

## Linux aansluiten op de beveiligde UvA-netwerken (WiFi of bedraad)

Deze tekst legt beknopt uit hoe men op een computer die Linux draait toegang krijgt tot de beveiligde netwerken van de UvA. In sectie 1 bespreken we de WiFi-netten 'uva' en 'eduroam', sectie 2 gaat over het bedrade Zelfsupport-net (VLAN 256) en het UvA-congresLAN (VLAN 18).

### 1 Verbinding opzetten met WiFi-netwerken 'uva' en 'eduroam'

De Universiteit van Amsterdam biedt de medewerkers en studenten in al haar gebouwen toegang tot twee verschillende draadloze netwerken aan genaamd 'uva' en 'eduroam'. Daarnaast is er op elke locatie een publiek netwerk beschikbaar 'UvA Open Wi-Fi' genaamd behalve op Science Park waar dit 'Amsterdam Science Park' heet. Het publieke netwerk vereist geen authenticatie maar is onbeveiligd, langzaam en staat afgesloten van het intranet. Gebruik het alleen wanneer het niet anders kan. Verbinding maken met het publieke netwerk wijst zichzelf en wordt hier niet besproken.

De procedures om uva en eduroam te configureren zijn identiek. Voor oudere hardware geldt mogelijk dat het nieuwere WiFi-protocol dat op 5 GHz communiceert niet wordt ondersteund. Oude netwerkkaarten werken op 2,4 GHz en zullen het uva-netwerk niet waarnemen maar alleen eduroam (dat op beide frequentiebanden 2,4 GHz en 5 GHz uitzendt). Aangezien, in tegenstelling tot het uva-netwerk, de authenticatie bij eduroam via een externe partij loopt raden we mensen met een UvAnetID aan, waar mogelijk, uva te gebruiken.

#### 1.1 WPA Supplicant

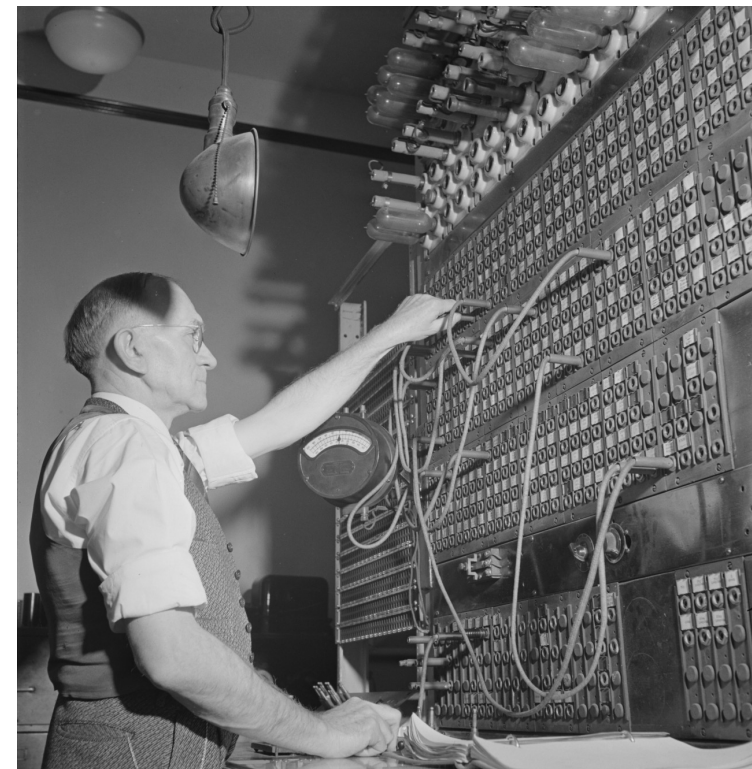
Stel eerst vast dat het pakket `wpa_supplicant` op uw computer aanwezig is. Op een RPM-gebaseerd systeem (Redhat, SuSE, enz.) kunt u dat doen door bijv. in een terminal het volgende commando te geven:

```
$ sudo rpm -q wpa_supplicant
```

Op APT-gebaseerde systemen (Debian, Ubuntu enz.) luidt het commando:

```
$ sudo dpkg -l wpasupplicant
```

Indien `wpa_supplicant` ontbreekt dan moet u deze via een alternatieve internetverbinding zien te verkrijgen. Voor de details verwijzen wij u naar de handleiding van uw Linux-distributie.



## 1.2 Parameters

Alle benodigde parameters voor het verbinding maken met de draadloze netwerken worden in de onderstaande tabel opgesomd.

WiFi-netwerken	
SSID:	uva of eduroam
Mode:	Infrastructure
IPv4 Settings:	Automatic (DHCP)
Wireless security:	WPA & WPA2 Enterprise
Authentication:	Protected EAP (PEAP)
Anonymous identity:	anonymous@uva.nl
Domain:	uva.nl (zie onderstaande toelichting)
CA certificate:	(zie onderstaande toelichting)
Inner authentication:	MSCHAPv2
Username:	UvAnetID@uva.nl
Password:	wachtwoord van uw UvAnetID

Toelichting:

