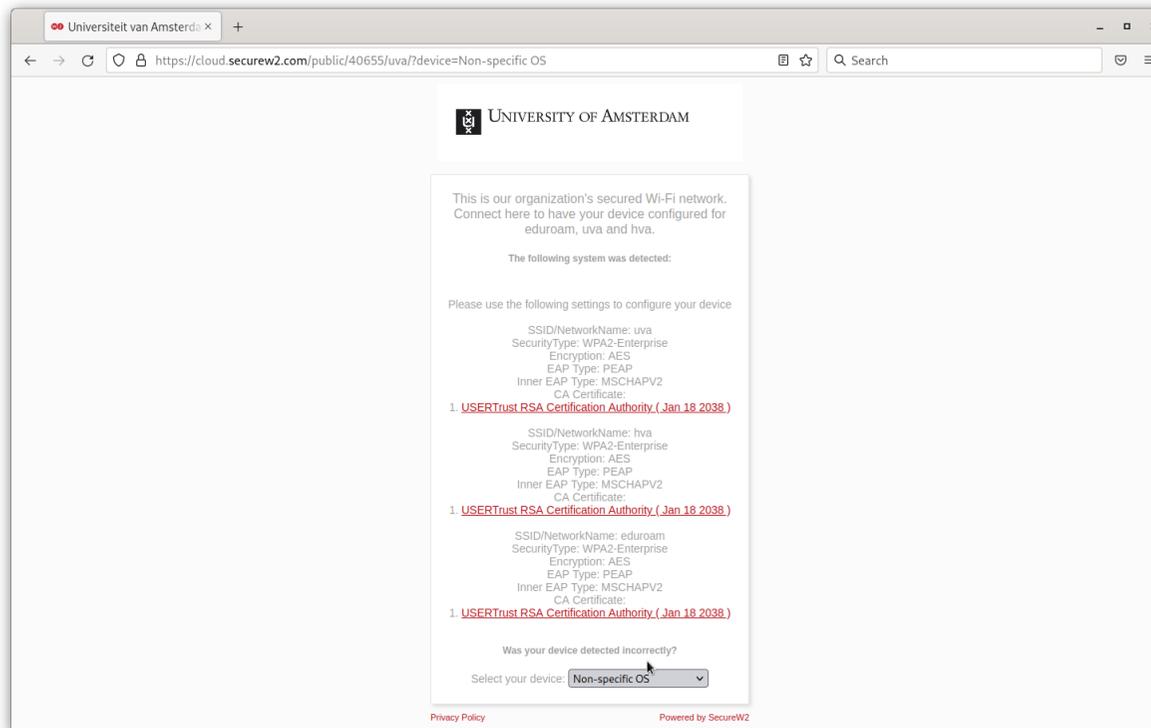
WiFi networks	
SSID:	<i>uva or eduroam</i>
Mode:	Infrastructure
IPv4 Settings:	Automatic (DHCP)
Wireless security:	WPA & WPA2 Enterprise
Authentication:	Protected EAP (PEAP)
Anonymous identity:	<i>anonymous@uva.nl</i>
Domain:	<i>uva.nl (see notes below)</i>
CA certificate:	<i>(see notes below)</i>
Inner authentication:	MSCHAPv2
Username:	<i>UvAnetID@uva.nl</i>
Password:	<i>associated with your UvAnetID</i>

Notes:

- The **Username** always includes a suffix specifying the institution the user account belongs to. For UvA employees this is their UvAnetID in lowercase letters followed by “@uva.nl”. Note that this is *not* the same as your e-mail address (e.g. *rmugabe1@uva.nl* and *not* *r.g.mugabe@uva.nl*.) If you enter “uva.nl” in the **Domain** field, appending “@uva.nl” to your UvAnetID is not required but won't hurt.
- Non-UvA accounts from eduroam-enabled institutions only have access through the *eduroam* network. Access to the *uva* Wi-Fi network is restricted to UvA accounts.
- A student's UvAnetID corresponds to his or her student number, making the Wi-Fi username string look something like *12345678@uva.nl*.
- ‘**CA certificate**’ refers to a little file containing information by which your computer can verify the authenticity of a corresponding network. This is to prevent a man-in-the-middle attack, a situation in which a third party falsely poses as the host we want to communicate with compromising ones password. The following section explains how to use UvA's certificate.

1.3 Downloading and Installing UvA's CA Certificate

UvA's CA Certificate can be downloaded from <http://wifiportal.uva.nl> under "Select your device:" choosing "Non-specific OS" (obs. *not* "Linux") as shown below.



