

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.

	vap2 (ct	521-1ac-f20) Config	jure Settings	
]	Current: LINK-UF Driver Info: Port Ty	Port Status Informat GRO NONE pe: WIFI-AP Parent:	ion wiphyl wiphyl.	
Standard Configuration	Advanced Con	Port Configurable	s nfiguration Custo	om WiFi
Enable — Set MAC Set TX Q Len Set MTU	Down DHCP-IPv <u>6</u>	General In	DHCP Vendor ID:	None
Set Offload	DNS Servers: IP Address: IP Mask:	BLANK 20.100.1.1 255.255.255.0	Peer IP: Global IPv6: Link IPv6:	
Services HTTP FTP IPSEC-Client	Gateway IP: Alias: MAC Addr: Rpt Timer: IPSec GW:	0.0.0.0 00:0e:8e:6c:2d:b5 medium (8 s) v	IPv6 GW: MTU: TX Q Len WiFi Bridge: IPSec Password:	AUTO 1500 1000 NONE
	IPSec Local ID.: SSID: ABC	WiF D-wpa3	IPSec Remote ID.: i Settings ▼ AP: DEF	AULT
PROMISC TSO Enabled UFO Enabled GSO Enabled LRO Enabled GRO Enabled	Key/Phrase: hell Freq/Channel: 57 DTIM-Period: 2 Beacon: 240 WPA WPA2 Disable HT40	0123 45/149 ✓ WPA3 OSEN Disable HT80 □	Node: (80 Rate: 05 Max-STA: 200 WEP Enable VHT160	2.11abqn-AC) Default D7 Verbose Debug Disable SGI
Print Display Logs	Probe	Display Sca <u>n</u>	Sync	Apply <u>QK</u> <u>C</u> ancel

B. Setup the VAP with 11w PMF option Required.

	Driver Info: Port Type:	WIFI-A	P Parent: wiphy	1 wiphy1
	P	ort Co	onfigurables	
Standard Configuration	on Advanced Configur	ation	Misc Configur	ation Custom WiFi
j	Adv	anced	d WiFi Settings	
Select 'WPA2' on th and enable Advanc	e Standard Configuratio ed/802.1x to enable mo	n scre st of t	een to enable Ad hese. Enabling 8	wanced/802.1x 802.11u enables others.
Pairwise Ciphers:	DEFAULT	-	Group Ciphers:	DEFAULT
Ignore Probes:	zero (0%)	-	HESSID:	
Ignore Auth-Assoc:	zero (0%)	-	Realm:	
Ignore Assoc:	zero (O%)	-	IMSI:	
Ignore Re-Assoc:	zero (0%)	-	Milenage:	
Corrupt GTK:	zero (0%)	-	Domain:	
HS20 Capabilities			Consortium:	
HS20 Oper Class			RADIUS IP	127.0.0.1
HS20 WAN Metrics			RADIUS Port	1812
leee80211w:	Required (2)	•	RADIUS Secret	
Venue Group:	Unspecified (0)	-	Venue Type:	Unspecified (0) 👻
Network Type:	Private (0)	-	Address Types:	Not Available (0) 🗸
Network Auth:			3GPP Cell Net:	
🗌 Use 80211d 🛛	Use 80211h 🛛 🔲 BSS-	Load	🗌 Neighbor Re	eports 🗌 BSS Transition
Advanced/802.1	x 🔲 Short-Preamble	H	otSpot 2.0 🗌 🛛	Disable DGAF
🗌 Enable 802.11u	🗌 802.11u Internet	8 🗌	02.11u ASRA	802.11u ESR 802.11u UESA

C. Setup the STA with SSID, WPA3 security and a PSK.

	sta202 (ct	:523-3n-f20) Config	gure Settings	
Cu	rrent: LINK-UP	Port Status Informat GRO Authorized	ion	
Dri	ver into: Port Typ	e: WIFI-STA Parent:	wipny2 wipny2	
		Port Configurable	s	
Standard Configuration	Advanced Co	nfiguration Misc C	onfiguration Cor	ruptions Custom WiFi
Enable		General In	terface Settings	1
Set MAC	Down	🗌 Aux-Mgt		
Set TX Q Len	DHCP-IPv <u>6</u>	☑ DHCP Release	DHCP Vendor ID:	None 💌
Set MTU	☑ DHCP-IPv4	Secondary-IPs	DHCP Client ID:	None
Set Officiad	DNS Servers:	BLANK	Peer IP:	NA
Set PROMISE	IP Address:	0.0.0.0	Global IPv6:	AUTO
Services	IP Mask:	0.0.0.0	Link IPv6:	AUTO
HTTP	Gateway IP:	0.0.0.0	IPv6 GW:	AUTO
FTP	Alias:		MTU:	1500
RADIUS	MAC Addr:	00:03:7f:30:e0:00	TX Q Len	1000
IPSEC-Client	Rpt Timer:	medium (8 s) 🔻	WiFi Bridge:	NONE
IPsec-Upstream	IPSec GW:		IPSec Password:	
	IPSec Local ID.:		IPSec Remote ID.:	
		WiF	i Settings	
TSO Enabled	SSID: AB	CD-wpa3	AP: DEFA	ULT
UFO Enabled	Key/Phrase: he	llo123	Mode: 802.3	llabqn-AC 🔽
GS0 Enabled	Freq/Channel: 5	745/149	Rate: OS De	efault 💌
LRO Enabled	WPA WPA	2 VPA3 OSEN	I WEP	
GRO Enabled	Disable HT4	0 🗌 Enable VHT160	Disable SGI	
Print Display	Probe D	isplay Sca <u>n</u> Sy	nc <u>A</u> pply	/ <u>O</u> K <u>C</u> ancel

D. Setup the STA with 11w PMF option Required.

Currer Driver	nt: LINK-UP GRO Info: Port Type: W	/IFI-STA	rized Parent: wiphy:	2 wiphy2	
	Po	ort Conf	igurables		
Standard Configuration	Advanced Configu	uration	Misc Configur	ration Corruptions Cust	om WiFi
	Adva	anced w	/IFI Settings		
Select "WPA2" on th	e Standard Config	uration	screen to ena	hla Advancad/802 1 v	
and enable Advance	ed/802.1x to enab	ple most	t of these. Enab	ble Advanced/802.11 bling 802.11u enables other	s.
Key Management:	DEFAULT	-	HESSID:		
Pairwise Ciphers:	DEFAULT	-	Realm:		
Group Ciphers:	DEFAULT	-	Client Cert:		
WPA PSK:			IMSI:		
EAP Methods:	DEFAULT	-	Milenage:		
EAP Identity:			Domain:		
EAP Anon Identity:			Consortium:		
EAP Password:			Phase-1:		
EAP Pin:			Phase-2:		
Private Key:			PK Password:		
CA Cert File:			PAC File:		
Network Auth:			leee80211w:	Required (2)	-
Advanced/802.1	x Enable 802	2.11u	HotSpot 2.0	Enable PKC	

