

Quick Start Guide for WPA3

Contents

| | |
|---|----------|
| Introduction..... | 1 |
| 1. WPA3-Peresonal Required for RTK driver..... | 1 |
| 2. WPA3-Enterpris Required for RTK driver..... | 2 |
| 3. Start the WPA3-Personal..... | 2 |
| 4. Start the WPA3-Enterprise..... | 4 |
| 5. Document revision history..... | 5 |

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

You can use official wpa_supplicant version must be greater than v2.8 or use wpa_supplicant that we provided in our software release packages.

A. Linux Kernel Version and wpa_supplicant

- a. Available for WPA3-Personal Station **above kernel v4.17**. If kernel version below v4.17, you shall merge patch¹ to kernel.
- b. Available for WPA3-Personal SoftAP **above kernel v5.1**. If kernel version below v5.1, you shall merge patch² to kernel.

¹ Support offloading wireless authentication to userspace via NL80211_CMD_EXTERNAL_AUTH
<https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=40cbfa90218bc570a7959b436b9d48a18c361041>
<https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=10773a7c09b327d02144c7d181e6544b7015ffc7>
<https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=db8d93a7a355121d49777c059afbca23c53c8628>

² Authentication offload to user space in AP mode

- c. You need to add patch³ to fix bug if you use wpa_supplicant v2.9. Also, you need to define **CONFIG_KERNEL_PATCH_EXTERNAL_AUTH** flag in driver.
- d. You shall use wpa_supplicant that we provided in our software release packages if you are not able to patch your system kernel.
- e. If your system kernel version is newer than v3.8, the WPA3-Personal functionality can work fine by using RTK version of hostapd/wpa_supplicant.

B. Realtek Linux Driver Version

- a. Available for WPA3-Personal Station/SoftAP above driver v5.8.

C. RTK maintain's hostapd/wpa_supplicant Version

- a. For Pure Linux, you have to use version wpa_supplicant_8_O_8x_rtw⁴ 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.

<https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=fe4943702c850fa07f963eaa6f1530d9d4c2da78>

³ Fix send_mlme for SAE external auth

<http://w1.fi/cgiit/hostap/commit/?id=aad414e956fdb463d3b45eb61c42792bf0c9f558>

⁴ wpa_supplicant_8_O_8.x_rtw-6-g8c4af17fe.20200221.tar.gz.

```
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:

```
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 |
| 1.2 | 2021-12-15 | 1. Update the instructions for wpa_wuppllicant in WPA3. |