Fortinet Event Logging Facility

(FortiWLC Station Log)

Table of Contents

This document describes some common station log events generated by FortiWLC. The triggered events are consolidated, captured and displayed in the station logs.

MAC Filtering

A mobile station goes through this stage when a MAC filtering is enabled. A MAC filtering is either ACL-based or RADIUS-based. If the authentication of MAC filtering succeeds, a mobile station goes through the next stage, assignment. Otherwise, the mobile station is not assigned to any of AP.

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Mac in permit list - accept client	A client is present in controller local permit list and so MAC authentication succeeded. (In sec profile PERMIT list chosen)	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Mac not in permit list - reject client	A client is not present in controller local permit list and so MAC authentication failed and client rejected from assignment.(In sec profile PERMIT list chosen)	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Mac not in deny list - accept client	A client is not present in controller local deny list and so MAC authentication succeeded.(In sec profile DENY list chosen)	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Mac in deny list - reject client	A client is present in controller local deny list and so MAC authentication failed.(In sec	Informative

Event	Description	Action
	profile DENY list chosen)	
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Sent Radius request	RADIUS MAC filtering is enabled and hence RADIUS MAC filtering request is sent to RADIUS server for authentication.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Radius authentication succeeded (vlan 0)	RADIUS MAC filtering succeeded and client will be provided assignment.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Radius authentication failed	RADIUS MAC filtering succeeded and client will be rejected assignment.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Mac not in deny list - Radius Mac Filter enabled	A client is not in controller deny list and RADIUS authentication is enabled.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Failed to send Radius request - reject client	Connection attempts to a RADIUS server marked as unreachable.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Mac not in permit list - Radius Mac Filter enabled	When both RADIUS and local MAC filtering are enabled and local MAC filtering fails (permit list) and tries to validate	Informative

Event	Description	Action
	the client authentication via RADIUS.	

Example

This section gives examples of events when a MAC filtering is enabled.

```
 In Radius database: 00:66:77:c2:02:01
            In permit list: 00:66:77:c2:03:01
            In deny list: 00:66:77:c2:04:01

            (1) ACL = permit mode, Radius = enabled


2017-Sep-30 14:01:21.029511 | 00:66:77:c2:02:01 | Mac Filtering  | Sent Radius
request
2017-Sep-30 14:01:21.031167 | 00:66:77:c2:02:01 | Mac Filtering  | Radius
authentication succeeded (vlan 0)
2017-Sep-30 14:01:40.996531 | 00:66:77:c2:02:06 | Mac Filtering  | Sent Radius
request
2017-Sep-30 14:01:41.997881 | 00:66:77:c2:02:06 | Mac Filtering  | Radius
authentication failed
2017-Sep-30 14:03:47.544390 | 00:66:77:c2:03:01 | Mac Filtering  | Mac in permit
list - accept client
2017-Sep-30 14:04:04.829993 | 00:66:77:c2:04:01 | Mac Filtering  | Sent Radius
request
2017-Sep-30 14:04:05.832154 | 00:66:77:c2:04:01 | Mac Filtering  | Radius
authentication failed

            (2) ACL = deny mode, Radius = enabled


2017-Sep-30 15:11:37.925101 | 00:66:77:c2:03:01 | Mac Filtering  | Sent Radius
request
2017-Sep-30 15:11:38.926267 | 00:66:77:c2:03:01 | Mac Filtering  | Radius
authentication failed
2017-Sep-30 15:11:52.097631 | 00:66:77:c2:04:01 | Mac Filtering  | Mac in deny list
- reject client
2017-Sep-30 15:13:38.194093 | 00:66:77:c2:02:01 | Mac Filtering  | Radius
authentication succeeded (vlan 0)
2017-Sep-30 15:13:45.730981 | 00:66:77:c2:02:06 | Mac Filtering  | Sent Radius
request
2017-Sep-30 15:13:46.732779 | 00:66:77:c2:02:06 | Mac Filtering  | Radius
authentication failed

            (3) ACL = deny mode, Radius = disabled


2017-Sep-30 14:18:36.413893 | 00:66:77:c2:03:01 | Mac Filtering  | Mac not in deny
list - accept client
2017-Sep-30 14:18:41.310501 | 00:66:77:c2:04:01 | Mac Filtering  | Mac in deny list
- reject client
```

Fortinet Station Assignment

A mobile station must be assigned to a BSSID of an ESSID in order to get associated to the BSSID. A mobile station can be assigned to more than one BSSID at a time. When a mobile station doesn't get associated to a BSSID after assigned within a configured time, Station Assignment Aging Time under qosvars, the assignment state is removed. A mobile station can be unassigned to a BSSID because of the threshold of a load balancing or the threshold of AP limit.