E. A capture of the association.

0		wpa3-pe	rsonal.pcapr	g (as superuser) 📀 🔊 🤇	×
File Edit View Go C	apture <u>A</u> nalyze <u>S</u> tatistics	Telephony <u>W</u> ireless	Tools <u>H</u> elp		
	🛯 🗋 🖹 🎑 🔍 🔶	• 🔶 警 🚡 🛓 📘	•	Q. Q. III	
wlan.addr==00:03:7f	:30:e0:00 and wlan.addr==0	00:0e:8e:6c:2d:b5		Expression +	
No. Time	Source	Destination	Protocol	Length Info	
No. Time 3465 74.324976814 3466 74.52020052 3470 74.580270153 3470 74.580270153 3472 74.592681729 3474 74.592681729 3478 74.595487088 3478 74.595487089 3488 74.600308007 3488 74.600308007 3488 74.60040120 3499 74.60547767 3492 74.605477678 3499 74.605477678 3499 74.605477678 3499 74.605477678 3499 74.605418 byte 74801747768 3499 74.605418 byte 74801747768 7490 74.605418 byte 7490 749	Source 00:00:10:10:10:10:10:10:10:10:10:10:10:1	Destination 0:0377;30:20:00 0:06:20:20:20 0:0377;30:20:00 0:00:20:20:20 0:0377;30:20:00 0:00:20:20:20 0:0377;30:20:00 0:00:20:20:20 0:00:27;30:20:00 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20:20 0:00:20:20:20:20 0:00:20:20:20:20 0:00:20:20:20:20 0:00:20:20:20:20 0:00:20:20:20:20 0:00:20:20:20:20 0:00:20:20:20:20 0:00:20:20:20:20 0:00:20:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20:20 0:00:20 0:00:20:20 0:00:2	Protocol 802.11 802.11 802.11 802.11 802.11 802.11 802.11 EAPOL EAPOL EAPOL EAPOL 802.11 802.11 802.11 802.11 802.11 802.11 802.11	Length Info 234 Probe Response, SN=2371, FN=0, Flags= 188 Authentication, SN=237, FN=0, Flags= 188 Authentication, SN=237, FN=0, Flags= 124 Authentication, SN=237, FN=0, Flags= 206 Association Response, SN=2374, FN=0, Flags=, 214 Authentication, SN=235, FN=0, Flags=, 206 Association Response, SN=2375, FN=0, Flags=, 215 Key (Message 1 of 4) 221 Key (Message 3 of 4) 221 Key (Message 3 of 4) 234 Key (Message 3 of 4) 139 Astor, SN=0, FH=0, Flags= 199 Action, SN=2377, FN=0, Flags=.p 199 Action, SN=2377, FN=0, Flags=.p 193 Action, SN=2377, FN=0, Flags=.p 193 Action, SN=2377, FN=0, Flags=.p 193 Action, SN=2377, FN=0, Flags=.p	•
Scalar: 5b5b7d Finite Field E	9e3ccb0b548b2f9cdf5a03dcf lement: 252e82dc16c2ec389	'b944cb543cf9f6fac 94a770a7dde36396a99e200f	591a96c7		

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	urrent: LINK-UF	Port Status Informat 9 GRO_NONE	tion	
[river Info: Port Ty	pe: WIFI-AP Parent:	wiphyl wiphyl	
		Port Configurable	s	
Standard Configuration	Advanced Con	figuration Misc Co	nfiguration Cust	om WiFi
Enable		General In	terface Settings	1
Set MAC	Down	🗌 Aux-Mgt		
🔲 Set TX Q Len	DHCP-IPv6	☑ DHCP Release	DHCP Vendor ID:	None
Set MTU	DHCP-IPv4	Secondary-IPs	DHCP Client ID:	None
Set Officiad	DNS Servers:	BLANK	Peer IP:	NA
	IP Address:	20.100.1.1	Global IPv6:	AUTO
	IP Mask:	255.255.255.0	Link IPv6:	AUTO
	Gateway IP:	0.0.0.0	IPv6 GW:	AUTO
Services —	Alias:		MTU:	1500
	MAC Addr:	00:0e:8e:6c:2d:b5	TX Q Len	1000
	Rpt Timer:	medium (8 s) 🔻	WiFi Bridge:	NONE
IPsec-Upstream	IPSec GW:	0.0.0.0	IPSec Password:	
	IPSec Local ID.:		IPSec Remote ID.:	
		WiF	ii Settings	
	SSID: ABC	DE-wpa3	AP: DEF	FAULT
	Key/Phrase:		14ode: (80	2.11abqn-AC) 💌
TS0 Enabled	Freq/Channel: 57	45/149	Rate: OS	Default 💌
UFO Enabled	DTIM-Period: 2		Max-STA: 200	07
GS0 Enabled	Beacon: 240)		
LRO Enabled	WPA WPA2	WPA3 OSEN	WEP	Verbose Debug
🗹 GRO Enabled	Disable HT40	Disable HT80	Enable VHT160 🗌	Disable SGI

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.

⊗ ■ ■ vap2 (ct521-1a)	c-f20) Configure Settings
Port S	itatus Information
Current: LINK-UP GRO	NONE
Driver Info: Port Type: WIF	FI-AP Parent: wiphy1 wiphy1
Port	t Configurables
Standard Configuration Advanced Configurat	ion Misc Configuration Custom WiFi
Advan	nced WiFi Settings
Select 'WPA2' on the Standard Configuration s and enable Advanced/802.1x to enable most	screen to enable Advanced/802.1x of these. Enabling 802.11u enables others.
Pairwise Ciphers: DEFAULT	▼ Group Ciphers: DEFAULT ▼
Ignore Probes: zero (0%)	➡ HESSID: 00:00:00:00:00
Ignore Auth-Assoc: zero (0%)	▼ Realm:
Ignore Assoc: zero (0%)	▼ IMSI:
Ignore Re-Assoc: zero (0%)	▼ Milenage:
Corrupt GTK: zero (0%)	▼ Domain:
HS20 Capabilities	Consortium:
HS20 Oper Class	RADIUS IP 127.0.0.1
HS20 WAN Metrics	RADIUS Port 1812
leee80211w: Required (2)	RADIUS Secret lanforge
Venue Group: Unspecified (0)	✓ Venue Type: Unspecified (0)
Network Type: Private (0)	▼ Address Types: Not Available (0) ▼
Network Auth:	3GPP Cell Net:
Use 80211d Use 80211h BSS-Lo	ad 🗌 Neighbor Reports 🔲 BSS Transition
Advanced/802.1x Short-Preamble	HotSpot 2.0 Disable DGAF
Enable 802.11u 802.11u Internet	802.11u ASRA 802.11u ESR 802.11u UESA
Print Display Logs Probe Di	Isplay Scan Sync Apply OK Cancel

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.

