sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

# Corrupting EAPOL-Key 3/4 Handshake Message RSNXE WPA-Key Information Elements

**Goal**: Manually override RSN-Extension-Element (RSNXE) of 3 of 4-way EAPOL authentication handshake messages sent by a LANforge system in AP Mode for testing purposes.

The `rsnxe_override_eapol` field in LANforge **Custom WiFi Parameters** provides capability to corrupt specific information elements of **EAPOL-Key Message 3 of 4** of WPA3 authentication sequence using SAE with encrypted management frames (802.11w). The Robust Security Network Extension Element (RSNXE), used to communicate and confirm certain aspects of security negotiation such as "SAE-hash-to-element", must be consistent between Beacon frames and EAPOL-Key messages; this method corrupts this RSNXE IE, provoking authentication failure with a distinctive response message: `WPA: RSNXE mismatch between Beacon/ProbeResp and EAPOL-Key msg 3/4`.

---

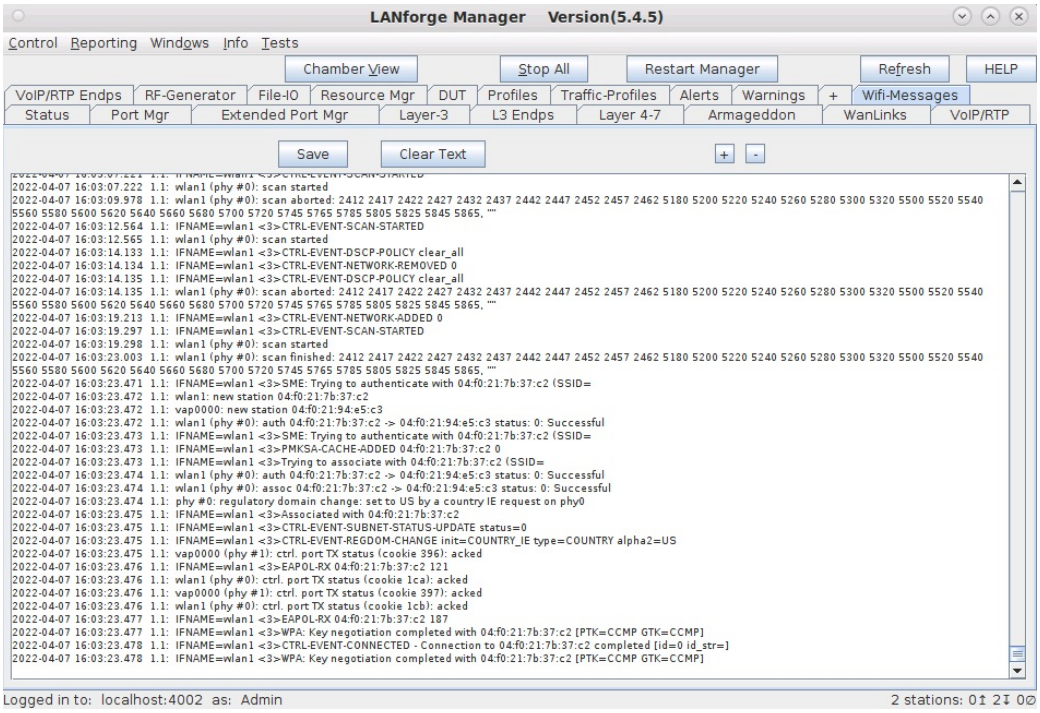
1. **Initial Setup for WPA3-Authentication Testing with Simultaneous Authentication of Equals (SAE).**
   The setup requires AP and station NIC drivers capable of enabling SAE encryption (this example uses MediaTEK radios with ath10k(988x) driver), enabling encrypted management frames (`802.11w`), enabling WPA3 and disabling WPA2-PSK authentication in both station and AP.
   A. Set up a virtual AP for testing.
      In this test, it is named `vap0000` on parent device `wiphy0`.
      For more information see Create VAP in Bridge Mode
   B. On a separate radio, create a station to authenticate with `vap0000`:
      In the **Port Manager** tab, select `wiphy1` and click **Create**; select **WiFi STA**, then click **Apply**.
      In this test, the station is named `wlan1` on parent device `wiphy1`.
      For more information see Generating Traffic for WLAN Testing
   C. Configure `vap0000` and `wlan1` to use **WPA3-SAE** encrypted authentication.
      Ensure that `802.11w` is enabled, since it is required for WPA3.
      For more information see Setting up WPA3
   D. Configure `vap0000` and `wlan1` with **SSID** `test-wpa2-psk` and **Keyphrase** `qwertyuiop`.
   E. Create a Monitor Port on its own radio to sniff wireless packets.
      In this test, the monitor port is named `moni3a`.
      For more information see Using Wireshark to Sniff WiFi Monitors