Note: A-BSSID refers to a 5GHz band, B-BSSID refers to a 2.4GHz band.

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | <AID=1>[bg](v0) assigned to <AP=31> ESSID=swhan-essid BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Station probed	A mobile station gets assigned to the BSSID as it sends a Probe message to BSSID. Once a mobile station is assigned to AP::ESSID::BSSID, the mobile can proceed to the next stage, 802.11 authentication/association. The AID value is assigned to the station if it goes through 802.11 authentication/association.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | <AID=16>[abgn](v0) removed from <AP=11> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Normal Handoff	When a mobile station assignment to an AP is removed due to normal handoff.	Informative
2017-Oct-10 08:02:49.058278 | 00:40:96:ad:d4:3c | Station Assign | <AID=1>[bg](v0) assigned to <AP=5> ESSID=Clear_ESS BSSID=00:0c:e6:8a:01:f5 Ch=6 reason=Normal handoff	When a mobile station is assigned to a new AP due to normal handoff.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | <AID=81>[ab](v0) removed from <AP=11> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Assignment Age Out	A mobile station's assignment state gets removed from AP::ESSID::BSSID.	Informative

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | <AID=81>[ab](v0) removed from <AP=11> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Band steering	A mobile station's assignment state gets removed from AP::ESSID::BSSID due to Band Steering operation.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=81>[ab](v0) removed from <AP=11> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=No Serving AP	A mobile station's assignment state gets removed from AP::ESSID::BSSID due to no Assigned AP or Alternate AP is available.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=81>[ab](v0) removed from <AP=11> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Removal Due to LB	A mobile station's assignment state gets removed from AP::ESSID::BSSID due to Load Balancing.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=80211State downgraded	A mobile station's assignment state gets removed from AP::ESSID::BSSID due to downgrade in 802.11 state.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Forced removal for sync with AP	When Controller and AP are out of sync for Station Assignment, Controller forcefully removes Station assignment from AP to bring the state back in sync.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=NMS requested delete	Controller removes assignment when the NMS process running inside the controller requests for removing	Informative

Event	Description	Action
	the station. This can happen for instance when the *no station stamac* command is used.	
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Assignment aged out	Controller removes assignment when an assignment is unused (unassociated) for more than the *Assignment Aging Time*. This is a routine cleanup operation.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Inactivity timer expired	Controller removes assignment when an associated station remains inactive for more than the inactivity timer. The default value of this timer is 2000 seconds.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Macfiltering config changed	Whenever there is a change in the ACL configuration of MAC filtering, all assignments for the station are removed.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Client moved to wired network	When a wireless client MAC address is visible on the wired side of the controller, controller removes wireless assignment of that client.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31>	When controller encounters an	Informative

Event	Description	Action
ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Route update failed	internal error when updating route for a station, assignments for that station are removed.	
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | Sent deauth remove to <AP=1> ESSID=swhan-essid Ch=36 BSSID=00:0c:e6:9d:4f:be reason=NMS requested delete	Controller instructs AP to send a deauth to the station and also at the same time removes assignment for the station. This can happen for example when coord steers a station away from its associated band. Another scenario is when “no station” command is executed.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | Sent deauth remove to <AP=1> ESSID=swhan-essid Ch=36 BSSID=00:0c:e6:9d:4f:be reason=CAC orig failed	When a SIP call origination fails due to CAC limits being reached and if CAC deauth feature is turned on, controller deauths and removes assignment for the client.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | Sent deauth remove to <AP=1> ESSID=swhan-essid Ch=36 BSSID=00:0c:e6:9d:4f:be reason=CAC limited	When a voice client having an active call roams to an AP which is unable to accept a new call due to CAC limits being reached, controller deauths the station and also removes its assignment.	Informative