<pre>cat /home/lanforge/wifi/hostapd_vap2.conf</pre>
<pre>wpa_key_mgmt=WPA-EAP-SUITE-B WPA-EAP-SUITE-B-192</pre>

E. Setup the STA with WPA3 security and no PSK on the standard configuration screen.

• •	sta203 (c	t523-3n-f20) Confi	gure Settings	_	
		Port Status Informa	tion		
Ci	urrent: LINK-UP	GRO Authorized			
Di	river Info: Port Ty	pe: WIFI-STA Parent	:: wiphy2 wiphy2	2	
		Port Configurable	es		
Standard Configuratio	n Advanced Co	onfiguration Misc (Configuration Co	rruptions Cus	tom WiFi
Enable		General Ir	nterface Settings		1
Set MAC	🗌 Down	🗌 Aux-Mgt			
🔲 Set TX Q Len	DHCP-IPv6	✓ DHCP Release	DHCP Vendor ID:	None	-
Set MTU	☑ DHCP-IPv4	Secondary-IPs	DHCP Client ID:	None	-
	DNS Servers:	BLANK	Peer IP:	NA	
	IP Address:	0.0.0.0	Global IPv6:	AUTO	
Services —	IP Mask:	0.0.0.0	Link IPv6:	AUTO	
HTTP	Gateway IP:	0.0.0.0	IPv6 GW:	AUTO	
FTP	Alias:		MTU:	1500	
RADIUS	MAC Addr:	00:03:7f:ce:63:00	TX Q Len	1000	
IPSEC-Client	Rpt Timer:	medium (8 s) 🔻	WiFi Bridge:	NONE	-
🔲 IPsec-Upstream	IPSec GW:	0.0.0.0	IPSec Password:		
	IPSec Local ID.:		IPSec Remote ID.:		
		Wif	Ei Settings		
TSO Enabled	SSID: AB	CDE-wpa3	AP: DEFA	AULT	
UFO Enabled	Key/Phrase:		Mode: 802.	llabqn-AC	-
GS0 Enabled	Freq/Channel: 5	5745/149	Rate: OS D	efault	-
LRO Enabled	WPA WPA	A2 WPA3 OSEI	N WEP		
GRO Enabled	Disable HT4	0 🗌 Enable VHT160) 🗌 Disable SGI		
1					
rint Display	Probe [Display Sca <u>n</u> <u>S</u> y	nc <u>A</u> ppl	у <u>О</u> К	<u>C</u> anc

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-SUITE-B with EAP-TTLS and a user identity and password that were configured with the RADIUS server setup.

	sta203	(ct523-3n-f2	20)	Configure S	ettings	
	Current: LINk Driver Info: Por	Port Statu C-UP GRO Auth t Type: WIFI-ST/	is Ir nori: A	nformation zed Parent: wiphy2	2 wiphy2	
		Port Co	nfig	gurables		1
Standard Configura	ation Advanced	d Configuration Advanced	ר Wil	Misc Configur Fi Settings	ation Corruptions Cust	om WiFi
Select 'WPA and enable	2' on the Standa Advanced/802.1)	rd Configuratio	on s	screen to enat of these. Enab	ole Advanced/802.1x vling 802.11u enables others	s.
Key Manage	ement: WPA-EAP-	SUITE-B	•	HESSID:		
Pairwise Cip	hers: DEFAULT		•	Realm:		
Group Ciphe	ers: DEFAULT		-	Client Cert:		
WPA PSK:				IMSI:		
EAP Method	ls: EAP-TTLS		-	4ilenage:		
EAP Identity	lanforge.	ttls		Domain:		
EAP Anon Io	lentity:			Consortium:		
EAP Passwo	ord: <u>!!ttls123</u>			Phase-1:		
EAP Pin:				Phase-2:		
Private Key:			4	PK Password:		
CA Cert File			-r	PAC File:	Deguined (2)	
			ļ	leee80211W:		
Advance	60/802.1x	able 802.11U	L	_ HotSpot 2.0	Enable PKC	
Print Display	Probe	Display Sca	n	<u>S</u> ync	Apply OK	<u>C</u> ancel

