Raspberry Pi on eduroam Wifi Network

eduroam Info

SSID: eduroam
Security Type: WPA2-Enterprise
Encryption Type: AES (CCMP)
EAP Method: EAP-TLS (or TLS)
Root CA Certificate(s): University of New Hampshire Root CA I
Server Name: cloudpath.unh.edu
Client Certificate: <UNH username>@cpuser.unh.edu
Username: <UNH Username>@cpuser.unh.edu

* Labels on fields will differ based on the operating system.

1. Configuring /etc/wpa_supplicant/wpa_supplicant.config

1. Backup the default wpa_supplicant.config
2. Open the file and remove any other SSID's that may be defined
1. A full example config is below:

```
# wpa-supplicant.config
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
country=US

network={
	ssid="eduroam"
	proto=RSN
	key_mgmt=WPA-EAP
	pairwise=CCMP
	group=CCMP
	eap=TLS
	identity="<UNH Username>@cpuser.unh.edu"
	ca_cert="/etc/cert/CA-6A0E76B9655601F8F18DD7A8CAB6831324C69D0C.pem"
	client_cert="/etc/cert/certificate.pem"
	private_key="/etc/cert/certificate.key"
	private_key_passwd="<password from step 3 below>"
```

```
    priority=1
}
```

2. Configuring /etc/network/interfaces

1. backup the default /etc/network/interfaces file

1. open and setup your interfaces file using the example below

```
# /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)

# Please note that this file is written to be used with dhcpcd
# For static IP, consult /etc/dhcpcd.conf and 'man dhcpcd.conf'

# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d

auto lo
iface lo inet loopback
iface eth0 inet manual

allow-hotplug wlan0
iface wlan0 inet dhcp
  wpa-ssid eduroam
  pre-up wpa_supplicant -dd -B -Dwext -i wlan0 -c/etc/wpa_supplicant/wpa_supplicant.conf -f
/var/log/wpa_supplicant.log
  wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf

#allow-hotplug wlan1
#iface wlan1 inet manual
#   wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
```

3. Create the certificates:

1. Open your browser and connect to cloudpath.unh.edu

1. accepts the "Acceptable Use Policy" at the bottom and click start

2. Select Faculty, Staff, and Students

3. Log in using your UNH username and password
4. Select "Show All Operating Systems"
5. Select "Other Operating System"
2. download the CA certificate by selecting the PEM format link under Step 1.
3. download the client certificate.p12 file to split into a cert and key format
1. extract the crt as a pem file:
1. openssl pkcs12 -in client-certificate.p12 -out user.pem -nodes
2. extract the key:
1. openssl pkcs12 -in client-certificate.p12 -out user.key -nocerts
2. The first prompt for a password is for your UNH email password
3. The second prompt for a password is the password you want to use to encrypt the extracted key.
4. do not make the new password the same as your UNH password as it will be stored in the wpa_supplicant.conf file
4. Create the directory /etc/cert
5. Copy user.pem, user.key, and CA-[long series of characters].pem to /etc/cert

4. Restart networking

There are two ways to do this.

1. Method 1 - Run the following commands
1. sudo killall wpa_supplicant
1. Alternatively, run 'ps aux | grep wpa_supplicant', and use the resulting PID number for the process as the argument to 'sudo kill -9 <PID>'
2. sudo rm -f /var/run/wpa_supplicant/*

3. sudo service daemon-reload
4. sudo service networking restart

2. Method 2 - Reboot