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | Sent deauth to <AP=1> ESSID=swhan-essid Ch=36 BSSID=00:0c:e6:9d:4f:be reason=Radius session expire	A mobile station's assignment state gets removed from AP::ESSID::BSSID due to expiry of RADIUS Session.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | Sent deauth to <AP=1> ESSID=swhan-essid Ch=36 BSSID=00:0c:e6:9d:4f:be reason=Radius session inactive	When the RADIUS session of a station becomes inactive (i.e it has been inactive for the configured time), controller disconnects the client.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | Sent deauth to <AP=1> ESSID=swhan-essid Ch=36 BSSID=00:0c:e6:9d:4f:be reason=User requested termination	A mobile station's assignment state gets removed from AP::ESSID::BSSID due to User requested RADIUS session termination; when the internal captive portal user clicks *logout*.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Ping pong	A mobile station's assignment state gets removed from AP::ESSID::BSSID due to ping pong to another BSSID.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6 reason=Client moved to wired network	Client has migrated to wired network from wireless.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | <AID=1>[ab](v0) removed from <AP=31> ESSID=corp-peap-mix BSSID=00:0c:e6:9d:4f:be Ch=6	A mobile station's assignment state gets removed from	Informative

Event	Description	Action
reason=Service removed	AP::ESSID::BSSID due to removal of SSID from the radio interface.	
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | Rejecting assignment: no free slot on ATS[00:0c:e6:16:dd:39] in string-BSSID [00:0c:e6:9d:4f:be]	Controller rejects assignment due to AP being CPU overloaded as known from the client capacity messages sent by the AP.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | Rejecting assignment on A-BSSID [00:0c:e6:9d:4f:be] because MaxCallsPerBss(4) reached (CAC limited)	A mobile station's assignment is rejected due to *MaxCallsPerBss* limit.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | Rejecting assignment on ATS[00:0c:e6:16:dd:39] because MaxCallsPerAP(10) reached	A mobile station's assignment is rejected due to *MaxCallsPerAP* limit.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | Rejecting assignment on ATS[00:0c:e6:16:dd:39] because MaxCallsPerInterfRegion(14) reached	A mobile station's assignment is rejected due to *MaxCallsPerInterRegion* limit.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | Rejecting assignment. ATS [00:0c:e6:16:dd:39] has reached MaxClientsPerAP(40) staSize=140 numAPAss=128/41 numBssAss=106	A mobile station's assignment is rejected due to *MaxClientsPerAP* limit.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | Rejecting assignment on nonassignable (LB) A-BSSID [00:0c:e6:9d:4f:be] num_associated(10) num_assigned(15)	Controller rejects assignment on a BSSID that is marked non-assignable as per LB algorithm.	Informative

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | Rejecting assignment on overfull A-BSSID [00:0c:e6:9d:4f:be] num_assigned(5) maxStaPerBss(4)	A mobile station's assignment is rejected when the *MaxStaPerBss* limit is reached and the native load balance overflow is disabled.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | BSSID[00:0c:e6:9d:4f:be] becomes blocked due to LB numAssoc(7) lowAssoc(3) maxAssocDiff(3)	Due to blocking by LB, a BSSID becomes non-assignable.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | BSSID[00:0c:e6:9d:4f:be] becomes unblocked due to LB numAssoc(5) lowAssoc(3) maxAssocDiff(3)	Due to unblocking LB, a blocked Bssid becomes assignable.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | MaxStaPerBss of ESS[swhan-essid] intf:1 increased from 4 to 7	Controller sets a new increased *MaxStaPerBss* value for a particular BSS on a given ESS ID, as per the LB algorithm.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | MaxStaPerBss of ESS[swhan-essid] intf:1 decreased from 7 to 6	Controller sets a new decreased *MaxStaPerBss* value for a particular BSS on a given ESS ID, as per the LB algorithm.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | Rejecting assignment due to MaxCallsPerBssid(4) reached on A-BSSID [00:0c:e6:9d:4f:be]	A mobile station's assignment is rejected due to *MaxCallsPerBssid* Limit.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | Rejecting assignment on B-BSSID[00:0c:e6:9d:4f:be] on ATS[00:0c:e6:16:dd:39] as	A mobile station's assignment is rejected due to	Informative