G. A capture of the association.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Image: Control of the statistics of telephony Wireless Tools Help Image: Control of the statistics of telephony Wireless Tools Help Image: Control of the statistics of telephony Wireless Tools Help Image: Control of the statistics of telephony Wireless Tools Help Image: Control of the statistics of telephony Wireless Tools Help Image: Control of the statistics of telephony Wireless Tools Help Image: Control of the statistics of telephony Wireless Tools Help Image: Control of the statistics of telephony Wireless Tools Help Image: Control of the statistics of telephony Wireless Tools Help Image: Control of telephony Wirelesstatistis Image: Con	0			*m	ioni3a (as	superuser) 💿 📀	
No. No. <td>File</td> <td><u>E</u>dit ⊻iew <u>G</u>o <u>C</u></td> <td>apture <u>A</u>nalyze <u>S</u>tatistics</td> <td>Telephony Wireless Too</td> <td>ols <u>H</u>elp</td> <td></td> <td></td>	File	<u>E</u> dit ⊻iew <u>G</u> o <u>C</u>	apture <u>A</u> nalyze <u>S</u> tatistics	Telephony Wireless Too	ols <u>H</u> elp		
Wain.addr-=00.03:7fcet63:00 and wain.addr-=00.0e:8e:6c:2d:b5 Protocol Length Info Expression Expression No. Time Source Destination Protocol Length Info 773 19.07758464 00100.800:60:2010:05 00100:7fcet633:00 000:11 239 Frobe Response, SH=1274, FHES, Flagss, SSID=ABCDE=xppa3 773 19.02730984 00100:7fcet633:00 00100:7fcet633:00 000:11 190 Authentication, SH=237, FHES, Flagss, SSID=ABCDE=xppa3 773 19.02730984 00100:7fcet633:00 000:027fcet633:00 000:11 193 ASSOCIATION Request, SH=1274, FHES, Flagss, SSID=ABCDE=xppa3 773 19.03138500 00100:7fcet633:00 000:037fcet633:00 000:07fcet633:00			। 🔝 🖹 🎑 🗢	٠ 🖻 کې 🖻	•	Q, Q, II	
No. Time Source Destination Protocol Length Info 775 15:07268444 00001976502015 00001971602015 0001971602010 00019717602010 00019717602010 00019717602010 00019717602010 00019717602010 00019717602010 00019717602010 00019717602010 00019717602010 00019717602010 00019717602010 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 00019717602000 0001971602000 0001971602000 0001971602000 00019716020000 00019716020000 00019716020000000000	W	/lan.addr==00:03:7f:	ce:63:00 and wlan.addr==00	0:0e:8e:6c:2d:b5		Expression	+
763 19.677894844 00.00137fice:63:00 000137fice:63:00 <	No.	Time	Source	Destination	Protocol	Length Info	-
<pre>775 19.92792788 06:03:7f:ce:03:00 00:00:02:6c:22:05 802.11 00 Authentication, SH=275, FHe9, Flags= 776 19.93139509 00:03:7f:ce:03:00 00:00:02:6c:22:05 802.11 207 Association Request, SH=285, FHe9, Flags= 778 19.93251364 00:00:02:6c:22:05 00:03:7f:ce:03:00 EAP 10 Request, Identity 778 19.93139509 00:03:7f:ce:03:00 00:00:02:05:22:05 EAP 115 Response, Johnty 778 19.934869120 00:03:7f:ce:03:00 00:00:02:05:22:05 EAP 115 Response, Johnty 778 19.9313903 00:00:00:00:07:00:02:05:22:05 EAP 115 Response, Johnty 779 19.934869120 00:00:00:07:00:00:00:00:00:00:00:00:00:0</pre>		763 19.677894644	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	802.11	239 Probe Response, SN=1274, FN=0, Flags=, BI=240, SSID=ABCDE-wpa3	
777 19.923834327 00.00377(cet83:00 00		775 19.927290798		00:0e:8e:6c:2d:b5		90 Authentication, SN=257, FN=0, Flags=	
779 10.93139500 00100771:0010310 0010001807:00103171:0010310 00100110 207 Association Reguest, SH=256, FH=0, Flags=, SSID=ABCDE-upa3 781 10.93251364 001001001801801:001001 001001101100 EAP 103 Reguest, Identity 783 10.93251364 001001001801:001001 001001101000 EAP 103 Reguest, Identity 781 10.93251364 0010010010010010000 0010011010000 EAP 103 Reguest, Identity 771 10.93051364 0010010010010000000000000000000000000		777 19.928384327				90 Authentication, SN=1276, FN=0, Flags=	
781 15.83253864 00:00:80:66:62:20:D5 00:03:77:02:63:00 00:21 139 Association Response, Identity 781 15.83258013 00:00:87:10:06:20:D5 00:03:77:02:63:00 00:00:82:60:20:D5 EAP 116 Response, Identity 103 Request, Identity 785 15.83480913 00:00:87:10:06:30:00 00:00:82:60:20:D5 EAP 116 Response, Identity 103 Request, IIS EAP (EAP-TLS) 785 15.83480913 00:00:87:10:06:30:00 00:00:82:60:20:D5 EAP 104 Response, Legacy Hak (Response only) 1131 Association Response, Legacy Hak (Response only) 731 15.83784035 00:00:87:10:06:30:00 00:00:82:60:20:D5 TLSN1.2 344 Client Hello 104 Request, Iunneld TLS EAP (EAP-TLS) 733 15.83877522 00:00:87:10:06:30:00 00:00:82:60:20:D5 TLSN1.2 344 Client Hello 104 Request, Iunneld TLS EAP (EAP-TLS) 731 15.4317522 00:00:87:10:06:30:00 00:00:82:60:20:D5 TLSN1.2 344 Client Hello 104 Request, Iunneld TLS EAP (EAP-TLS) 731 15.44174798 00:00:80:71:00:83:00 00:00:82:60:20:D5 TLSN1.2 344 Client Hello 104 Request, Iunneld TLS EAP (EAP-TLS) 731 15.44174798 00:00:80:60:20:D5 00:00:77:00:00:10 TLSN1.2 344 Client Hello 105 Request Hello, OFTTIC:00:00 DEAP 731 15.44174798 00:00:80:60:00:07:71:00:83:00 TLSN1.2 10:00:07:00:00:00 DEAP 104 Request LSN (Response, Tunneld TLS EAP (EAP-TLS) 731 15.4417479 00:00:80:60:20:05 TLSN1.2 10:00:07:00:00:00:00:00:00:00:00:00:00:00	Г.	779 19.931395509	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	802.11	207 Association Request, SN=258, FN=0, Flags=, SSID=ABCDE-wpa3	
783 10.833260310 00.00.826:6c:22:055 00.00.827:7c:e:83:00 EAP 108 Request, Identity 785 10.838368030 00:00:82:6c:22:055 00.00:82:6c:22:055 EAP 104 Request, TLS EAP (EAP-TLS) 785 10.838567226 00:00:82:6c:22:055 00:00:82:6c:22:055 EAP 104 Request, Tunneld TLS EAP (EAP-TLS) 783 10.838775226 00:00:82:6c:22:055 00:00:82:6c:22:055 TLSV1.2 150 Request, Tunneld TLS EAP (EAP-TLS) 785 10.842174798 00:00:82:6c:22:055 00:00:82:6c:22:055 TLSV1.2 150 Request, Tunneld TLS EAP (EAP-TLS) 795 10.842174798 00:00:82:6c:22:055 00:00:82:6c:22:055 TLSV1.2 150 Request, Tunneld TLS EAP (EAP-TLS) 795 10.842174798 00:00:82:6c:22:055 00:00:82:6c:22:055 TLSV1.2 150 Request, Tunneld TLS EAP (EAP-TLS) 795 10.842174798 00:00:82:6c:22:055 00:00:82:6c:22:055 TLSV1.2 150 Request, Tunneld TLS EAP (EAP-TLS) 795 10.842174798 00:00:82:6c:22:055 00:00:82:6c:22:055 TLSV1.2 150 Request, Tunneld TLS EAP (EAP-TLS) 795 10.842174798 00:00:82:6c:22:055 TLSV1.2 150 Request, Tunneld TLS EAP (EAP-TLS) 795 10.842574992 00:00:81:6c:62:20:05 TLSV1.2 150 Application Data </td <td></td> <td>781 19.932513664</td> <td>00:0e:8e:6c:2d:b5</td> <td>00:03:7f:ce:63:00</td> <td>802.11</td> <td>193 Association Response, SN=1277, FN=0, Flags=</td> <td></td>		781 19.932513664	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	802.11	193 Association Response, SN=1277, FN=0, Flags=	
