Support for Hash-to-Element for Password Element in SAE Authentication

Hash-to-Element (H2E)

Hash-to-Element (H2E) is a new SAE Password Element (PWE) method. In this method, the secret PWE used in the SAE protocol is generated from a password.

When a STA that supports H2E initiates SAE with an AP, it checks whether AP supports H2E. If yes, the AP uses the H2E to derive the PWE by using a newly defined Status Code value in the SAE Commit message.

If STA uses Hunting-and-Pecking, the entire SAE exchange remains unchanged.

While using the H2E, the PWE derivation is divided into the following components:

- Derivation of a secret intermediary element PT from the password. This can be performed offline when the password is initially configured on the device for each supported group.
- Derivation of the PWE from the stored PT. This depends on the negotiated group and MAC addresses of peers. This is performed in real-time during the SAE exchange.

Note

- The H2E method also incorporates protection against the Group Downgrade man-in-the-middle attacks. During the SAE exchange, the peers exchange lists of rejected groups binded into the PMK derivation. Each peer compares the received list with the list of groups supported, any discrepancy detects a downgrade attack and terminates the authentication.

YANG (RPC model)

To create an RPC for SAE Password Element (PWE) mode, use the following RPC model:

```
<nc:rpc xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:0a77124f-c563-469d-bd21-cc625a9691cc">
<nc:edit-config>
<nc:target>
<nc:running/>
</nc:target>
<nc:config>
<wlan-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-wlan-cfg">
<wlan-cfg-entries>
<wlan-cfg-entry>
<profile-name>test</profile-name>
<wlan-id>2</wlan-id>
<sae-pwe-mode>both-h2e-hnp</sae-pwe-mode>
</wlan-cfg-entry>
</wlan-cfg-entries>
</wlan-cfg-data>
</nc:config>
</nc:edit-config>
</nc:rpc>
```

Note The **delete** operation performs one action at a time due to the current infra limitation. That is, in YANG module, the **delete** operation on multiple nodes are not supported.

Configuring WPA3 SAE H2E

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan WPA3 1 WPA3`	Enters the WLAN configuration sub-mode.
Step 3	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 4	**no security ft over-the-ds** **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables fast transition over the data source on the WLAN.
Step 5	**no security ft** **Example:**	Disables 802.11r fast transition on the WLAN.

	Command or Action	Purpose
	`Device(config-wlan)# no security ft`	
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security. PMF is disabled now.
Step 7	**security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# security wpa wpa2 ciphers aes`	Configures WPA2 cipher. **Note** You can check whether cipher is configured using **no security wpa wpa2 ciphers aes** command. If cipher is not reset, configure the cipher.
Step 8	**security wpa psk set-key ascii** *value preshared-key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123`	Specifies a preshared key.
Step 9	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 10	**security wpa akm sae** **Example:** `Device(config-wlan)# security wpa akm sae`	Enables AKM SAE support.
Step 11	**security wpa akm sae pwe** {**h2e** | **hnp** | **both-h2e-hnp**} **Example:** `Device(config-wlan)# security wpa akm sae pwe`	Enables AKM SAE PWE support. PWE supports the following options: • h2e—Hash-to-Element only; disables HnP. • hnp—Hunting and Pecking only; disables H2E. • Both-h2e-hnp—Both Hash-to-Element and Hunting and Pecking support (Is the default option).
Step 12	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 13	**end** **Example:**	Returns to the privileged EXEC mode.

