802.11r BSS Fast Transition

- Feature History for 802.11r Fast Transition, on page 1
- Information About 802.11r Fast Transition, on page 2
- Information About 802.11r Fast Transition for SAE (FT-SAE) Authenticated Clients, on page 3
- Restrictions for 802.11r Fast Transition, on page 4
- Monitoring 802.11r Fast Transition (CLI), on page 5
- Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI), on page 6
- Configuring 802.11r Fast Transition in an Open WLAN (CLI), on page 7
- Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI), on page 9
- Configuring 802.11r Fast Transition on a SAE Security-Enabled WLAN (GUI), on page 10
- Configuring 802.11r Fast Transition on an SAE Security-Enabled WLAN (CLI), on page 10
- Disabling 802.11r Fast Transition (GUI), on page 12
- Disabling 802.11r Fast Transition (CLI), on page 12
- Verifying 802.11r Fast Transition SAE, on page 12

Feature History for 802.11r Fast Transition

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature History for 802.11r Fast Transition

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	802.11r Fast Transition for SAE (FT-SAE) Authenticated Clients	From Cisco-IOS XE 17.9.1 release onwards, the Fast Transition supports SAE-based Fast Roaming support along with PMK caching. This feature is an addition to the existing PMK caching-based fast roam support.

Information About 802.11r Fast Transition

802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with a new AP is done even before the corresponding client roams to the target access point. This concept is called Fast Transition. The initial handshake allows a client and the access points to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and the access points after the client responds to the reassociation request or responds to the exchange with new target AP.

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

Client Roaming

For a client to move from its current AP to a target AP using the FT protocols, message exchanges are performed using one of the following methods:

- Over-the-Air—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- Over-the-Distribution System (DS)—The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the device.

Figure 1: Message Exchanges when Over–the–Air Client Roaming is Configured

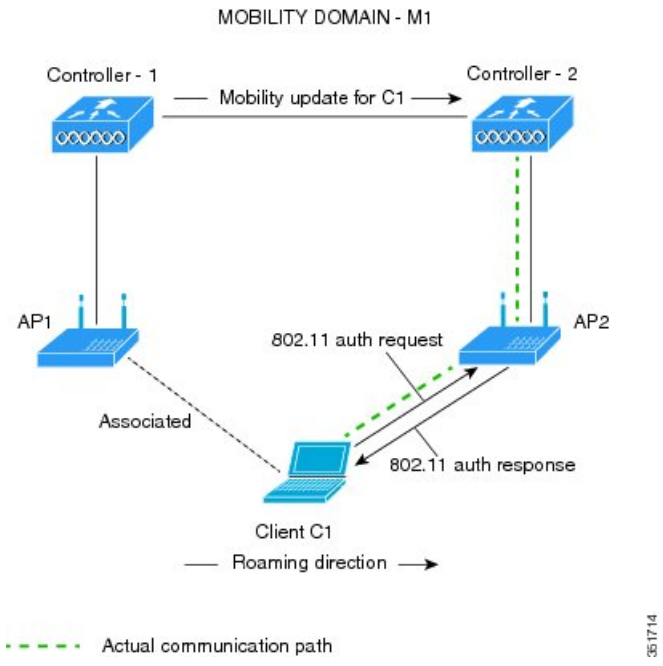
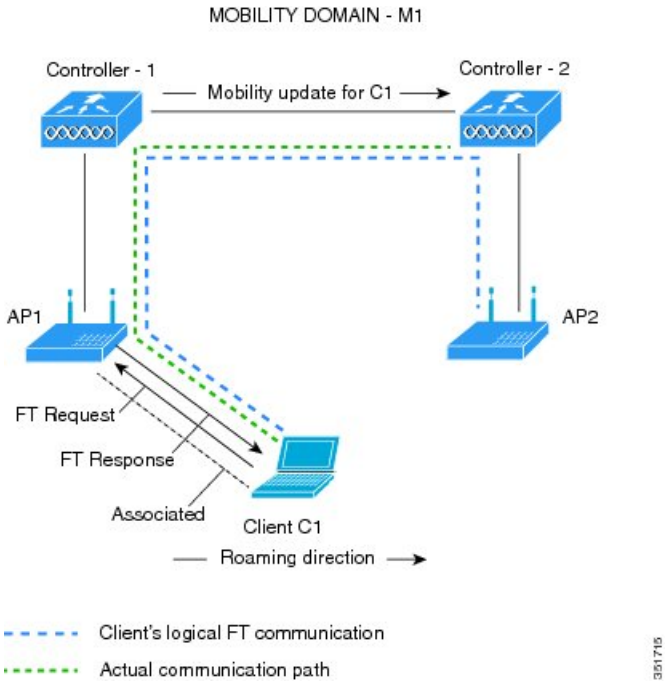