Event	Description	Action
MaxCallsPerAP(4) reached	*MaxCallsPerAP* limit.	
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | Rejecting assignment on A-BSSID[00:0c:e6:9d:4f:be] due to maximum number of stations (500) reached.	A mobile station's assignment is rejected due to *MaxStations* Limit.	Informative
2017-Oct-10 08:02:49.056279 | 00:0f:8f:9d:d3:23 | Station Assign | Rejecting assignment on BSSID[00:0c:e6:9d:4f:be] due to aid generation failure	A mobile station's assignment is rejected due to AID Generation failure.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | VLAN pool office capacity exceeded. No VLAN assigned.	VLAN capacity exceeded	Increase maximum number of clients in the VLANs of pools, if already at maximum possible no action can be taken.
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | <AID=1>[an](v0) deauthed and assigned to <AP=3> ESSID=corpwifi BSSID=00:0c:e6:9d:4f:be Ch=36 reason=Re-assignment due to handoff nack	Reset of assignment done followed by deauth.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | VLAN tag 11 assigned from VLAN pool office.	A VLAN has been assigned to the client from the VLAN pool.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | <AID=81>[ab](v0) Reassigning from <AP=6>(rssi=70) to <AP=4>(rssi=52) ESSID=corp-wifi Ch=36 A-BSSID=00:0c:e6:9d:4f:be	Changing the assignment of unassociated station from one AP to another due to better rssi s received for station on new AP.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | Rejecting assignment. ATS [00:0c:e6:16:dd:39] has reached MaxClientsPerAP(100)	Assigment for wired station get rejected when maximum number of stations	Informative

Event	Description	Action
	supported for AP is reached	
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | Rejecting assignment due to maximum number of stations (128) reached.	Assignment for wired station get rejected when maximum number of stations supported for controller is reached.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | VLAN tag [3] specified in VLAN pool [0] not found.	An error case, in which a VLAN specified in VLAN pool has been removed, should not normally happen.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | wired Assign to <AP_ID=10>(v0)	Wired station get assignment on AP.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Station Assign | wired Assign Removed From <AP_ID=12>(v0)	Wired station assignment removed from AP.	Informative

Band Steering Feature

Band Steering feature can be enabled/disabled on Per ESS basis. If Band steering is enabled, Fortinet System will try to steer stations trying to connect on that ESS ID to the preferred band. In case, Station cannot be steered within a time frame, steering will be stopped and station can connect to any band. For more details on configuration and usage, please refer the configuration guide.

Event	Description	Action
2018-May- 5 07:41:02.235862 | 00:26:82:12:21:55 | Band Steering | <AID=81>[ab](v0) Steering to 5Ghz under policy=N Blocking 2.4Ghz, present staType=ABGN ESSID=corp-wifi 5Ghz-BSSID=00:0c:e6:9d:4f:be Ch=36	N-Type Band Steering is enabled on ESS Id on which Station is trying to connect. Since station is trying on 2.4 GHz band and it has ABGN capability, N-Steering has been initiated to steer the client to 5 GHz band.	Informative
2018-May- 5 07:41:03.650448 | 00:26:82:12:21:55 | Band Steering | <AID=81>[ab](v0) Steered to 5Ghz under policy=N staType=ABGN[15] ESSID=engwifi A-BSSID=00:0c:e6:9d:4f:be Ch=36 Steering time = 1.414671 seconds	N-Type Band Steering is enabled on ESS Id on which Station is trying to connect. While station was trying on 2.4 GHz, it was steered successfully to connect on 5 GHz.	Informative
2017-Oct-10 08:02:49.056279 | 00:26:82:12:21:55 | Band Steering | <AID=81>[ab](v0) Steering disabled due to SteeringTimeout(5) policy=N, present staType=ABGN ESSID=engwifi A-BSSID=00:0c:e6:9d:4f:be Ch=36	N-Type Band Steering is enabled on ESS ID on which Station is trying to connect. After 5 GHz (preferred) band steering was initiated, Station did not connect on preferred band, so Band steering is disabled.	Informative
2017-Oct-10 08:02:49.056279 | 00:26:82:12:21:55 | Band Steering | <AID=81>[ab](v0) Band steering re-enabled	Band Steering tries to steer the client to	Informative