	Command or Action	Purpose
	Device(config-wlan)# end	

Verifying WPA3 SAE H2E Support in WLAN

To view the WLAN properties (PWE method) based on the WLAN ID, use the following command:

```
Device# show wlan id 1
WLAN Profile Name     : wpa3
================================================
Identifier                                       : 1
Description                                      :
Network Name (SSID)                              : wpa3
Status                                           : Enabled
Broadcast SSID                                   : Enabled
Advertise-Apname                                 : Disabled
Universal AP Admin                               : Disabled
Max Associated Clients per WLAN                  : 0
Max Associated Clients per AP per WLAN           : 0
Max Associated Clients per AP Radio per WLAN     : 200
OKC                                              : Enabled
Number of Active Clients                         : 0
CHD per WLAN                                     : Enabled
WMM                                              : Allowed
WiFi Direct Policy                               : Disabled
Channel Scan Defer Priority:
  Priority (default)                             : 5
  Priority (default)                             : 6
Scan Defer Time (msecs)                          : 100
Media Stream Multicast-direct                    : Disabled
CCX - AironetIe Support                          : Disabled
Peer-to-Peer Blocking Action                     : Disabled
DTIM period for 802.11a radio                    : 1
DTIM period for 802.11b radio                    : 1
Local EAP Authentication                         : Disabled
Mac Filter Authorization list name               : Disabled
Mac Filter Override Authorization list name      : Disabled
Accounting list name                             :
802.1x authentication list name                  : Disabled
802.1x authorization list name                   : Disabled
Security
    802.11 Authentication                        : Open System
    Static WEP Keys                              : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)       : Enabled
        WPA (SSN IE)                             : Disabled
        WPA2 (RSN IE)                            : Disabled
        WPA3 (WPA3 IE)                           : Enabled
            AES Cipher                           : Enabled
            CCMP256 Cipher                       : Disabled
            GCMP128 Cipher                       : Disabled
            GCMP256 Cipher                       : Disabled
        Auth Key Management
            802.1x                               : Disabled
            PSK                                  : Disabled
            CCKM                                 : Disabled
            FT dot1x                             : Disabled
            FT PSK                               : Disabled
            Dot1x-SHA256                         : Disabled
            PSK-SHA256                           : Disabled
            SAE                                  : Enabled
```

```
            OWE                                     : Disabled
            SUITEB-1X                               : Disabled
            SUITEB192-1X                            : Disabled
    SAE PWE Method                                  : Hash to Element(H2E)
    Transition Disable                              : Disabled
    CCKM TSF Tolerance (msecs)                      : 1000
    OWE Transition Mode                             : Disabled
    OSEN                                            : Disabled
    FT Support                                      : Disabled
        FT Reassociation Timeout (secs)             : 20
        FT Over-The-DS mode                         : Disabled
    PMF Support                                     : Required
        PMF Association Comeback Timeout (secs): 1
        PMF SA Query Time (msecs)                   : 200
    Web Based Authentication                        : Disabled
    Conditional Web Redirect                        : Disabled
    Splash-Page Web Redirect                        : Disabled
    Webauth On-mac-filter Failure                   : Disabled
    Webauth Authentication List Name                : Disabled
    Webauth Authorization List Name                 : Disabled
    Webauth Parameter Map                           : Disabled
Band Select                                         : Disabled
Load Balancing                                      : Disabled
Multicast Buffer                                    : Disabled
Multicast Buffers (frames)                          : 0
IP Source Guard                                     : Disabled
Assisted-Roaming
    Neighbor List                                   : Enabled
    Prediction List                                 : Disabled
    Dual Band Support                               : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                      : Enabled
    BSS Max Idle                                    : Enabled
        Protected Mode                              : Disabled
    Traffic Filtering Service                       : Disabled
    BSS Transition                                  : Enabled
        Disassociation Imminent                     : Disabled
            Optimised Roaming Timer (TBTTS)         : 40
            Timer (TBTTS)                           : 200
        Dual Neighbor List                          : Disabled
    WNM Sleep Mode                                  : Disabled
802.11ac MU-MIMO                                    : Enabled
802.11ax parameters
    802.11ax Operation Status                       : Enabled
    OFDMA Downlink                                  : Enabled
    OFDMA Uplink                                    : Enabled
    MU-MIMO Downlink                                : Enabled
    MU-MIMO Uplink                                  : Enabled
    BSS Target Wake Up Time                         : Enabled
    BSS Target Wake Up Time Broadcast Support  : Enabled
802.11 protocols in 2.4ghz band
    Protocol                                        : dot11bg
Advanced Scheduling Requests Handling           : Enabled
mDNS Gateway Status                                 : Bridge
WIFI Alliance Agile Multiband                   : Disabled
Device Analytics
    Advertise Support                               : Enabled
    Advertise Support for PC analytics          : Enabled
    Share Data with Client                          : Disabled
Client Scan Report (11k Beacon Radio Measurement)
    Request on Association                          : Disabled
    Request on Roam                                 : Disabled
WiFi to Cellular Steering                           : Disabled
Advanced Scheduling Requests Handling           : Enabled
```

```
Locally Administered Address Configuration
    Deny LAA clients                          : Disabled
```