Figure 2: Message Exchanges when Over–the–DS Client Roaming is Configured



Note The 802.11r Fast Transition for SAE (FT-SAE) is not restricted to inter controller roaming.

Information About 802.11r Fast Transition for SAE (FT-SAE) Authenticated Clients

From Cisco-IOS XE 17.9.1 release onwards, the Fast Transition feature supports Simultaneous Authentication of Equals-based (SAE-based) fast roaming support along with Pairwise Master Key (PMK) caching.

This feature is an addition to the existing PMK caching-based fast roaming support.

Fast Transition Protocol

During a Base Station Subsystem (BSS) transition, the Fast BSS transition feature reduces the connectivity time loss between an Station (STA) and Direct Switching. The Fast Transition protocols are part of the reassociation service, and apply to the STA transitions between the APs in the same mobility domain and Exteneded Service Set (ESS). The Fast Transition protocols need information to be exchanged during the initial association (or a later reassociation) between an STA and an AP. The initial exchange is referred to as the *FT initial mobility domain association*. Similarly, subsequent reassociations to the APs in the same mobility domain use the Fast Transition protocols.

Note STA is known as Fast Transition Originator.

The following are the FT protocols:

- **Fast Transition Protocol**: This protocol is executed when a Fast Transition Originator makes a transition to a target AP and does not require a resource request before its transition.
- **Fast Transition Resource Request Protocol**: This protocol is executed when a Fast Transition Originator requires a resource request prior to its transition.
- **Over-the-Air**: The Fast Transition Originator communicates with the target AP using IEEE 802.11 authentication with Fast Transition authentication algorithm.
- **Over-the-DS**: The Fast Transition Originator communicates with the target AP using the current AP. The communication between the Fast Transition Originator and target AP is carried in Fast Transition action frames between the Fast Transition Originator and the current AP.

The Fast Transition feature supports a new AKM for FT-SAE, specifically the **00-0F-AC:9**.

Fast Transition Initial Mobility Domain Association

An STA includes Mobility Domain Element (MDE) and Robust Security Network Element (RSNE) in the (re)association request frame. The AP responds by including FTE, MDE, and RSNE in the (re)association response frame.

That is, an STA initiates the Fast Transition initial mobility domain association procedures by performing an IEEE 802.11 authentication using the SAE algorithm.

After successful SAE authentication, the STA and AP perform a Fast Transition four-way handshake.

Note

- If the MDE that is received by an AP or a controller does not match the contents advertised in the beacon and probe response frames, the AP or controller rejects the (re)association request frame with the STATUS_INVALID_MDE code.
- If an MDE is available in the (re)association request frame and the contents of RSNE do not indicate a negotiated SAE AKM of Fast BSS Transition (00-0F-AC:9 suite type), the AP rejects with STATUS_INVALID_AKMP code.

After an SAE authentication, the controller receives the PMK, resulting in the successful completion of SAE.

Restrictions for 802.11r Fast Transition

- EAP LEAP method is not supported.
- Traffic Specification (TSPEC) is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.

