Setting up WPA3

Goal: To set up LANforge wireless access points and clients with WPA3.

This example will cover WPA3-Personal, WPA3-Enterprise and OWE. For an introduction or review of WPA3, see Hemant Chaskar’s WLPC video.

1. WPA3-Personal for a VAP and a STA client.
   A. Setup the VAP with SSID, WPA3 security and a PSK.
B. Setup the VAP with 11w PMF option Required.
C. Setup the STA with SSID, WPA3 security and a PSK.

Sta202 (ct:523-3n-f20) Configure Settings

Port Status Information
Current: LINK-UP GRO Authorized
Driver info: Port Type: WiFi-STA Parent: wiphy2

Port Configurables
Standard Configuration
Enable
- Set MAC
- Set TX Q Len
- Set MTU
- Set Offload
- Set PROMISC

Services
- HTTP
- FTP
- RADIUS
- IPSEC-client
- IPSEC-UPstream

Low Level
- PROMISC
- TSO Enabled
- UFO Enabled
- GSO Enabled
- LRO Enabled
- GRO Enabled

General Interface Settings
- Down
- Aux-Mgt
- DHCP-IPv6
- DHCP-IPv4
- DHCP Release
- Secondary-IPs
- DHCP Vendor ID: None
- DHCP Client ID: None
- DNS Servers: BLANK Peer IP: NA
- IP Address: 0.0.0.0 Global IPv6: AUTO
- IP Mask: 0.0.0.0 Link IPv6: AUTO
- Gateway IP: 0.0.0.0 IPv6 GW: AUTO
- Alias:
- MAC Addr: 00:03:7f:30:00:00 TX Q Len: MTU:
- Rpt Timer: medium (8 s) WiFi Bridge: NONE
- IPSec GW: 0.0.0.0 IPSec Password:
- IPSec Local ID:
- IPSec Remote ID:

WIFI Settings
SSID: Android-wpa3
Key/Phrase: hello123
Mode: 802.11abgn ACM
Freq/Channel: 5745/149 Rate: Of Default
- WPA
- WPA2
- WPA3
- OSEn
- WEP
- Disable HT40
- Enable VHT60
- Disable SGi

Actions:
- Print
- Display
- Probe
- Display Scan
- Sync
- Apply
- OK
- Cancel
D. Setup the STA with 11w PMF option Required.

![Image of STA configuring settings]

Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

- **Key Management:** Default
- **HESSID:** 00:00:00:00:00:00
- **Pairwise Ciphers:** Default
- **Realm:**
- **Group Ciphers:** Default
- **Client Cert:**
- **WPA PSK:**
- **EAP Methods:** Default
- **EAP Identity:**
- **EAP Anon Identity:**
- **EAP Password:**
- **EAP Pin:**
- **Private Key:**
- **CA Cert File:**
- **Network Auth:** IEEE80211w Required (2)
- **Advanced/802.1x**
- **Enable 802.11u**
- **HotSpot 2.0**
- **Enable PKC**

![Image of WPA3-Enterprise association capture]

E. A capture of the association.

2. **WPA3-Enterprise for a VAP and a STA client.**
   
   A. Setup a RADIUS server for the VAP. This example uses a LANforge hostapd RADIUS server on the same system as the VAP.
B. Setup the VAP with WPA3 security and no PSK on the standard configuration screen.
C. Setup the VAP with 11w PMF option Required and select the checkbox for Advanced/802.1X which will also inform the VAP where its RADIUS server is located. In this example the LANforge hostapd RADIUS server is on the localhost.

D. After enabling Advanced/802.1X, the VAP is automatically configured for both WPA-EAP-SUITE-B and WPA-EAP-SUITE-B-192 as shown in the back-end configuration for the VAP.

```
cat /home/lanforge/wifi/hostapd_vap2.conf
...
wpa_key_mgmt=WPA-EAP-SUITE-B WPA-EAP-SUITE-B-192
...
```
E. Setup the STA with WPA3 security and no PSK on the standard configuration screen.
F. Setup the STA with 11w PMF option Required and select the checkbox for Advanced/802.1X which allows choosing the Key Management scheme and EAP Method. Here the STA is setup to use WPA-EAP-SUIT-B with EAP-TTLS and a user identity and password that were configured with the RADIUS server setup.

- **Key Management:** EAP-EAP-SUIT-B
- **EAP Methods:** EAP-TTLS
- **EAP Identity:** lanforge.ttls
- **EAP Anon Identity:**
- **EAP Password:** ttls123
- **Network Auth:** ieee80211w: Required (2)

Enabling 802.11u enables others.

A. Setup the VAP with WPA3 security and a PSK on the standard configuration, then select option 11w PMF option. Required on the advanced configuration, then admin up the VAP.

B. Copy the back-end config file for the VAP to a new filename and edit the wpa_key_mgmt from SAE to OWE.

```bash
cd /home/lanforge/wifi
cp hostapd_vap2.conf vap2-owe.conf
vi vap2-owe.conf
wpa_key_mgmt=OWE
```
C. Modify the VAP and select Custom WPA Cfg on the Misc Configuration screen then type in the location of the new VAP config file.
D. Setup the STA with WPA3 security and no PSK on the standard configuration screen.
E. Setup the STA with 11w PMF option Required and select the checkbox for Advanced/802.1X which allows choosing the Key Management scheme. Here the STA will use OWE and a WPA PSK.

F. A capture of the association.