765 19.934893130 00:00:80:60:20:210:5 00:00:71:c0:63:00 00:00:80:60:20:210:5 EAP 116 Response, Identity 767 10.933316030 00:00:80:60:220:125 00:00:71:c0:83:00 00:00:80:60:220:155 EAP 104 Response, Legacy Hak (Response only) 793 19.936746362 00:00:80:60:220:155 00:00:71:c0:83:00 00:00:80:60:220:155 EAP 104 Response, Tunneled TLS EAP (EAP-TTLS) 793 19.94217780 00:00:80:60:220:155 TLSN1.2 1348 Client Hello 79 799 19.942176785 00:00:80:60:220:155 TLSN1.2 103 Server Hello Cont 79 799 19.942176875 00:00:80:60:220:155 TLSN1.2 103 Server Hello Cont 79 799 19.942176875 00:00:80:60:220:155 TLSN1.2 103 Server Hello Cont 70 799 19.942475875 00:00:80:60:220:155 TLSN1.2 103 Server Hello Cont 70 800 19.95179190 00:00:80:60:220:155 TLSN1.2 106 Application Data 70 807 19.95382125 00:00:80:60:220:155 TLSN1.2 105 Application Data 70 807 19.956927808 00:00:80:60:220:155 TLSN1.2 105 Application Data 70 20:00:07:7:c0:63:00 70:00:00:80:60:220:155 <td></td> <td>783 19.933260310</td> <td>00:0e:8e:6c:2d:b5</td> <td>00:03:7f:ce:63:00</td> <td>EAP</td> <td>103 Request, Identity</td> <td></td>		783 19.933260310	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAP	103 Request, Identity	
787 19.353136903 00:08:08:06:20:05 00:08:28:06:22:05 00:08:28:06:22:05 EAP 104 Request, TLS EAP (EAP-TLS) 793 19.33567252 00:08:17:06:33:00 00:08:28:06:22:05 00:08:28:06:22:05 EAP 104 Request, Tunneld TLS EAP (EAP-TLS) 793 19.33677522 00:08:17:06:33:00 00:08:28:06:22:05 00:08:28:06:22:05 TLSV1.2 150:Server Hello, Certificate, Server Hello Done 795 19.442174798 00:08:07:06:30:00 00:08:28:06:22:05 00:08:17:06:33:00 TLSV1.2 150:Server Hello, Certificate, Server Hello Done 795 19.442174798 00:08:07:06:30:00 00:08:28:06:22:05 TLSV1.2 150:Server Hello, Certificate, Server Hello Done 795 19.442174798 00:08:07:06:30:00 00:08:28:06:22:05 TLSV1.2 150:Server Hello, Certificate, Server Hello Done 795 19.442174798 00:08:07:06:30:00 00:08:28:06:22:05 TLSV1.2 150:Server Hello, Certificate, Server Hello Done 601 19.44785432 00:08:07:07:06:30:00 TLSV1.2 150:Server Hello, Certificate, Server Hello Done 803 19.55232420 00:08:07:07:06:30:00 00:08:28:07:20:00 TLSV1.2 150:Application Data 805 19.5525452 00:03:77:06:30:00 00:03:77:06:30:00 TLSV1.2 165:Application Data 813 19.55505155 00:00:03:77:06:30:00 00:03:77:06:30:00 EAPOL 21: Key (Mes		785 19.934869130	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	EAP	116 Response, Identity	
798 19.35878225 00:02171/CE103:00 00:0021871/CE103:00 EAP 104 Response, Lunneld TK (Response OILY) 793 19.33878352 00:02171/CE103:00 00:00171/CE103:00 TLSV1.2 343 Client Hello 793 19.338775226 00:02171/CE103:00 00:00171/CE103:00 TLSV1.2 343 Client Hello 793 19.42174786 00:00171/CE103:00 00:00171/CE103:00 TLSV1.2 104 Response, Tunneld TLS EAP (EAP-TTLS) 799 19.44504722 00:00171/CE103:00 00:00171/CE103:00 TLSV1.2 103 Server Hello Cortificate, Server Hello Done 801 19.44504022 00:00171/CE103:00 00:00171/CE103:00 TLSV1.2 103 Server Hello, Certificate, Server Hello Done 801 19.4504022 00:00171/CE103:00 00:00171/CE103:00 TLSV1.2 103 Server Hello, Certificate, Server Hello Done 801 19.4504022 00:00171/CE103:00 00:00171/CE103:00 TLSV1.2 163 Application Data 807 19.4504022 00:00171/CE103:00 00:00171/CE103:00 TLSV1.2 165 Application Data 807 19.4550428 00:00171/CE103:00 00:00171/CE103:00 EAP 105 Success 813 19.4550429 00:00171/CE103:00 CE101 21 Key (Message 1 of 4) 815 19.45607252405		787 19.936316903	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAP	104 Request, TLS EAP (EAP-TLS)	
731 10.357483652 00:00:20:20:20:20:20:20:00 00:00:20:20:20:20:20:00 735 13.3577522 00:00:20:20:20:20:20:20:00 TLSN.2 100 Redues: 735 13.34217478 00:00:20:20:20:20:20:00 TLSN.2 150 Server Hello, Certificate, Server Hello Done 735 13.34217478 00:00:20:20:20:20:20:00 TLSN.2 150 Server Hello, Certificate, Server Hello Done 735 13.34217478 00:00:20:20:20:20:20:00 TLSN.2 150 Server Hello, Certificate, Server Hello Done 735 13.34217478 00:00:20:20:20:20:20:00 TLSN.2 150 Server Hello, Certificate, Server Hello Done 735 13.34217478 00:00:20:20:20:20:20:00 TLSN.2 150 Server Hello, Certificate, Server Hello Done 601 13.5425120 00:00:20:20:20:20:20:00 TLSN.2 150 Server Hello, Certificate, Server Hello, Done 805 13.55:352421 00:00:20:20:20:20:20:00 TLSN.2 150 Application Data 805 13.55:352420 00:00:20:20:20:20:00 TLSN.2 156 Application Data 805 13.55:251210 00:00:20:20:20:20:00 TLSN.2 156 Application Data 813 13.555251320 00:00:27:00:20:20:20:00 10:30:20:27:00 20:00:27:00:20:20:20:20:20:20:20:20:20:20:20:20:		789 19.936678226	00:03:7f:Ce:63:00	00:0e:8e:6C:2d:05	EAP	104 Response, Legacy Nak (Response Only)	
735 135 335 0110 115 115 335 01111 115 <t< td=""><td></td><td>791 19.937948362</td><td>00:00:80:60:20:05</td><td>00:03:7T:Ce:63:00</td><td>EAP</td><td>104 Request, lunneled ILS EAP (EAP-TILS)</td><td></td></t<>		791 19.937948362	00:00:80:60:20:05	00:03:7T:Ce:63:00	EAP	104 Request, lunneled ILS EAP (EAP-TILS)	
739 10.942/17476 00.002000 00.002000 00.0020000 110.00000 739 10.942/17476 00.0020000 00.0020000 110.00000 150.00000 739 10.942/17476 00.0020000 00.0020000 110.00000 150.00000 110.00000 739 10.942/17476 00.00200000 00.00200000 110.00000 100.000000 100.000000 100.000000 100.000000 100.000000 100.000000 100.000000 100.000000 100.000000 100.000000 100.000000 100.0000000 100.0000000 100.0000000000 100.0000000000000000000000000000000000		793 19.930775229	00.03.71.Ce.63.00	00.02.71.00.20.05	TLSV1.2	348 Cirent neilo	
739 13 54540422 000000000000000000000000000000000000		795 19.942174790	00.00.00.00.00.00	00.03.71.Ce.03.00	FAP	1301 Server nello, certificate, server nello bone	
000 0		799 19 945040229	00:00:71:00:00	00:02:7f:co:62:00	TIEV1 2	104 Kesponse, Tunneleu Tas EAT (EAT-TIS)	.