Event	Description	Action
under policy = N, staType = ABGN	preferred band for pre-defined time period. If client does not connect within that time period on preferred band, then Band Steering is disabled. And client is allowed to connect on any band. After this, If client somehow comes back on preferred band, then this message is generated. After this, band steering won't send assignment on forbidden band, client itself has connected on preferred band.	
2017-Oct-10 08:02:49.056279 | 00:21:6a:6c:00:9e | Band Steering | <AID=81>[ab](v0) Self-steered to 5Ghz under policy = N staType = ABGN ESSID=engwifi 5Ghz-BSSID=00:0c:e6:9d:4f:be Ch=36 Steering time = 0	When the band steering is enabled on the ESS ID and the client itself start probing on preferred band, then this message is seen.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Band Steering | <AID=81>[ab](v0) Steering disabled due to no preferred band found under policy=N for staType=abgn ESSID=corp-wifi 5Ghz-BSSID=00:0c:e6:9d:4f:be Ch=6	No indication from the station to the AP to proceed on the preferred band; band steering times out.	Informative

Example

```
(1) Successful Band Steering Operation

2018-May- 5 07:41:02.033668 | 00:26:82:12:21:55 | Station Assign  |   <AID=6>[abgn](v0)
assigned to <AP=29> ESSID=bwfwpa2psk BSSID=00:0c:e6:7e:32:dc Ch=36 reason=Station probed
2018-May- 5 07:41:02.235862 | 00:26:82:12:21:55 | Band Steering  |   <AID=81>[ab](v0) Steering
to 5Ghz under policy=N Blocking 2.4Ghz, present staType=ABGN ESSID=corp-wifi 5Ghz-
```

```
BSSID=00:0c:e6:9d:4f:be Ch=36
2017-Oct-10 08:02:49.056279 | 00:26:82:12:21:55 | 802.11 State  | * <AID=81>[abgn](v0) state
change <old=Unauthenticated> <new=Authenticated> <AP[4]=00:0c:e6:11:26:43> ESSID=engwifi Ch=36
A-<BSSID=00:0c:e6:7e:32:dc>
2017-Oct-10 08:02:49.056279 | 00:26:82:12:21:55 | 802.11 State  | * <AID=81>[abgn](v0) state
change <old=Authenticated> <new=Associated> <AP[4]=00:0c:e6:11:26:43> ESSID=engwifi Ch=36 A-
<BSSID=00:0c:e6:7e:32:dc>
2018-May- 5 07:41:03.650448 | 00:26:82:12:21:55 | Band Steering  |   <AID=81>[ab](v0) Steered
to 5Ghz under policy=N staType=ABGN[15] ESSID=engwifi A-BSSID=00:0c:e6:9d:4f:be Ch=36 Steering
time = 1.414671 seconds
```

(2) Band Steering Timeout

```
2018-May- 5 09:32:27.701135 | 00:26:82:12:21:55 | Station Assign  |   <AID=1>[abgn](v0)
assigned to <AP=25> ESSID=BSwpa2psk BSSID=00:0c:e6:91:2c:4c Ch=6 reason=Station probed
2018-May- 5 09:32:27.712719 | 00:26:82:12:21:55 | Station Assign  |   <AID=1>[abgn](v0)
removed from <AP=25> ESSID=BSwpa2psk BSSID=00:0c:e6:91:2c:4c Ch=6 reason=Band steering
2018-May- 5 07:41:02.235862 | 00:26:82:12:21:55 | Band Steering  |   <AID=81>[ab](v0) Steering
to 5Ghz under policy=N Blocking 2.4Ghz, present staType=ABGN ESSID=corp-wifi 5Ghz-
BSSID=00:0c:e6:9d:4f:be Ch=36
2018-May- 5 09:32:28.148377 | 00:26:82:12:21:55 | Station Assign  |   <AID=1>[abgn](v0)
assigned to <AP=29> ESSID=BSwpa2psk BSSID=00:0c:e6:bd:a6:55 Ch=36 reason=Station probed
2017-Oct-10 08:02:49.056279 | 00:26:82:12:21:55 | Band Steering  |   <AID=81>[ab](v0) Steering
disabled due to SteeringTimeout(5) policy=N, present staType=ABGN ESSID=engwifi A-
BSSID=00:0c:e6:9d:4f:be Ch=36
```