- If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The Cisco WLC handles 802.11r Fast Transition authentication requests during roaming for both Over-the-Air and Over-the-DS methods.
- Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r-capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

  The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r-enabled WLANs.

  Another workaround is to have two SSIDs with the same name, but with different security settings (FT and non-FT).
- Fast Transition resource–request protocol is not supported because clients do not support this protocol. Also, the resource–request protocol is an optional protocol.
- To avoid any Denial of Service (DoS) attack, each Cisco WLC allows a maximum of three Fast Transition handshakes with different APs.
- Non-802.11r–capable devices will not be able to associate with FT-enabled WLAN.
- We do not recommend 802.11r FT + PMF.
- We recommend 802.11r FT Over-the-Air roaming for FlexConnect deployments.
- FT-SAE Over-the-DS roam is not supported in FlexConnect local authentication mode.
- 802.11r ft-over-ds is enabled by default, when a WLAN is created in the controller . In Cisco Wave 2 APs, local switching local authentication with 802.11r is not supported. To make the local switching local authentication work with Cisco Wave 2 APs, explicitly disable 802.11r in WLAN. A sample configuration is given below:

```
wlan local-dot1x 24 local-dot1x
no security ft over-the-ds
no security ft adaptive
security dot1x authentication-list spwifi_dot1x
no shutdown
```

Monitoring 802.11r Fast Transition (CLI)

The following command can be used to monitor 802.11r Fast Transition:

Command	Description
show wlan name *wlan-name*	Displays a summary of the configured parameters on the WLAN.

Command	Description
show wireless client mac-address *mac-address*	Displays the summary of the 802.11r authentication key management configuration on a client. . . . . . . Client Capabilities CF Pollable : Not implemented CF Poll Request : Not implemented Short Preamble : Not implemented PBCC : Not implemented Channel Agility : Not implemented Listen Interval : 15 Fast BSS Transition : Implemented Fast BSS Transition Details : Client Statistics: Number of Bytes Received : 9019 Number of Bytes Sent : 3765 Number of Packets Received : 130 Number of Packets Sent : 36 Number of EAP Id Request Msg Timeouts : 0 Number of EAP Request Msg Timeouts : 0 Number of EAP Key Msg Timeouts : 0 Number of Data Retries : 1 Number of RTS Retries : 0 Number of Duplicate Received Packets : 1 Number of Decrypt Failed Packets : 0 Number of Mic Failured Packets : 0 Number of Mic Missing Packets : 0 Number of Policy Errors : 0 Radio Signal Strength Indicator : -48 dBm Signal to Noise Ratio : 40 dB . . . . . .

Configuring 802.11r BSS Fast Transition on a Dot1x Security Enabled WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**client vlan** *vlan-name* **Example:** `Device(config-wlan)# client vlan 0120`	Associates the client VLAN to this WLAN.
Step 4	**local-auth** *local-auth-profile-eap* **Example:** `Device(config-wlan)# local-auth`	Enables the local auth EAP profile.
Step 5	**security dot1x authentication-list default** **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 6	**security ft** **Example:** `Device(config-wlan)# security ft`	Enables 802.11r Fast Transition on the WLAN.
Step 7	**security wpa akm ft dot1x** **Example:** `Device(config-wlan)# security wpa akm ft dot1x`	Enables 802.1x security on the WLAN.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Configuring 802.11r Fast Transition in an Open WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.

