Rocky Enterprise Linux 9.2 Manual Pages on command 'wpa_supplicant.conf.5'

C:\>man wpa_supplicant.conf.5

WPA_SUPPLICANT.CONF(5) WPA_SUPPLICANT.CONF(5)

NAME

wpa_supplicant.conf - configuration file for wpa_supplicant

OVERVIEW

wpa_supplicant is configured using a text file that lists all accepted networks and security policies, including pre-shared keys. See the example configuration file, probably in /usr/share/doc/wpa_supplicant/, for detailed information about the con? figuration format and supported fields.

All file paths in this configuration file should use full (absolute, not relative to working directory) path in order to allow working directory to be changed. This can happen if wpa_supplicant is run in the background.

Changes to configuration file can be reloaded be sending SIGHUP signal to wpa_sup? plicant ('killall -HUP wpa_supplicant'). Similarly, reloading can be triggered with the wpa_cli reconfigure command.

Configuration file can include one or more network blocks, e.g., one for each used SSID. wpa_supplicant will automatically select the best network based on the order of network blocks in the configuration file, network security level (WPA/WPA2 is preferred), and signal strength.

QUICK EXAMPLES

1. WPA-Personal (PSK) as home network and WPA-Enterprise with EAP-TLS as work net? work.

allow frontend (e.g., wpa_cli) to be used by all users in 'wheel' group

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=wheel
#
# home network; allow all valid ciphers
network={
    ssid="home"
    scan_ssid=1
    key_mgmt=WPA-PSK
    psk="very secret passphrase"
}
#
# work network; use EAP-TLS with WPA; allow only CCMP and TKIP ciphers
network={
    ssid="work"
    scan_ssid=1
    key_mgmt=WPA-EAP
    pairwise=CCMP TKIP
    group=CCMP TKIP
    eap=TLS
    identity="user@example.com"
    ca_cert="/etc/cert/ca.pem"
    client_cert="/etc/cert/user.pem"
    private_key="/etc/cert/user.prv"
    private_key_passwd="password"
}
```

2. WPA-RADIUS/EAP-PEAP/MSCHAPv2 with RADIUS servers that use old peaplabel (e.g., Funk Odyssey and SBR, Meetinghouse Aegis, Interlink RAD-Series)

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=wheel
network={
    ssid="example"
    scan_ssid=1
    key_mgmt=WPA-EAP
    eap=PEAP
    identity="user@example.com"
```

password="foobar"

ca_cert="/etc/cert/ca.pem"

phase1="peaplabel=0"

phase2="auth=MSCHAPV2"

}

3. EAP-TTLS/EAP-MD5-Challenge configuration with anonymous identity for the unen?

crypted use. Real identity is sent only within an encrypted TLS tunnel.

ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=wheel

network={

ssid="example"

scan_ssid=1

key_mgmt=WPA-EAP

eap=TTLS

identity="user@example.com"

anonymous_identity="anonymous@example.com"

password="foobar"

ca_cert="/etc/cert/ca.pem"

phase2="auth=MD5"

}

4. IEEE 802.1X (i.e., no WPA) with dynamic WEP keys (require both unicast and

broadcast); use EAP-TLS for authentication

ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=wheel

network={

ssid="1x-test"

scan_ssid=1

key_mgmt=IEEE8021X

eap=TLS

identity="user@example.com"

ca_cert="/etc/cert/ca.pem"

client_cert="/etc/cert/user.pem"

private_key="/etc/cert/user.prv"

private_key_passwd="password"

eapol_flags=3

```
}
```

5. Catch all example that allows more or less all configuration modes. The configu?
ration options are used based on what security policy is used in the selected
SSID. This is mostly for testing and is not recommended for normal use.

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=wheel
network={
    ssid="example"
    scan_ssid=1
    key_mgmt=WPA-EAP WPA-PSK IEEE8021X NONE
    pairwise=CCMP TKIP
    group=CCMP TKIP WEP104 WEP40
    psk="very secret passphrase"
    eap=TTLS PEAP TLS
    identity="user@example.com"
    password="foobar"
    ca_cert="/etc/cert/ca.pem"
    client_cert="/etc/cert/user.pem"
    private_key="/etc/cert/user.prv"
    private_key_passwd="password"
    phase1="peaplabel=0"
    ca_cert2="/etc/cert/ca2.pem"
    client_cert2="/etc/cer/user.pem"
    private_key2="/etc/cer/user.prv"
    private_key2_passwd="password"
}
```

6. Authentication for wired Ethernet. This can be used with wired or roboswitch in?
terface (-Dwired or -Droboswitch on command line).

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=wheel
ap_scan=0
network={
    key_mgmt=IEEE8021X
    eap=MD5
    identity="user"
```

```
        password="password"
        eapol_flags=0
    }
```

CERTIFICATES

Some EAP authentication methods require use of certificates. EAP-TLS uses both server side and client certificates whereas EAP-PEAP and EAP-TTLS only require the server side certificate. When client certificate is used, a matching private key file has to also be included in configuration. If the private key uses a passphrase, this has to be configured in wpa_supplicant.conf ("private_key_passwd").

wpa_supplicant supports X.509 certificates in PEM and DER formats. User certificate and private key can be included in the same file.

If the user certificate and private key is received in PKCS#12/PFX format, they need to be converted to suitable PEM/DER format for wpa_supplicant. This can be done, e.g., with following commands:

```
    # convert client certificate and private key to PEM format
    openssl pkcs12 -in example.pfx -out user.pem -clcerts
    # convert CA certificate (if included in PFX file) to PEM format
    openssl pkcs12 -in example.pfx -out ca.pem -cacerts -nokeys
```

SEE ALSO

wpa_supplicant(8) openssl(1)