(3) Band Steering Re-Enabled

```
2018-May- 5 09:32:27.701135 | 00:26:82:12:21:55 | Station Assign  |   <AID=1>[abgn](v0)
assigned to <AP=25> ESSID=BSwpa2psk BSSID=00:0c:e6:91:2c:4c Ch=6 reason=Station probed
2018-May- 5 09:32:27.712719 | 00:26:82:12:21:55 | Station Assign  |   <AID=1>[abgn](v0)
removed from <AP=25> ESSID=BSwpa2psk BSSID=00:0c:e6:91:2c:4c Ch=6 reason=Band steering
2018-May- 5 09:32:27.712721 | 00:26:82:12:21:55 | Band Steering          | Steering initiated
to 5Ghz under steering policy = N, staType = ABGN

2018-May- 5 07:41:02.235862 | 00:26:82:12:21:55 | Band Steering  |   <AID=81>[ab](v0) Steering
to 5Ghz under policy=N Blocking 2.4Ghz, present staType=ABGN ESSID=corp-wifi 5Ghz-
BSSID=00:0c:e6:9d:4f:be Ch=36
2018-May- 5 09:32:28.148377 | 00:26:82:12:21:55 | Station Assign  |   <AID=1>[abgn](v0)
assigned to <AP=29> ESSID=BSwpa2psk BSSID=00:0c:e6:bd:a6:55 Ch=36 reason=Station probed
2017-Oct-10 08:02:49.056279 | 00:26:82:12:21:55 | Band Steering  |   <AID=81>[ab](v0) Steering
disabled due to SteeringTimeout(5) policy=N, present staType=ABGN ESSID=engwifi A-
BSSID=00:0c:e6:9d:4f:be Ch=36
2018-May- 5 09:32:29.296709 | 00:26:82:12:21:55 | Station Assign  |   <AID=1>[abgn](v0)
assigned to <AP=3> ESSID=BSwpa2psk BSSID=00:0c:e6:91:2c:4c Ch=36 reason=Station probed
2017-Oct-10 08:02:49.056279 | 00:26:82:12:21:55 | 802.11 State  | * <AID=81>[abgn](v0) state
change <old=Unauthenticated> <new=Authenticated> <AP[4]=00:0c:e6:11:26:43> ESSID=BSwpa2psk
Ch=36 A-<BSSID=00:0c:e6:bd:a6:55>
2017-Oct-10 08:02:49.056279 | 00:26:82:12:21:55 | 802.11 State  | * <AID=81>[abgn](v0) state
change <old=Authenticated> <new=Associated> <AP[4]=00:0c:e6:11:26:43> ESSID=BSwpa2psk Ch=36 A-
<BSSID=00:0c:e6:bd:a6:55>
2017-Oct-10 08:02:49.056279 | 00:26:82:12:21:55 | Band Steering  |   <AID=81>[ab](v0) Band
steering re-enabled under policy = N, staType = ABGN
2018-May- 5 09:32:29.379072 | 00:26:82:12:21:55 | Station Assign  |   <AID=1>[abgn](v0)
removed from <AP=3> ESSID=BSwpa2psk BSSID=00:0c:e6:91:2c:4c Ch=6 reason=Band steering
```