	Command or Action	Purpose
Step 3	**client vlan** *vlan-id* **Example:** `Device(config-wlan)# client vlan 0120`	Associates the client VLAN to the WLAN.
Step 4	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA security.
Step 5	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 6	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 7	**no wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	**security ft** **Example:** `Device(config-wlan)# security ft`	Specifies the 802.11r Fast Transition parameters.
Step 9	**no shutdown** **Example:** `Device(config-wlan)# shutdown`	Shuts down the WLAN.
Step 10	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Configuring 802.11r Fast Transition on a PSK Security–Enabled WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**client vlan** *vlan-name* **Example:** `Device(config-wlan)# client vlan 0120`	Associates the client VLAN to this WLAN.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**security wpa akm ft psk** **Example:** `Device(config-wlan)# security wpa akm ft psk`	Configures Fast Transition PSK support.
Step 6	**security wpa akm psk set-key** {**ascii** {**0** | **8**} | **hex** {**0** | **8**}} **Example:** `Device(config-wlan)# security wpa akm psk set-key ascii 0 test`	Configures PSK AKM shared key.
Step 7	**security ft** **Example:** `Device(config-wlan)# security ft`	Configures 802.11r Fast Transition.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config-wlan)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode

Configuring 802.11r Fast Transition on a SAE Security-Enabled WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Profile Name**, the **SSID**, and the **WLAN ID**.

Step 4 Choose **Security** > **Layer2** tab.

Step 5 Click the **WPA3** radio button as security mode.

Step 6 Check the required **WPA Parameters** check boxes and the **AES(CCMP128)** check box.

Step 7 From the **Status** drop-down list, choose **Enabled**.

Step 8 Check the **FT+SAE** check box.

Step 9 Enter the **Pre-Shared Key**.

Step 10 From the **PSK Format** drop-down list, choose PSK Format and from the **PSK Type** drop-down list, choose PSK Type.

Step 11 Click **Apply to Device**.

Configuring 802.11r Fast Transition on an SAE Security-Enabled WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enables configuration mode.

	Command or Action	Purpose
Step 3	**wlan** *wlan-name wlan-id ssid* **Example:** `Device(config)# wlan wlan-ft-sae 10 wlan-ft-sae`	Configures the WLAN and SSID.
Step 4	**security ft** **Example:** `Device(config-wlan)# security ft`	Enables 802.11r Fast Transition on the WLAN.
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**security wpa psk set-key ascii** *asciii/hex key* **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 123456789`	Configures the preshared key on a WLAN. **Note** WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
Step 7	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 8	**security wpa akm ft sae** **Example:** `Device(config-wlan)# security wpa akm ft sae`	Configures 802.11r Fast Transition on an SAE security–enabled WLAN.
Step 9	**security wpa wpa3** **Example:** `Device(config-wlan)# security wpa wpa3`	Enables WPA3 support.
Step 10	**security pmf mandatory** **Example:** `Device(config-wlan)# security pmf mandatory`	Requires clients to negotiate 802.11w PMF protection on a WLAN.
Step 11	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Disabling 802.11r Fast Transition (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **WLANs** page, click the WLAN name.

Step 3 In the **Edit WLAN** window, click the **Security** > **Layer2** tab.

Step 4 From the **Fast Transition** drop-down list, choose **Disabled**. Note that you cannot enable or disable Fast Transition, if you have configured an SSID with Open Authentication.

Step 5 Click **Update & Apply to Device**.

Disabling 802.11r Fast Transition (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** `Device# wlan test4`	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*] **Example:** `Device(config-wlan)# no security ft over-the-ds`	Disables 802.11r Fast Transition on the WLAN.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Verifying 802.11r Fast Transition SAE

To view the Fast Transition SAE details, use the following command:

```
Device# show wireless client summary
Number of Clients: 1
```

```
MAC Address AP Name Type ID State Protocol Method Role
-------------------------------------------------------------------------------------------------------------------
2c33.7a5b.8fc5 APF4BD.9EBD.A66C WLAN 10 Run 11n(2.4) FT-SAE Local

Number of Excluded Clients: 0
```