- Voer uw UvAnetID in kleine letters in.
- Het domein van uw gebruikersaccount (@uva.nl) dient vermeld te worden, dan wel in een apart veld, of als achtervoegsel van uw UvAnetID gescheiden door een apostrof (@), d.w.z. *UvAnetID@uva.nl*
- Authenticatie met externe Eduroam-accounts (bijv. VUnetID) werkt ook, maar uitsluiten op het eduroam-netwerk. Het domein moet overeenkomen met de beheerder van het account.
- Voor studenten geldt dat het UvAnetID gelijk is aan hun collegekaartnummer.
- Het veld '**CA certificate**' vraagt om een kleine file met informatie waarmee uw computer de authenticiteit van een desbetreffend netwerk kan verifiëren. Hiermee voorkomt u een zg. *man-in-the-middle attack*, de situatie waarin een derde partij zich valselyk voordoet als de authentieke server. U dient het certificaat natuurlijk op te halen via een ander kanaal, ofwel downloaden na eerst verbinding te maken met het publieke netwerk (UvA Open Wi-Fi of Amsterdam Science Park) of vanaf een andere computer. U vindt het certificaat door op pagina <http://wifiportal.uva.nl> onder "Select your device:" de optie "Non-specific OS" te selecteren (let op: *niet* "Linux"). Download de file `usertrustrsaca [jdk].cer` vanaf de bovenste link [USERTrust RSA Certification Authority \(Jan 18 2038\)](#). U kunt het certificaat in uw home-directory laten en de configuratie ernaar laten verwijzen, maar we raden aan het op te slaan in de centrale "trust store" van uw systeem. Hiermee regelt het besturingssysteem zelf het gebruik van het UvA-certificaat en kunt u voortaan het veld **CA certificate** leeg laten. Als u gebruik wilt gaan maken van UvA-VPN dan zal Linux gebruik maken van hetzelfde in de trust-store opgeslagen UvA-certificaat.

Het gedownloade UvA-certificaat installeren in de trust-store gaat voor de verschillende Linux-distributies een beetje anders. Open een commando-venster zoals **Terminal**.

Bij de Redhat-familie zijn de commando's als volgt:

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

Bij op Debian gebaseerde distributies gaat het zo:

```
$ openssl x509 -in usertrustsaca\ [jdk].cer -outform PEM -out usertrustsaca\ [jdk].cert  
$ sudo cp usertrustsaca\ [jdk].cert /usr/local/share/ca-certificates/  
$ sudo update-ca-certificates
```

Bij SuSE zo:

```
$ openssl x509 -in usertrustsaca\ [jdk].cer -outform PEM -out usertrustsaca\ [jdk].cert  
$ sudo cp usertrustsaca\ [jdk].cert /etc/pki/trust/anchors/  
$ sudo update-ca-certificates
```

Voor andere Linux-versies verwijzen wij u naar de desbetreffende documentatie. Na afloop kunt u de .cer- en .cert-bestanden in uw home weggooien. Zoals gezegd, wanneer u nu de netwerkparameters invult vinkt u gewoon de optie **“No CA certificate is required”** aan.

## 2 Verbinding opzetten met het bedrade Zelfsupport-netwerk (VLAN 256)

Speciaal voor gebruikers van een eigen-beheerde computer die van een bedraad LAN willen gebruik maken heeft de UvA een speciaal netwerk in het leven geroepen: het Zelfsupport-netwerk of VLAN 256. Net als bij de beveiligde WiFi-netwerken moet de gebruiker zich eerst authenticeren met zijn UvAnetID voordat de verbinding bruikbaar wordt.

Naast VLAN 256 heeft de UvA nog een beveiligd bedraad netwerk: het UvA-congresnet of VLAN 18. Dit LAN wordt ook wel 'laptopnet' of schertsend 'draadloos-met-een-draadje' genoemd. VLAN 18 wordt vooral ingezet bij bijeenkomsten waar niet-UvA laptops worden gebruikt, maar waarvoor de WiFi-netten te traag of onbetrouwbaar zijn. Het voornaamste verschil tussen het congresnet en het Zelfsupportnet is dat bij het congresnet het mac-adres van de computer niet bij de DHCP-server bekend hoeft te zijn. Vanuit het oogpunt van de gebruiker zijn beide LANs identiek.

Om een verbinding op te zetten met het Zelfsupport-netwerk of UvA congresnet moet aan de volgende voorwaarden voldaan zijn:

- er loopt een netwerkkabel tussen uw computer en een wall-outlet (eventueel bevindt zich tussen de computer en de outlet nog een IP-telefoon).
- de wall-outlet is aangesloten op een netwerkswitch (wij zeggen 'gepatcht') en de aansluiting is geconfigureerd voor het Zelfsupport-netwerk (VLAN 256) of het UvA-congresnet (VLAN 18).
- in het geval van Zelfsupport heeft de ICTS het mac-adres van uw computers ethernetkaart correct ingevoerd in de DHCP-server.

Alle benodigde parameters voor het verbinding maken met het Zelfsupport-netwerk of UvA-congresnet worden in de tabel opgesomd:

Zelfsupport-netwerk / UvA-congresnet	
IPv4 Settings:	Automatic (DHCP)
802.1x Security:	<i>Aan</i>
Authentication:	Protected EAP (PEAP)
PEAP version:	Automatic
Anonymous identity:	<i>anonymous@uva.nl</i>
CA certificate:	<i>niet verplicht</i>
Inner authentication:	MSCHAPv2
Username:	<i>UvAnetID@uva.nl</i>
Password:	<i>wachtwoord van uw UvAnetID</i>

Toelichting:

- De in te vullen gebruikersnaam (**Username**) is uw UvAnetID (in kleine letters) gevolgd door "@uva.nl". Dit achtervoegsel wordt vaak vergeten. Bedenk ook dat het hier niet uw e-mailadres betreft.
- Het veld '**CA certificate**' vraagt om een kleine file met informatie waarmee uw computer de authenticiteit van een desbetreffend netwerk kan verifiëren. Hiermee voorkomt u een zg. *man-in-the-middle attack*, de situatie waarin een derde partij zich valselijk voordoe als de authentieke UvA-server. Dit is voor WiFi erg belangrijk, maar voor bedrade netwerken minder relevant. Wij kiezen er hier voor het veld blanco te laten. Zie evt. de uitleg onder sectie 1.