2. **Control (No Change):**
   A. Configure **Custom WiFi** in `vap0000`:
      Select `vap0000` and click **Modify**.
      Navigate to the **Custom WiFi** tab.
      Ensure that no `sae_commit_override` parameter is set in **User-Specified supplicant/hostapd configuration text**.
      Click **Apply** then **OK**.
   B. Set the vAP down and back up to allow changes to take effect:
      In the **Port Manager** tab, select `vap0000`.
      Admin all selected interfaces **DOWN** (CTRL-PLUS).
      Admin all selected interfaces **UP** (CTRL-MINUS).
   C. Sniff packets to observe the authentication behavior:
      On the observation system in the **Port Manager** tab, select only `moni3a`:
      Click **Sniff Packets**.

D. Observe the results, which should be similar to the following:
- The station `wlan1` succeeds in authenticating with `vap0000`.
- LANforge **WiFi Messages** shows `WPA: Key negotiation completed`.

E. Example results:

A. Behavior in LANforge **Wifi Messages**: Control Test




3. **RSNXE Mismatch in EAPOL-Key Message 3/4:**

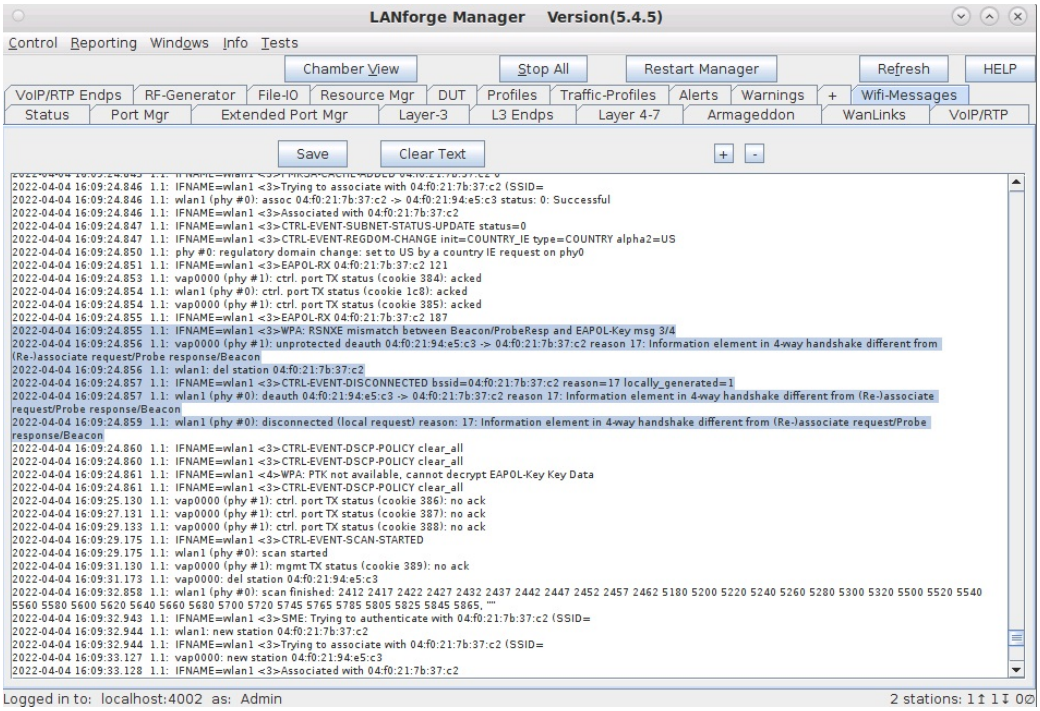
A. Configure **Custom WiFi** in `vap0000`:
Select `vap0000` and click **Modify**.
Navigate to the **Custom WiFi** tab.
In the **User-Specified supplicant/hostapd configuration text** field, write:
`rsnxe_override_eapol=F40100`.
Click **Apply** then **OK**.

