

Thermo Scientific™ DeviceLink™ Connect Advanced Network Configuration Setup

Excerpt taken from DeviceLink Connect Configuration and Installation Instruction Guide

For more information regarding 802.1x, please reference official WPA Supplicant docs available at https://w1.fi/wpa_supplicant/

1. For networks that require 802.1x security authentication, set Advanced Mode to “Enabled” in the DeviceLink Connect Commissioner Application (Wi-Fi tab)

The screenshot shows the 'Configure WiFi' interface. At the top, a red banner states 'The wifi network is currently down...'. The left sidebar is dark blue with a navigation menu including 'Offline', 'Welcome', 'WiFi', 'Cloud', 'NTP', 'DHCP', 'Sensors', 'Calibration', 'Multidrop', 'DeviceLink', 'Quality Control', 'Logs', 'Save & Restore', 'User Profile', and 'Logout'. The main content area has a blue header 'Configure WiFi'. Below it, the 'Advanced Mode' dropdown is set to 'Disabled' and is highlighted with a red box. The 'Authentication' dropdown is set to 'WPA'. The 'Network' text input field contains 'motes-wifi'. Below this is a note: 'Use the box on the right to scan for available WiFi networks in the area and select the appropriate network.' The 'Password' field is masked with dots and has an eye icon. To the right, a 'Networks' panel shows a list of detected networks with 'Select' buttons next to each. At the bottom of the panel is a 'Scan WiFi Networks' button. A blue 'Submit' button is located at the bottom center of the configuration area.

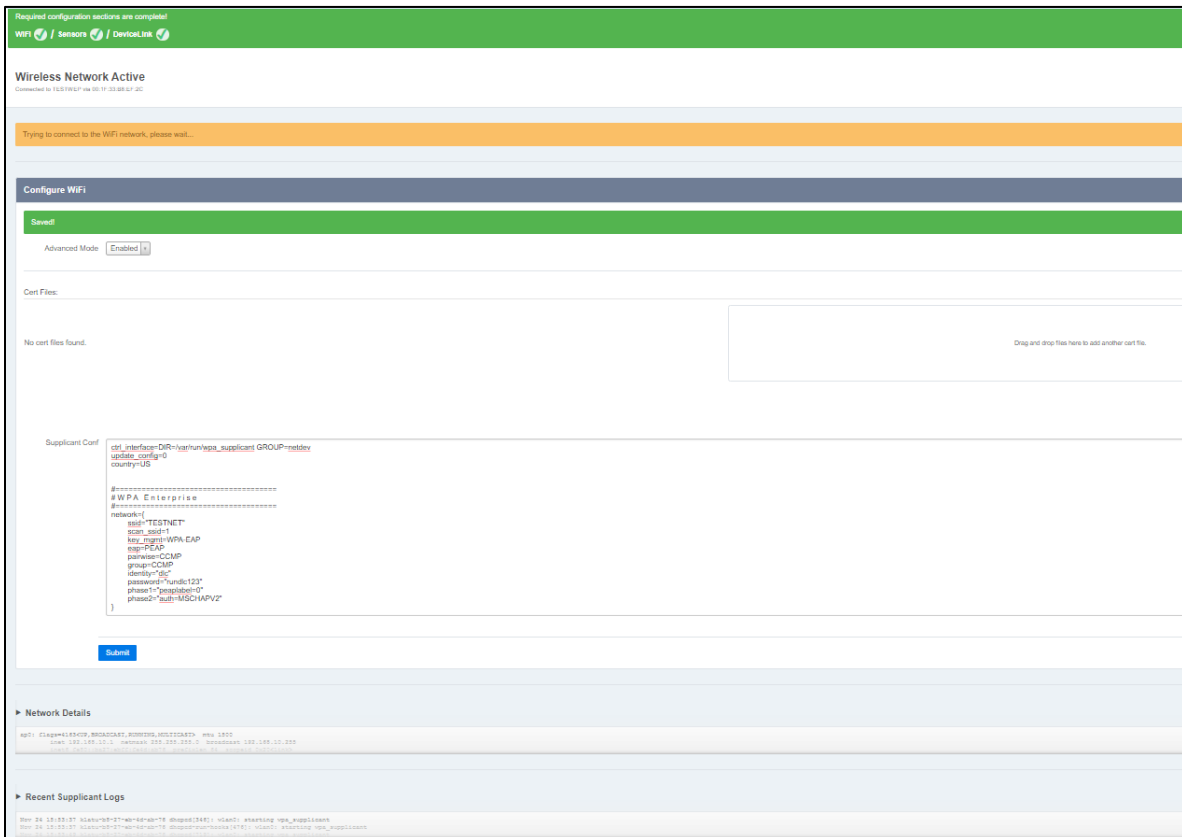
2. If the network requires 802.1x, then:

- Certificates can be uploaded. Use the Drag/Drop box to add a certificate file.
- The WPA Supplicant configuration can be edited in the “Supplicant Conf” box.

Example Enterprise Supplicant Script:

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=0
country=US
```

```
#=====
# WPA Enterprise
#=====
network={
  ssid="ENTER-SSID-HERE"
  scan_ssid=1
  key_mgmt=WPA-EAP
  eap=PEAP
  pairwise=CCMP
  group=CCMP
  identity="ENTER-USERNAME-HERE"
  password="ENTER-PASSWORD-HERE"
  phase1="peaplabel=0"
  phase2="auth=MSCHAPV2"
```



3. Supported WPA/IEEE 802.11i features:

- WPA2-PSK
- WPA with EAP (e.g., with RADIUS authentication server) (“WPA-Enterprise”)
- Key management for CCMP and TKIP
- WPA and full IEEE 802.11i/RSN/WPA2
- RSN: PMKSA caching, pre-authentication
- IEEE 802.11r
- IEEE 802.11w
- Wi-Fi Protected Setup (WPS)

4. Supported EAP methods (IEEE 802 Supplicant):

- EAP-TLS
- EAP-PEAP/MSCHAPv2 (both PEAPv0 and PEAPv1)
- EAP-PEAP/TLS (both PEAPv0 and PEAPv1)
- EAP-PEAP/GTC (both PEAPv0 and PEAPv1)
- EAP-PEAP/OTP (both PEAPv0 and PEAPv1)
- EAP-PEAP/MD5-Challenge (both PEAPv0 and PEAPv1)
- EAP-TTLS/EAP-MD5-Challenge
- EAP-TTLS/EAP-GTC
- EAP-TTLS/EAP-OTP
- EAP-TTLS/EAP-MSCHAPv2
- EAP-TTLS/EAP-TLS
- EAP-TTLS/MSCHAPv2
- EAP-TTLS/MSCHAP
- EAP-TTLS/PAP
- EAP-TTLS/CHAP
- EAP-SIM
- EAP-AKA
- EAP-AKA'
- EAP-PSK
- EAP-FAST
- EAP-PAX
- EAP-SAKE
- EAP-IKEv2
- EAP-GPSK