00110 01010 01000 010000 010000 0100000 0100000 01000000 010000000 0100000000 01000000000 0100000000000000 0100000000000000000000000000000000000		801 10 047805435	00:00:00:00:00:00	80:00:03:77:00:03:00	TISV1.2	A22 Client Key Evchange Change Clienter Sher Encryntad Handshake Message	
00010 000000000000000000000000000000000000		803 19 951791992	00:00:00:00:00:00	80:03:7f:ce:63:00	TISV1 2	155 Change Cipher Sher Encrysted Handshake Message	
807 19 95382372 00-00:95:62:62:62:05 00:02:77:62:63:00 TLSV1.2 165 Application Data 808 19 95372372 00-00:95:62:62:20:155 00:02:77:62:63:00 EAP 102 Success 811 19.955718400 00:02:62:62:20:155 00:03:77:62:63:00 EAP 102 Success 813 19.955827380 00:02:62:62:20:155 00:03:77:62:63:00 EAPOL 215 Key (Message 1 of 4) 815 19.95927380 00:03:77:62:63:00 00:00:26:62:62:01:15 EAPOL 215 Key (Message 2 of 4) 817 19.958275229 00:00:07:62:62:02:155 00:00:27:76:62:30:00 EAPOL 28 Key (Message 2 of 4) 817 19.958752292 00:00:07:62:62:02:155 00:00:27:76:62:00:05 EAPOL 28 Key (Message 2 of 4) 817 19.958752292 00:00:27:76:62:02:155 EAPOL 28 Key (Message 2 of 4) 817 19.958752292 00:00:27:76:62:02:155 EAPOL 28 Key (Message 2 of 4) 817 19.958752292 00:00:27:76:62:02:155 EAPOL 28 Key (Message 2 of 4) 817 19:00:00:01:1 Tag length:28 73 length:16:00:01:01:01:01:01:01:01:00:01:01:00:01:16:00:01:01:00:01:10:00:01:10:00:01:10:00:0		805 19 952392491	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	TISV1 2	161 Annication Data	
800 19.55253420 00.00:7ff.cc:63:00 00:00:7ff.cc:63:00 EAP 105 Supplication Data 811 19.55561256 00.00:7ff.cc:63:00 00:00:7ff.cc:63:00 EAP 105 Supplication Data 815 19.555627360 00:00:7ff.cc:63:00 00:00:7ff.cc:63:00 EAPL 215 Key (Messape 2 of 4) 815 19.55675280 00:00:7ff.cc:63:00 00:00:7ff.cc:63:00 00:00:7ff.cc:63:00 EAPDL 221 Key (Messape 2 of 4) 815 19.558752020 00:00:7ff.cc:63:00 00:00:80:60:2d:05 EAPDL 221 Key (Messape 3 of 4) 91 19.558752020 00:00:7ff.cc:63:00 00:00:80:60:2d:05 EAPDL 231 Key (Messape 3 of 4) 91 7 30: SUpported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec] 133 Key (Message 4 of 4) 133 Key (Message 4 of 4) • Tag: SNI Information Tag length: 26 RSN Version: 1 Farmagement (AKH) Suite Count: 1 • Pairvise Cipher Suite Count: 1 Pairvise Cipher Suite Count: 1 Pairvise Cipher Suite 10:0:0f:ac AES (CCM) • Auth Key Manageent (AKH) Suite: 00:0f:ac WPA (SHA256-SuiteB) Auth Key Manageent (AKH) Suite: 00:0f:ac WPA (SHA256-SuiteB) • Auth Key Manageent (AKH) Uppe: WFA (SHA256-SuiteB) Auth Key Manageent (AKH) Uppe: WFA (SHA256-SuiteB) • Auth Key Manageent (AKH) Uppe: WFA (SHA256-SuiteB) (11)		807 19,953832132	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	TISV1.2	165 Application Data	
<pre>stills.strike.stri</pre>		809 19,954261428	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	TLSv1.2	165 Application Data	
<pre>Bill 19.958651256 00-00:Field:2015 00:0377f:ce:83:00 EAPOL 215 Key (Messape 1 of 4) Bill 19.958254854 00-00:Field:2015 00:06:Field:2015 EAPOL 221 Key (Messape 2 of 4) Bill 19.95825292 00-00:Field:2015 00:06:Field:2015 EAPOL 281 Key (Messape 3 of 4) Bill 19.95825292 00-00:Field:2015 00:06:Field:2015 EAPOL 281 Key (Messape 4 of 4) Flag: SSID parameter set: ABCCE-upa3 Flag: SSID parameter set: SSID flog: SSID set: SSID set:</pre>		811 19,955718490	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAP	102 Success	
Bi1 19.95827898 00:00:7f(cc:63:00 00:00:8c:6c:2d:b5 EAPOL 221 Keý (Message 2 of 4) Bi1 19.958752292 00:00:7f(cc:63:00 00:00:7f(cc:63:00 EAPOL 221 Keý (Message 3 of 4) Bi1 19.958752292 00:00:7f(cc:63:00 00:00:7f(cc:63:00 EAPOL 231 Keý (Message 3 of 4) Bi1 19.958752292 00:00:7f(cc:63:00 00:00:8e:8c:2d:b5 EAPOL 193 Keý (Message 3 of 4) Bi Tag: SUpportale Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec] - - Tag: RNU Information Tag: RNU Information - - - - - Tag: Number: RSN Information (48) - - - - - Tag Number: RSN Information (48) -		813 19,956051256	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAPOL	215 Key (Message 1 of 4)	
817 19.958252854 00:00:18:6c:2d:b5 00:00:17:1:c:63:00 EAPOL 281 Key (Message 3 of 4) 819 19.95875229 00:00:18:6c:2d:b5 EAPOL 103 Key (Message 4 of 4) > Tag: SSID parameter set: ABCDE-wpa3 103 Key (Message 4 of 4) 103 Key (Message 4 of 4) > Tag: SNI Information Tag length: 26 RSN Version: 1 Fague 10:00:07:07:07:07:07:07:07:07:07:07:07:07		815 19.956927898	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	EAPOL	221 Key (Message 2 of 4)	- 1
819 19.958752292 00.03:7fice:83:00 00:00:80:80:22:1b) EAPOL 193 Key (Message 4 of 4) Tag: SSID parameter set: ABCDE-wpa3 Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec] Tag: RSN Information Tag length: 26 RSN Version: 1 Group Cipher Suite: 00:0f:ac AES (CCM) Pairwise Cipher Suite List 00:0f:ac AES (CCM) Auth Key Management (AKM) Suite: 00:0f:ac WFA (SHA256-SuiteB) Auth Key Management (AKM) Suite: 00:0f:ac WFA (SHA256-SuiteB) Auth Key Management (AKM) type: WFA (SHA256-		817 19.958254854	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAPOL	281 Key (Message 3 of 4)	
 Tag: SSID parameter set: ABCDE-wpa3 Tag: SSUpported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec] Tag: RSNI Information Tag Humber: RSNI Information (48) Tag length: 26 RSN Version: 1 Jeroput Cipher Suite : 00:0f:ac AES (CCH) Pairvise Cipher Suite is 00:0f:ac AES (CCH) Auth Key Management (AKM) Suite Count: 1 Value Cipher Suite Is 00:0f:ac WFA (SHA256-SuiteB) v Auth Key Management (AKM) Suite: 00:0f:ac WFA (SHA256-SuiteB) Auth Key Management (AKM) Suite: 00:0f:ac Auth Key Management (AKM) Suite: 00:0f:ac		819 19.958752292			EAPOL	193 Key (Message 4 of 4)	-
PHKID Count: 0 PHKID LIST		 Tag: SSID para Tag: SSID para Tag: RSN Inform Tag: RSN Inform Tag length: RSN version Group ciphen Pairwise Cip Pairwise Cip Pairwise Cip Auth Key Mar <	meter set: ABCDE-wpa3 Rates 6, 9, 12, 18, 24, 3 mation RSW Information (48) 26 : 1 r suite: 00:0f:ac AES (CCM) oher suite count: 1 oher suite count: 1 oher suite count: 1 agement (AKM) Suite: 0 ey Management (AKM) OUI: ey Management (AKM) OUI: ey Management (AKM) OUI: ey Management (AKM) USE: 1 (16) (16) (16) (17) (17) (17) (17) (17) (17) (17) (17	H6, 48, 54, [Mbit/sec]) ES (CCM) : 1 ac WPA (SHA256-SuiteB) 0:0f:ac WPA (SHA256-Suite 0:0f:ac WPA (SHA256-SuiteB) (11)	8)		