B. Reset ports and sniff packets:
Repeat steps B through D of Step 2.

C. Observe the results, which should be similar to the following:
- Message 2/4 shows only encrypted in Wireshark due to having enabled `802.11w`.
- The station `wlan1` fails to authenticate with `vap0000`.
- LANforge **Wifi-Messages** recognizes `WPA:RSNXE mismatch between Beacon/ProbeResp and EAPOL-Key msg 3/4` and gives `CTRL-EVENT-DISCONNECTED for reason 17: Information element in 4-way handshake different from (Re-)associate request/Probe response/Beacon`.
- `Deauthentication` management frame is sent by the station with `Reason code: Information element in 4-way Handshake different from (Re)Association Request/Probe Response/Beacon frame (0x0011)`.
- Compare **EAPOL-Key Message 3 of 4** and **BEACON** RSNXE information for mismatch.

D. Example results:

A. Behavior in LANforge **Wifi Messages**: RSNXE Override Test




B. **Deauthentication**: RSNXE Override Test

```
    Type/Subtype: Deauthentication (0x000c)
  ▾ Frame Control Field: 0xc000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1100 .... = Subtype: 12
    ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: 04:f0:21:7b:37:c2
    Destination address: 04:f0:21:7b:37:c2
    Transmitter address: 04:f0:21:94:e5:c3
    Source address: 04:f0:21:94:e5:c3
    BSS Id: 04:f0:21:7b:37:c2
    .... .... .... 0000 = Fragment number: 0
    0001 0000 1000 .... = Sequence number: 264
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (2 bytes)
      Reason code: Information element in 4-Way Handshake different from (Re)Association Request/Probe Response/Beacon frame (0x0011)

0000  00 00 44 00 2f 40 40 a0  20 08 00 a0 20 08 00 a0   ··D·/@@·  ··· ···
0010  20 08 00 a0 20 08 00 00  0b 3a 77 fb 00 00 00 00   ···· ···  ·:w·····
0020  00 0c 3c 14 40 01 ee 00  00 00 00 00 00 00 00 00   ··<·@··· ········
0030  0b 3a 77 fb 00 00 00 00  00 00 01 01 ee 00 e3 01   ·:w····· ········
0040  e3 02 e4 03 c0 00 3c 00  04 f0 21 7b 37 c2 04 f0   ·····<·  ··!{7···
0050  21 94 e5 c3 04 f0 21 7b  37 c2 80 10 11 00         !·····!{ 7·····
```

C. **EAPOL-Key Message 3 of 4**: RSNXE Override Test

```
Frame 263: 289 bytes on wire (2312 bits), 289 bytes captured (2312 bits) on interface moni3a, id 0
Radiotap Header v0, Length 68
802.11 radio information
IEEE 802.11 QoS Data, Flags: ......F.
Logical-Link Control
802.1X Authentication
   Version: 802.1X-2004 (2)
   Type: Key (3)
   Length: 183
   Key Descriptor Type: EAPOL RSN Key (2)
   [Message number: 3]
 Key Information: 0x13c8
      .... .... .... .000 = Key Descriptor Version: Unknown (0)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .1.. .... = Install: Set
      .... .... 1... .... = Key ACK: Set
      .... ...1 .... .... = Key MIC: Set
      .... ..1. .... .... = Secure: Set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...1 .... .... .... = Encrypted Key Data: Set
      ..0. .... .... .... = SMK Message: Not set
   Key Length: 16
   Replay Counter: 2
   WPA Key Nonce: 6502b4fda34d00be8fba0cb671f6034263d9c8a92c21a73c…
   Key IV: 00000000000000000000000000000000
   WPA Key RSC: 0000000000000000
   WPA Key ID: 0000000000000000
   WPA Key MIC: 31e19714b1e9446765b97589060f326e
   WPA Key Data Length: 88
   WPA Key Data: 33dbdd5179a576dbc3f7d2b58baf36b897159e50d4f4ead7…
```

```
0000  00 00 44 00 2f 40 40 a0  20 08 00 a0 20 08 00 a0   ··D·/@@·  ··· ···
0010  20 08 00 a0 20 08 00 00  9e 01 77 fb 00 00 00 00    ··· ···  ··w·····
0020  00 0c 3c 14 40 01 e7 00  00 00 00 00 00 00 00 00   ··<·@··· ········
0030  9e 01 77 fb 00 00 00 00  00 00 01 01 e6 00 e2 01   ··w····· ········
0040  df 02 dc 03 88 02 24 00  04 f0 21 94 e5 c3 04 f0   ······$· ··!·····
0050  21 7b 37 c2 04 f0 21 7b  37 c2 10 00 07 00 aa aa   !{7···!{ 7·······
0060  03 00 00 00 88 8e 02 03  00 b7 02 13 c8 00 10 00   ········ ········
0070  00 00 00 00 00 00 02 65  02 b4 fd a3 4d 00 be 8f   ·······e ····M···
0080  ba 0c b6 71 f6 03 42 63  d9 c8 a9 2c 21 a7 3c 0d   ···q··Bc ···,!·<·
0090  4e 1c a1 59 af 0c 0f 00  00 00 00 00 00 00 00 00   N··Y···· ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 31  e1 97 14 b1 e9 44 67 65   ·······1 ·····Dge
00c0  b9 75 89 06 0f 32 6e 00  58 33 db dd 51 79 a5 76   ·u···2n· X3··Qy·v
00d0  db c3 f7 d2 b5 8b af 36  b8 97 15 9e 50 d4 f4 ea   ·······6 ····P···
00e0  d7 58 47 72 85 ea 2f 00  25 f4 d9 e0 3e 72 d5 f3   ·XGr··/· %···>r··
00f0  57 3c 6f 2d fa 34 42 22  fd c7 53 ef 12 7a 2d ad   W<o-·4B" ··S··z-·
0100  4f 08 a8 51 68 5e 0d 78  5a a7 d2 2b 31 35 ba ea   O··Qh^·x Z··+15··
0110  66 ee 01 42 6a 6e d2 69  88 fd e0 55 92 2e ef 05   f··Bjn·i ···U·.··
0120  91                                                ·
```