To verify the client association who have used the PWE method as H2E or HnP, use the following command:

```
Device# show wireless client mac-address e884.a52c.47a5 detail
Client MAC Address : e884.a52c.47a5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 11.11.0.65
Client IPv6 Addresses : fe80::c80f:bb8c:86f6:f71f
Client Username: N/A
AP MAC Address : d4ad.bda2.e9e0
AP Name: APA453.0E7B.E73C
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : N/A
Wireless LAN Id: 1
WLAN Profile Name: wpa3
Wireless LAN Network Name (SSID): wpa3
BSSID : d4ad.bda2.e9ef
Connected For : 72 seconds
Protocol : 802.11ax - 5 GHz
Channel : 36
Client IIF-ID : 0xa0000001
Association Id : 2
Authentication Algorithm : Simultaneous Authentication of Equals (SAE)
Idle state timeout : N/A
Session Timeout : 1800 sec (Remaining time: 1728 sec)
Session Warning Time : Timer not running
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Disabled
Fastlane Support : Disabled
Client Active State : Active
Power Save : OFF
Current Rate : m6 ss2
Supported Rates : 6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 0 (kbps)
  QoS Realtime Average Data Rate Upstream    : 0 (kbps)
  QoS Burst Data Rate Upstream               : 0 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 0 (kbps)
  QoS Average Data Rate Downstream           : 0 (kbps)
  QoS Realtime Average Data Rate Downstream  : 0 (kbps)
  QoS Burst Data Rate Downstream             : 0 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 0 (kbps)
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 08/24/2021 04:39:47 Pacific
Client Join Time:
  Join Time Of Client : 08/24/2021 04:39:47 Pacific
Client State Servers : None
Client ACLs : None
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 72 seconds
```

```
Policy Type : WPA3
Encryption Cipher : CCMP (AES)
Authentication Key Management : SAE
AAA override passphrase : No
SAE PWE Method : Hash to Element(H2E)
Transition Disable Bitmap : None
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
Protected Management Frame - 802.11w : Yes
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : VLAN0011
Multicast VLAN : 0
WiFi Direct Capabilities:
  WiFi Direct Capable           : No
Central NAT : DISABLED
Session Manager:
  Point of Attachment : capwap_90000006
  IIF ID              : 0x90000006
  Authorized          : TRUE
  Session timeout     : 1800
  Common Session ID: 000000000000000C76750C17
  Acct Session ID  : 0x00000000
  Auth Method Status List
   Method : SAE
  Local Policies:
   Service Template : wlan_svc_default-policy-profile_local (priority 254)
    VLAN              : VLAN0011
    Absolute-Timer    : 1800
  Server Policies:
  Resultant Policies:
                VLAN Name         : VLAN0011
    VLAN              : 11
    Absolute-Timer    : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Implemented
11v DMS Capable : No
QoS Map Capable : Yes
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
Client Statistics:
  Number of Bytes Received from Client : 21757
  Number of Bytes Sent to Client : 4963
  Number of Packets Received from Client : 196
  Number of Packets Sent to Client : 37
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -72 dBm
  Signal to Noise Ratio : 20 dB
Fabric status : Disabled
Radio Measurement Enabled Capabilities
  Capabilities: Neighbor Report, Passive Beacon Measurement, Active Beacon Measurement,
Table Beacon Measurement
```

```
Client Scan Report Time : Timer not running
Client Scan Reports
Assisted Roaming Neighbor List
```