(4) Self-Steering by Client

```
2018-May- 6 06:29:02.477236 | 00:21:6a:6c:00:9e | Station Assign  |   <AID=2>[abgn](v0)
assigned to <AP=3> ESSID=BSwpa2psk BSSID=00:0c:e6:bd:a6:55 Ch=36 reason=Probe RSSI handoff
2017-Oct-10 08:02:49.056279 | 00:21:6a:6c:00:9e | 802.11 State  | * <AID=81>[abgn](v0) state
change <old=Unauthenticated> <new=Authenticated> <AP[4]=00:0c:e6:11:26:43> ESSID=BSwpa2psk
Ch=36 A-<BSSID=00:0c:e6:bd:a6:55>
2017-Oct-10 08:02:49.056279 | 00:21:6a:6c:00:9e | 802.11 State  | * <AID=81>[abgn](v0) state
change <old=Authenticated> <new=Associated> <AP[4]=00:0c:e6:11:26:43> ESSID=BSwpa2psk Ch=36 A-
<BSSID=00:0c:e6:bd:a6:55>
2017-Oct-10 08:02:49.056279 | 00:21:6a:6c:00:9e | Band Steering  |   <AID=81>[ab](v0) Self-
steered to 5Ghz under policy = N staType = ABGN  ESSID=BSwpa2psk 5Ghz-BSSID=00:0c:e6:bd:a6:55
Ch=36 Steering time = 0
```

802.11 Authentication and Association

This stage is a mandatory stage toward the full layer 3 connectivity. One difference to note between this stage and an assignment stage is that a mobile station can be authenticated/associated only to one BSSID. So, if a mobile station gets associated to a new BSSID and it was associated to an old BSSID, the association state of the old BSSID is automatically cleaned up. When a mobile station gets hand-off from one AP to another AP within a BSSID, called soft handoff, it is also recorded as one of events.

Event	**Description**	**Action**
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 802.11 State | * <AID=81>[string](v0) state change <old=Unauthenticated> <new=Authenticated> <new AP=4> <new AID=81> (new v4) newESSID=engwifi newCh=36 A-<new BSSID=00:0c:e6:0a:ca:6e> <old AP=4> <old AID=4> (old v4) oldESSID=engwifi oldCh=36 A-<old BSSID=00:0c:e6:0a:ca:6e>	Shows the old and news 802.11 state change as well as If AID, AP ID Essid, Bssid, Channel get changes will be reported with new and old prefixes.	Informative, Client connectivity status.
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 802.11 State | * <AID=81>[ab](v0) state change <old=Authenticated> <new=Associated> <AP=4> ESSID=engwifi Ch=36 A-<BSSID=00:0c:e6:0a:ca:6e>	Shows the old and new 802.11 state change as well as If AID, AP ID Essid, Bssid, Channel get changes will be reported with new and old prefixes.	Informative, Client connectivity status.
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 802.11 State | * <AID=81>[ab](v0) state change <old=Associated> <new=Unauthenticated> <AP=4> ESSID=engwifi Ch=36 A-<BSSID=00:0c:e6:0a:ca:6e>	A station’s 802.11 state changes from Associated to unauthenticated. There are a few causes of this 802.11 state transition. Shows the old and news 802.11 state change as well as If AID, AP ID Essid, Bssid, Channel get changes will be	Informative, Get air capture during this issue and also enable all coord traces from AP as well as controller.

Event	Description	Action
	reported with new and old prefixes.	
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 802.11 State | * <AID=81>[string](v0) state change <old=Unauthenticated> <new=Authenticated> <AP[4]=00:0c:e6:11:26:43> ESSID=engwifi Ch=36 A-<BSSID=00:0c:e6:0a:ca:6e>	Shows the old and news 802.11 state change as well as If AID, AP ID Essid, Bssid, Channel get changes will be reported with new and old prefixes.	Informative, Client connectivity status.
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 802.11 State | * <AID=81>[ab](v0) state change <old=Authenticated> <new=Associated> <AP[4]=00:0c:e6:11:26:43> ESSID=engwifi Ch=36 A-<BSSID=00:0c:e6:0a:ca:6e>	Shows the old and news 802.11 state change as well as If AID, AP ID Essid, Bssid, Channel get changes will be reported with new and old prefixes.	Informative, Client connectivity status.
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 802.11 State | * <AID=81>[ab](v0) state change <old=Associated> <new=Unauthenticated> <AP[4]=00:0c:e6:11:26:43> ESSID=engwifi Ch=36 A-<BSSID=00:0c:e6:0a:ca:6e>	A station's 802.11 state changes from Associated to unauthenticated. There are a few causes of this 802.11 state transition. Shows the old and news 802.11 state change as well as If AID, AP ID Essid, Bssid, Channel get changes will be reported with new and old prefixes.	Informative, Get air capture during this issue and also enable all coord traces from AP as well as controller.
2017-Oct-10 08:06:07.374741 | 00:40:96:ad:d4:3c | 802.11 State | * <AID=2>[abgn](v0) handoff <OLD_AP=5>	A station is handed off from an AP to	Informative– Client