To view the client summary details from an AP, use the following command:

```
AP# show client summary

Radio Driver client Summary:
============================
apr0v1
-------
apr0v4
-------
ADDR AID CHAN TXRATE RXRATE RSSI MINRSSI MAXRSSI IDLE TXSEQ RXSEQ CAPS XCAPS ACAPS ERP STATE
 MAXRATE(DOT11) HTCAPS VHTCAPS ASSOCTIME IEs MODE RXNSS TXNSS PSMODE
a0:fb:c5:ab:c3:41 1 11 114M 97M -47 -60 -40 0 0 65535 EPSs BORI NULL 0 f 286800 AP 1g
00:19:53 RSN WME IEEE80211_MODE_11AXG_HE20 2 2 1
LM BRP BRA
RSSI is combined over chains in dBm
Minimum Tx Power : 0
Maximum Tx Power : 0
HT Capability : Yes
VHT Capability : No
MU capable : No
SNR : 48
Operating band : 2.4GHz
Current Operating class : 0
Supported Rates : 2 4 11 22 12 18 24 36 48 72 96 108
Channels supported : 2412 2417 2422 2427 2432 2437 2442 2447 2452 2457 2462 2467 2472
Max STA phymode : IEEE80211_MODE_11AXG_HE20
apr1v1
-------
apr1v4
-------

WCP client Summary:
====================
mac radio vap aid state encr Maxrate Assoc Cap is_wgb_wired wgb_mac_addr
A0:FB:C5:AB:C3:41 0 4 1 FWD AES_CCM128 MCS92SS HE HE false 00:00:00:00:00:00



Assoc time:
============
mac assoc_time
A0:FB:C5:AB:C3:41 00d:00h:19m:55s


Datapath IPv4 client Summary:
=============================
id vap port node tunnel mac seen_ip hashed_ip sniff_ago confirm_ago
A0:FB:C5:AB:C3:41 4 apr0v4 6.4.26.28 - A0:FB:C5:AB:C3:41 192.100.2.153 10.0.21.68 0.110000
 0.100000

Datapath IPv6 client Summary:
=============================
client mac seen_ip6 age scope port
1 A0:FB:C5:AB:C3:41 fe80::c2f:f0c4:9fa5:2608 1 link-local apr0v4
```

To view FlexConnect-related details from an AP, use the following command:

```
AP# show flexconnect dot11R

Total number of DOT11R cache entries: 1

HW Address Life Time(s) BSSID R0KhId R1KhId vlanOverride aclOverride ipv6AclOverride
qosOverride iPSK
A0:FB:C5:AB:C3:41 558 2C:57:41:59:F5:C4 239.13.224.36 45:49:7B:38:11:6A N/A 0 \<>
```

To view the authentication key management details, use the following command:

```
Device# show wireless client mac-address 28c2.1f54.e6d6 detail
Authentication Algorithm : Open System
Authentication Key Management : FT-SAE
FlexConnect Authentication : Central
```

To verify whether AKM Fast Transition-SAE is enabled or not, use the following command:

```
Device# show wlan name [wlan-profile-name]

Auth Key Management
FT SAE : [Enabled | Disabled]
```

To verify the PMK cache details, use the following command:

```
Device# show wireless pmk-cache
……..
Type Dot11R
……..
```

To view the WPA3 SAE details, use the following command:

```
Device# show wireless stats client detail

Total FT/LocalAuth requests                      : 20
Total 11r ft authentication requests received    : 9
Total 11r ft authentication response success     : 9
Total 11r ft authentication response failure     : 0
Total 11r ft action requests received            : 17
Total 11r ft action response success             : 8
Total 11r ft action response failure             : 9
Total 11r PMKR0-Name mismatch                    : 0
Total 11r PMKR1-Name mismatch                    : 5
Total 11r MDID mismatch                          : 9
Total roam attempts                              : 15
  Total 11r roam attempts                        : 15
……
……
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       : 8
  Total 11r flex roam attempts                   : 0
….. .
….
Total client delete reasons
  SAE authentication failure                                    : 0
  DOT11 SAE invalid message                                     : 0
```