3. WPA3 OWE - Opportunistic Wireless Encryption.

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.

		Port Status Informa	tion		1		Port	Status Information		
	Current: LINK-UF	GRO NONE					Current: LINK-UP GR0	NONE		
1	Driver Info: Port Ty	pe: WIFI-AP Parent:	wiphy1 wiphy1				Driver Info: Port Type: W	IFI-AP Parent: wiphy	y1 wiphy1	
		Port Configurable	s				Po	rt Configurables		
Standard Configuration	Advanced Con	figuration Misc Co	onfiguration Cust	tom WiFi		Standard Configuratio	on Advanced Configura	tion Misc Configu	ration Custom WiFi	
Enable		General Ir	nterface Settings		II F		Adva	nced WiFi Settings		ſ
Set MAC	Down	Aux-Mgt	-							
Set TX Q Len	DHCP-IPv6	DHCP Release	DHCP Vendor ID:	None		Select 'WPA2' on th and enable Advanc	e Standard Configuration ed/802.1x to enable most	screen to enable A of these. Enabling	dvanced/802.1x 802.11u enables others.	
Set MTU		Secondany/Ps	DHCP Client ID:	None		Pairwise Ciphers:	DEFAULT	Group Ciphers:	DEFAULT	
Set Offload	DNS Servers:	BLANK	Peer IP-	NA		lanore Probes:	zero (0%)	HESSID:	00:00:00:00:00	
Set PROMISC	IP Address:	20.100.1.1	Global IPv6:	AUTO		Ignore Auth-Assoc-	zero (0%)	▼ Realm		
	IP Mask:	255.255.255.0	Link IPv6:	AUTO		Ignoro Accos	70.00 (0%)	- IMCL		- !
	Gateway IP:	0.0.0.0	IPv6 GW:	AUTO		ignore Assoc.	2610 (06)	• 10151		
Services	Alias:		MTU:	1500		Ignore Re-Assoc:	zero (U%)	Milenage:		_ !
	MAC Addr:	00:0e:8e:6c:2d:b5	TX Q Len	1000		Corrupt GTK:	zero (0%)	Domain:		
IPSEC Client	Rpt Timer:	medium (8 s) 🔻	WiFi Bridge:	NONE		HS20 Capabilities		Consortium:		
IPsec-Unstream	IPSec GW:	0.0.0.0	IPSec Password:			HS20 Oper Class		RADIUS IP		
	IPSec Local ID.:		IPSec Remote ID.			HS20 WAN Metrics		RADIUS Port		
		Wi	Fi Settings			leee80211w:	Required (2)	RADIUS Secret	lantorge	
	SSID: ABC	D-OWE	AP: DE	FAULT		Venue Group:	Unspecified (0)	 Venue Type: 	Unspecified (0)	-
PROMISC	Key/Phrase: hell	0123	4ode: (80	02.11abqn-AC) 💌		Network Type:	Private (0)	Address Types:	Not Available (0)	-
TSO Enabled	Freq/Channel: 57	45/149	Rate: OS	Default 💌		Network Auth:		3GPP Cell Net:		
UFO Enabled	DTIM-Period: 2		Max-STA: 20	07		🗌 Use 80211d 🛛	Use 80211h 🛛 🔲 BSS-L	oad 🛛 🗌 Neighbor R	eports 🔄 BSS Transition	
GS0 Enabled	Beacon: 240					Advanced/802.1	x 🔲 Short-Preamble	HotSpot 2.0	Disable DGAF	
LRO Enabled	WPA WPA2	WPA3 OSEN	WEP	Verbose Debug		Enable 802.11u	0 802.11u Internet	802.11u ASRA	802.11u ESR 802.11u UESA	
GRO Enabled	Disable HT40	Disable HT80	Enable VHT160	Disable SGI						

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

		vap2 (ct521-1ac-f20) C	onfigure Sett	ings				
	Port Status Information								
	Current: LINK-UP GRO NONE								
	Driver Info: Port Type: WIFI-AP Parent: wiphy1 wiphy1								
	Port Configurables								
	Standard Configuration Ad	vanced Configuration	Mi	sc Configuratio	n Custom WiFi				
		More WiF	i Se	ttings					
	Enable TX0	SGI							
	TX-power:	Default (255)	-	Tries:	Single Tx (1)	-			
	Preamble:	OFDM (a/g) (0)	-	MCS:	0 (0)	-			
	NSS:	NSS 1 (0)	-	Bandwidth:	20 Mhz (0)	-			
	OCSP:	Disabled (0)	-						
	Freq-2.4:	0xfffffff		Freq-5:	0xfffffff				
	X-Coordinate:	0		Y-Coordinate:	0				
	Z-Coordinate:	0		Venue-ID:	0				
	Post IF-UP Script:					٩			
	Custom WPA Cfg	WPA Cfg: /home/lanforge/wifi/vap2-owe.com					- 		
	Allow Pri/Sec Switch								
_									
Print	Display <u>L</u> ogs	Probe Display	Sci	a <u>n</u> <u>S</u> ync	<u>Apply</u>	<u>o</u> K	<u>C</u> ancel		