The obvious problem is how to download UvA's CA certificate without using the Wi-Fi networks which require that same certificate. For this purpose the public Wi-Fi ('UvA Open Wi-Fi' or 'Amsterdam Science Park') comes in handy—if available. If not, you could choose to access eduroam through a temporary eVA guest account (with your celular phone browse to <https://eva.eduroam.nl> and follow the instructions there). Alternatively one could download the certificate with another computer and copy it by a USB stick.

From the WiFiportal page download the certificate file¹ specified as 'USERTrust RSA Certification Authority (Jan 18 2038)', (file name 'usertrustrsaca [jdk].cer'). You could choose to just leave the file somewhere in your home directory and point the network manager to it (with the risk of later accidentally deleting the file). We think it is more elegant to add the CA certificate to your computer's central trust store. This involves issuing a few commands through a command terminal so first open one (e.g. the **Terminal** application).

The procedure varies from Linux distro to Linux distro. With Redhat-based systems, as well as SuSE, issue the following commands:

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

After this we can safely remove the original files:

```
$ rm usertrustrsaca\ \[jdk\].cer
```

On Debian-based systems the UvA certificate first needs to be converted to PEM format. The commands are as follows:

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

Now we can safely remove the original files:

```
$ rm usertrustrsaca\ \[jdk\].cer usertrustrsaca\ \[jdk\].crt
```

In the network manager you can now specify the trust store location (the file in which all CA certificates are bundled). On Redhat-based systems this is /etc/pki/ca-trust/extracted/pem/directory-hash/ca-certificates.crt. On Debian-based systems the file is located at /etc/ssl/certs/ca-certificates.crt.

2 Setting up a connection to the wired Zelfsupport Network (VLAN 256)

For employees using a self-maintained (Zelfsupport) computer, UvA has created a separate wired virtual LAN, —VLAN 256— which is only accessible by authentication with a UvAnetID. The computer's MAC address has to be known to the DHCP server. For special occasions where people bring their non-UvA laptop computers, but where Wi-Fi access is inadequate (such as limited bandwidth, long network latency) UvA can activate UTP outlets in the walls patching them to the Wired UvAcongress Network: VLAN 18. This network is similar to VLAN 256 with the exception that the computer does not have to be registered

¹Note that it does not matter if you choose the hyperlink associated with SSID uva, hva or eduroam as they all point to the same certificate.

at UvA. In this sense it could be considered a “wired Wi-Fi” network. Another case in which VLAN 18 might be required is when a registered UvA laptop needs a wired connection but lacks an integrated UTP port. Solving this by connecting through a port replicator with UTP port or a UTP to USB adapter has as drawback that these devices use their own MAC address which for security reasons cannot be registered in the DHCP server. Before you can activate VLAN 256 or VLAN 18 the following requirements should be met:

- a network cable is present connecting your computer to a wall outlet (occasionally there might be a IP telephone chained in between).
- the wall outlet is active and connected to the Zelfsupport LAN (VLAN 256), or to the UvA congress LAN (VLAN 18).
- in the case of VLAN 256 (Zelfsupport LAN) the computer department (ICTS) should have correctly registered the mac address of your computer in the DHCP server.

All parameters relevant to setting up a connection to VLAN 256 and VLAN 18 are summed up in the following table.

VLAN 256 (Zelfsupport Network) / VLAN 18 (UvA congress network)	
IPv4 Settings:	Automatic (DHCP)
802.1x Security:	<i>On</i>
Authentication:	Protected EAP (PEAP)
PEAP version:	Automatic
Anonymous identity:	<i>anonymous@uva.nl</i>
CA certificate:	<i>optional; see notes below</i>
Inner authentication:	MSCHAPv2
Username:	<i>UvAnetID@uva.nl</i>
Password:	<i>the one associated with your UvAnetID</i>

Notes:

- The **Username** is your UvAnetID in lowercase letters, followed by @uva.nl (e.g. rmugabe1@uva.nl). Note that the string is *not* the same as your e-mail address (e.g. rmugabe1@uva.nl and *not* r.g.mugabe@uva.nl.)
- ‘**CA certificate**’ asks for a file with information by which your computer can verify the authenticity of the 802.1x network. Since we are dealing with a wired connection the chance of a man-in-the-middle attack, a situation in which a third party falsely poses as a UvA server, is quite small. So therefore we choose to leave this field empty and check the **No CA certificate is required** box. We nonetheless recommend installing the UvA CA certificate as explained in subsection [1.3](#)