D. **BEACON**: RSNXE Override Test

```
Tagged parameters (248 bytes)
   Tag: SSID parameter set: juicer-wifi
   Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
   Tag: DS Parameter set: Current Channel: 36
   Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
   Tag: Country Information: Country Code US, Environment Any
   Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 20
      RSN Version: 1
    Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)
    RSN Capabilities: 0x00cc
         .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
         .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
         .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
         .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0x0)
         .... .... .1.. .... = Management Frame Protection Required: True
         .... .... 1... .... = Management Frame Protection Capable: True
         .... ...0 .... .... = Joint Multi-band RSNA: False
         .... ..0. .... .... = PeerKey Enabled: False
         ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
   Tag: Supported Operating Classes
   Tag: HT Capabilities (802.11n D1.10)
   Tag: HT Information (802.11n D1.10)
   Tag: Extended Capabilities (10 octets)
   Tag: VHT Capabilities
   Tag: VHT Operation
   Tag: VHT Tx Power Envelope
   Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
   Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)
   Ext Tag: MU EDCA Parameter Set
   Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

```
0000  00 00 44 00 2f 40 40 a0  20 08 00 a0 20 08 00 a0   ··D·/@@·  ··· ···
0010  20 08 00 a0 20 08 00 00  9c df 5d fb 00 00 00 00    ··· ···  ··]·····
0020  00 0c 3c 14 40 01 f2 00  00 00 00 00 00 00 00 00   ··<·@··· ········
0030  9c df 5d fb 00 00 00 00  00 00 01 01 f1 00 ea 01   ··]····· ········
0040  e6 02 eb 03 80 00 00 00  ff ff ff ff ff ff 04 f0   ········ ········
0050  21 7b 37 c2 04 f0 21 7b  37 c2 d0 04 47 40 93 2f   !{7···!{ 7···G@·/
0060  66 00 00 00 f0 00 11 00  00 0b 6a 75 69 63 65 72   f·······  ··juicer
0070  2d 77 69 66 69 01 08 8c  12 98 24 b0 48 60 6c 03   -wifi···  ··$·H`l·
0080  01 24 05 04 00 02 00 00  07 0c 55 53 20 24 08 17   ·$····· ··US $··
0090  64 0c 17 95 05 1e 30 14  01 00 00 0f ac 04 01 00   d·····0· ········
00a0  00 0f ac 04 01 00 00 0f  ac 08 cc 00 3b 02 80 00   ········ ····;···
00b0  2d 1a 6e 00 03 ff ff ff  ff 00 00 00 00 00 00 00   -·n····· ········
00c0  00 01 00 00 00 00 00 00  00 00 00 00 3d 16 24 05   ········ ····=·$·
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 7f 0a 04 00  00 02 00 00 00 40 00 40   ········ ·····@·@
00f0  bf 0c b1 59 8a 31 aa ff  00 00 aa ff 00 00 c0 05   ···Y·1·· ········
```