D. Setup the STA with WPA3 security and no PSK on the standard configuration screen.

	sta204 (cl	t523-3n-f20) Confi	gure Settings							
Port Status Information Current: LINK-UP GRO Authorized Driver Info: Port Type: WIFI-STA Parent: wiphy2 wiphy2										
Port Configurables										
Standard Configuration	Advanced Configuration Misc Configuration Corruptions Custom WiFi									
Enable	General Interface Settings									
Set MAC	Down Aux-Mgt									
🔲 Set TX Q Len	DHCP-IPv <u>6</u>	DHCP Release	DHCP Vendor ID:	None						
Set MTU	☑ DHCP-IPv4	Secondary-IPs	DHCP Client ID:	None						
Set Offload	DNS Servers:	BLANK	Peer IP:	NA						
Set PROMISC	IP Address:	0.0.0.0	Global IPv6:	AUTO						
Services ——	IP Mask:	0.0.0.0	Link IPv6:	AUTO						
HTTP	Gateway IP:	0.0.0.0	IPv6 GW:	AUTO						
FTP	Alias:		MTU:	1500						
RADIUS	MAC Addr:	00:03:7f:a3:cc:00	TX Q Len	1000						
IPSEC-Client	Rpt Timer:	medium (8 s) 🔻	WiFi Bridge:	NONE						
🔲 IPsec-Upstream	IPSec GW:	0.0.0.0	IPSec Password:							
	IPSec Local ID.:		IPSec Remote ID.:							
TS0 Enabled	SSID: AB	CD-OWE	AP: DEFA	JULT						
UFO Enabled	Key/Phrase:		Mode: 802.3	llabqn-AC 💌						
GSO Enabled	Freq/Channel: 5	efault 💌								
LRO Enabled	WPA WPA2 WPA3 OSEN WEP									
GRO Enabled	Disable HT4	Disable HT40 Enable VHT160 Disable SGI								
Print Display	Probe [Display Scan Sv	nc <u>Apply</u>	y <u>O</u> K <u>C</u> ancel						

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.

	Driver	Info: Port Type: WIFI-S	TA	Parent: wiphy2	wiphy2
		Port Co	onfi	gurables	
Standar	d Configuration	Advanced Configuratio	n	Misc Configura	ation Corruptions Custom WiFi
		Advance	d Wi	Fi Settings	
9	Select 'WPA2' on th	e Standard Configurat	ion	screen to enab	le Advanced/802.1x
	and enable Advanc	ed/802.1x to enable m	ost	of these. Enab	ling 802.11u enables others.
k	Key Management:	OWE	-	HESSID:	
F	Pairwise Ciphers:	DEFAULT	•	Realm:	
0	Group Ciphers:	DEFAULT	•	Client Cert:	
N N	WPA PSK:	hello123		IMSI:	
E	EAP Methods:	DEFAULT	-	Milenage:	
E	EAP Identity:			Domain:	
E	EAP Anon Identity:			Consortium:	
E	EAP Password:			Phase-1:	
E	EAP Pin:			Phase-2:	
F	Private Key:			PK Password:	
C	CA Cert File:			PAC File:	
1	Network Auth:			leee80211w:	Required (2) 👻
	Advanced/802.1	x 🗌 Enable 802.11u		HotSpot 2.0	Enable PKC

F. A capture of the association.

0	\odot \bigcirc	×							
Eile	e <u>E</u> dit <u>V</u> iew <u>G</u> o <u>(</u>	<u>Capture Analyze Statisti</u>	ics Telephony <u>W</u> ireless <u>T</u>	ools <u>H</u> elp					
		= 🛅 🖹 🎑 🤇	◆ → 🖀 주 👱 🗔	•	€, €, ፹				
	📕 wlan.addr==00:03:7f:a3:cc:00 and wlan.addr==00:0e:8e:6c:2d:b5 🛛 🖉 🗨 Expression +								
No.	Time	Source	Destination	Protocol	Length Info		-		
	1298 14.469614504	00:0e:8e:6c:2d:b5	00:03:7f:a3:cc:00	802.11	233 Probe Response, SN=227	4, FN=0, Flags=, BI=240, SSID=ABCD-OWE			
	1325 14.721099536	00:03:7f:a3:cc:00	00:0e:8e:6c:2d:b5	802.11	90 Authentication, SN=257	, FN=0, Flags=			
	1327 14.722087175	00:02:71:22:00	00:03:71:33:00:00	802.11	242 Accordation Request S	b, FN=0, Flags=			
L C	1332 14.728191312	00:0e:8e:6c:2d:b5	00:03:7f:a3:cc:00	802.11	104 Action, SN=2277, EN=0.	Flags=.0			
	1334 14.728503653	00:0e:8e:6c:2d:b5	00:03:7f:a3:cc:00	802.11	200 Association Response,	SN=2278, FN=0, Flags=			
	1347 14.934144512	00:0e:8e:6c:2d:b5	00:03:7f:a3:cc:00	802.11	104 Action, SN=2280, FN=0,	Flags=.p			
	1394 15.140207519	00:0e:8e:6c:2d:b5	00:03:7f:a3:cc:00	802.11	104 Action, SN=2282, FN=0,	Flags=.p			
	1410 15.346202045	00:0e:8e:6c:2d:b5	00:03:7f:a3:cc:00	802.11	104 Action, SN=2284, FN=0,	Flags=.p			
	1429 15.552245876	00:0e:8e:6c:2d:b5	00:03:7f:a3:cc:00	802.11	104 Action, SN=2285, FN=0,	Flags=.p	4		
	14/9 15./62205591	00:00:20:20:00	00:00:80:60:20:05	802.11	242 ASSOCIATION Request, 5	N=259, FN=0, Flags=, SSID=ABCD-UWE			
	1483 15 767168734	00:0e:8e:6c:2d:b5	00:03:71:43:00:00	802.11	87 Action SN=2288 EN=0	Elans=			
	1485 15.767185458	00:0e:8e:6c:2d:b5	00:03:7f:a3:cc:00	802.11	87 Action, SN=2289, FN=0,	Flags=			
	1487 15.767566571	00:0e:8e:6c:2d:b5	00:03:7f:a3:cc:00	EAPOL	193 Key (Message 1 of 4)				
	1489 15.771306015			EAPOL	221 Key (Message 2 of 4)				
	1491 15.772482847	00:0e:8e:6c:2d:b5	00:03:7f:a3:cc:00	EAPOL	281 Key (Message 3 of 4)				
	1493 15.773088516	00:03:7f:a3:cc:00	00:0e:8e:6c:2d:b5	EAPOL	193 Key (Message 4 of 4)		•		
	<pre>Tag length: 8 Supported Rates: 6 (0x0c) Supported Rates: 9 (0x12) Supported Rates: 12 (0x18) Supported Rates: 12 (0x18) Supported Rates: 14 (0x30) Supported Rates: 44 (0x30) Supported Rates: 48 (0x6c) Supported Rates: 48 (0x6c) Supported Rates: 48 (0x6c) Tag Rumber: RSN Information Tag Number: RSN Information (48) Tag length: 26 RSN Version: 1 Fairvise cipher Suite : 00:0f:ac AES (CCM) Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption (18) </pre>								
	RSN Capabil PMKTD Count	ltles: 0x00c0							
	PMKID List						Ŧ		

Candela Technologies, Inc., 2417 Main Street, Suite 201, Ferndale, WA 98248, USA www.candelatech.com | sales@candelatech.com | +1.360.380.1618