Quick Start Guide for WPA3

Contents

Introduction

The next generation of Wi-Fi® security, bringing new capabilities to enhance Wi-Fi protections in personal and enterprise networks.:

- **WPA3-Personal (WPA3-SAE):**
  more resilient, password-based authentication even when users choose passwords that fall short of typical complexity recommendations. WPA3 leverages Simultaneous Authentication of Equals (SAE), a secure key establishment protocol between devices, to provide stronger protections for users against password guessing attempts by third parties.
- **WPA3-Enterprise (192-bit Mode/Suite B):**
  offers the equivalent of 192-bit cryptographic strength, providing additional protections for networks transmitting sensitive data, such as government or finance. The 192-bit security suite ensures a consistent combination of cryptographic tools are deployed across WPA3 networks.

1. WPA3-Peresonal Required for RTK driver

A. Linux Kernel Version
   a. Available for WPA3-Personal Station above kernel v4.17. If kernel version below v4.17, you can choose patch[1] kernel or use RTK maintain's hostapd/wpa_supplicant.
   b. Available for WPA3-Personal SoftAP above kernel v5.1. If kernel version below v5.1, you can choose patch[2] kernel or use RTK maintain's hostapd/wpa_supplicant.
   c. If you use the RTK maintain's hostapd/wpa_supplicant, it can available above kernel v3.8.

B. Realtek Linux Driver Version
   a. Available for WPA3-Personal Station/SoftAP above driver v5.8.

[1] Support offloading wireless authentication to userspace via NL80211_CMD_EXTERNAL_AUTH
[2] Authentication offload to user space in AP mode

C. RTK maintain's hostapd/wpa_supplicant Version

a. For Pure Linux, you have to use version wpa_supplicant_8_O_8x_rtw[3] above the patch 6.

b. For Android system, please contact the FAE.

2. WPA3-Enterpris Required for RTK driver

A. Linux Kernel Version

a. The mandatory as WPA-3-Personal Required.

b. The optional Suite-B/192-Bit as WPA-3-Personal Required.

B. Realtek Linux Driver Version

a. The mandatory, Station/SoftAP above driver v5.8.

b. The optional Suite-B/192-Bit, Station/SoftAP above driver v5.10.

i. Hardware have to supported crypto cipher GCMP_256 and BIP_GMAC_256

3. Start the WPA3-Personal

A. For further information about wpa_cli and wpa_supplicant, please refer to: document/wpa_cli_with_wpa_supplicant.pdf.

You have to enable below settings when build wpa_supplicant.

```
CONFIG_TLS=openssl
CONFIG_IEEE80211W=y
CONFIG_SAE=y
```

You can scan two kind of WPA3 Access Points.

a. **WPA3-SAE mode:**

Only WPA3-SAE station can connect.

```
bssid / frequency / signal level / flags / ssid
00:11:22:33:44:21   2432   -37      [WPA2-SAE-CCMP][WPS][ESS]  WPA3-
AP
```

b. **WPA3-SAE Transition Mode:**

WPA2-PSK and WPA3-SAE station can connect.

```
bssid / frequency / signal level / flags / ssid
00:11:22:33:44:21   2432   -37  [WPA2-PSK+SAE-CCMP][WPS][ESS]  WPA3-
AP
```

You can use the same configuration to connect both Access Point.

The sample configuration as:

[3] wpa_supplicant_8_O_8.x_rtw-6-g8c4af17fe.20200221.tar.gz.

```
ctrl_interface=/var/run/wpa_supplicant
network={
      ssid="WPA3-AP"
      key_mgmt=SAE
      psk="87654321"
      ieee80211w=2
}
```

B. For further information about hostapd_cli and hostapd, please refer to: document/Quick_Start_Guide_for_SoftAP.pdf.

You have to enable below settings when build hostapd.

```
CONFIG_TLS=openssl
CONFIG_IEEE80211W=y
CONFIG_SAE=y
```

You can setup the WPA3 SoftAP as:

a. **WPA3-SAE mode:**

There are three setting you have to configure as:

```
auth_algs=3
ieee80211w=2
wpa_key_mgmt=SAE
```

b. WPA3-SAE Transition Mode:

There are four setting you have to configure as:

```
auth_algs=3
ieee80211w=1
sae_require_mfp=1
wpa_key_mgmt=SAE WPA-PSK
```

The sample configuration:

```
ctrl_interface=/var/run/hostapd
interface=wlan0
driver=nl80211
ssid=WPA3-SAE
channel=1
beacon_int=100
hw_mode=g
ieee80211w=1
auth_algs=3
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase=87654321
wpa_key_mgmt=SAE WPA-PSK
sae_require_mfp=1
wpa_pairwise=CCMP
rsn_pairwise=CCMP
max_num_sta=16
wmm_enabled=1
```

4. Start the WPA3-Enterprise

A. For further information about wpa_cli and wpa_supplicant, please refer to: document/wpa_cli_with_wpa_supplicant.pdf.

You have to enable below settings when build wpa_supplicant.

```
CONFIG_TLS=openssl
CONFIG_IEEE80211W=y
CONFIG_SAE=y
CONFIG_SUITEB192=y
```

You can use the configuration to connect Access Point.

The sample configuration as:

```
network={
 ssid="WPA3ENTERPRISE"
 key_mgmt=WPA-EAP-SUITE-B-192
 pairwise=GCMP-256
 group=GCMP-256
 eap=TLS
 identity="Client Certificate IDL"
 ca_cert="./ec2-ca.pem"
 client_cert="./ec2-user.pem"
 private_key="./ec2-user.pem"
 private_key_passwd="wifi"
 openssl_ciphers="ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256"
 ieee80211w=2
}
```

B. For further information about hostapd_cli and hostapd, please refer to: document/Quick_Start_Guide_for_SoftAP.pdf.

You have to enable below settings when build hostapd.

```
CONFIG_TLS=openssl
CONFIG_IEEE80211W=y
CONFIG_SAE=y
CONFIG_SUITEB192=y
```

You can setup the WPA3 SoftAP as:

The sample configuration as:

```
interface=wlan0
driver=nl80211
ssid=WPA3ENTERPRISE
wpa=2
wpa_key_mgmt=WPA-EAP-SUITE-B-192
wpa_pairwise=GCMP-256
group_cipher=GCMP-256
group_mgmt_cipher=BIP-GMAC-256
ieee80211w=2
sae_anti_clogging_threshold=0
ieee8021x=1
eapol_version=2

# RADIUS authentication server
auth_server_addr=192.168.10.10
auth_server_port=1812
auth_server_shared_secret=12345678
```

5. Document revision history

Version	Date YYYY-MM-DD	Remarks
1.0	2018-05-28	Initial release
1.1	2020-02-20	1. Add Enterprise parts. 2. Update last support rtw_wpa_supplicant version. 8_O_8.x_rtw-6-g8c4af17fe