To view the number of SAE authentications using the H2E and HnP, use the following command:

```
Device# show wireless stats client detail
Total Number of Clients : 0

Protocol Statistics

--------------------------------------------------------------------------------
Protcol            Client Count
 802.11b              : 0
 802.11g              : 0
 802.11a              : 0
 802.11n-2.4GHz       : 0
 802.11n-5 GHz        : 0
 802.11ac             : 0
 802.11ax-5 GHz       : 0
 802.11ax-2.4 GHz     : 0
  802.11ax-6 GHz      : 0



Current client state statistics:
--------------------------------------------------------------------------------
  Authenticating         : 0
  Mobility               : 0
  IP Learn               : 0
  Webauth Pending        : 0
  Run                    : 0
  Delete-in-Progress     : 0


Client Summary
------------------------------
Current Clients : 0
Excluded Clients: 0
Disabled Clients: 0
Foreign Clients : 0
Anchor Clients  : 0
Local Clients   : 0
Idle Clients    : 0
Locally Administered MAC Clients: 0

client global statistics:
--------------------------------------------------------------------------------
Total association requests received              : 0
Total association attempts                       : 0
Total FT/LocalAuth requests                      : 0
Total association failures                       : 0
Total association response accepts               : 0
Total association response rejects               : 0
Total association response errors                : 0
Total association failures due to exclusion list      : 0
Total association drops due to multicast mac     : 0
Total association drops due to random mac        : 0
Total association drops due to throttling        : 0
Total association drops due to unknown bssid     : 0
Total association drops due to parse failure     : 0
Total association drops due to other reasons     : 0
Total association requests wired clients         : 0
Total association drops wired clients            : 0
```

```
Total association success wired clients          : 0
Total peer association requests wired clients    : 0
Total peer association drops wired clients       : 0
Total peer association success wired clients     : 0
Total association success wifi direct clients    : 0
Total association rejects wifi direct clients    : 0
Total association response errors                : 0
Total 11r ft authentication requests received    : 0
Total 11r ft authentication response success     : 0
Total 11r ft authentication response failure     : 0
Total 11r ft action requests received            : 0
Total 11r ft action response success             : 0
Total 11r ft action response failure             : 0
Total 11r PMKR0-Name mismatch                    : 0
Total 11r PMKR1-Name mismatch                    : 0
Total 11r MDID mismatch                          : 0
Total AID allocation failures                    : 0
Total AID free failures                          : 0
Total Roam Across Policy Profiles                : 0
Total roam attempts                              : 0
  Total CCKM roam attempts                       : 0
  Total 11r roam attempts                        : 0
  Total 11r slow roam attempts                   : 0
  Total 11i fast roam attempts                   : 0
  Total 11i slow roam attempts                   : 0
  Total other roam type attempts                 : 0
Total roam failures in dot11                     : 0

Total WPA3 SAE attempts                          : 0
Total WPA3 SAE successful authentications        : 0
Total WPA3 SAE authentication failures           : 0
  Total incomplete protocol failures             : 0
Total WPA3 SAE commit messages received          : 0
Total WPA3 SAE commit messages rejected                                    : 0
  Total unsupported group rejections                                       : 0
  Total PWE method mismatch for SAE Hash to Element commit received        : 0
  Total PWE method mismatch for SAE Hunting And Pecking commit received : 0
Total WPA3 SAE commit messages sent              : 0
Total WPA3 SAE confirm messages received         : 0
Total WPA3 SAE confirm messages rejected         : 0
  Total WPA3 SAE message confirm field mismatch  : 0
  Total WPA3 SAE confirm message invalid length  : 0
Total WPA3 SAE confirm messages sent             : 0
Total WPA3 SAE Open Sessions                     : 0
Total SAE Message drops due to throttling        : 0
Total WPA3 SAE Hash to Element commit received   : 0
Total WPA3 SAE Hunting and Pecking commit received : 0

Total Flexconnect local-auth roam attempts       : 0
  Total AP 11i fast roam attempts                : 0
  Total AP 11i slow roam attempts                : 0
  Total 11r flex roam attempts                   : 0
```