Event	Description	Action
RSSI (-49 -45) <NEW_AP=4> RSSI (-44 -43) ESSID=engwifi Ch=36 A-BSSID=00:0c:e6:8a:db:50 reason=Normal Handoff	another AP. This event is generated only if a mobile station is associated to the ESS of a virtual cell or a virtual port.	connectivity status. If seen repeatedly enable AP traces for coord and frame report and controller traces for coord
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: Unspecified<AID=2><BSSID=00:0c:e6:f9:01:01>	Dissassoc from AP for unspecified reason.	Get air capture during this issue and also enable all coord traces from AP as well as controller.
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 802.11 State | * <AID=10>[abg](v0) (pre quasi found) marked found as received assign ack from assigned <AP=4> ESSID=corp-wifi Ch=36 B-BSSID=00:0c:e6:9d:4f:be	*Pre-Quasi* is an intermediate state between the *Lost* and *Found* states, when a lost station is identified by the same AP.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 802.11 State | * <AID=81>[ab](v0) (pre quasi found) marked found as received handoff ack from assigned <AP=7> ESSID=corp-wifi Ch=6 B-BSSID=00:0c:e6:9d:4f:be	*Pre-Quasi* is an intermediate state between the *Lost* and *Found* states, when a lost station is identified by a different AP from the previous one.	Informative
2017-Oct-10 08:02:49.886864 | 00:40:96:ad:d4:3c | 802.11 State | Received Deauth frame from station <Deauth reason: authentication leave><Previous RSSI stored in station node = -44><Deauth packet RSSI = -44><AID=1><BSSID=8a:85:85:ad:d4:3c>	A station sends 802.11 de-association frame.	Get air capture during this issue
00:16:6f:3b:17:a9 | 802.11 State | Received Disassoc frame from station <Disassoc reason: association leave><deauth packet RSSI =	A station sends 802.11 de-association	Get air capture during this issue

Event	Description	Action
57><AID=3><BSSID=00:0c:e6:f9:01:01>	frame.	
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: association expired<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 dis-association frame due to association expiration.	Get air capture during this issue and also enable all coord traces from AP as well as controller.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: too many association<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 dis-association frame due to too many assoc request.	Get air capture during this issue and also enable all coord traces from AP as well as controller.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Deauth reason: not authenticated<AID=0><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-authentication frame as station is not authenticated.	Get air capture during this issue and also enable all coord traces from AP as well as controller.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: not associated<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 dis-association frame as station is not associated.	Get air capture during this issue and also enable all coord traces from AP as well as controller.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: not associated: data pckt is received with assoc id zero<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame as AP received data packet from station even though it's not associated yet.	Get air capture during this issue and also enable all coord traces from AP as well as controller.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: not associated: pspoll pckt is received with assoc id zero<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame as AP received ps poll from station even though it's not	Get air capture during this issue and also enable all coord traces from AP as well

Event	Description	Action
	associated yet.	as controller.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Pspoll is received with associd out of bound<AID=1><BSSID=00:0c:e6:f9:01:01>	Ps Poll is received by AP with assoc id out of bound.	Get air capture during this issue and also enable all coord traces from AP as well as controller.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: association leave<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 dis-association frame due to association removed.	Get air capture during this issue and also enable all coord traces from AP as well as controller.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: associated but not autheticated<AID=0><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame as station is associated but not authenticated.	Get air capture during this issue and also enable all coord traces from AP as well as controller.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: RSN required<AID=0><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to RSN required reason.	Get air capture during this issue.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: RSN inconsistent<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to RSN inconsistent reason.	Get air capture during this issue.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: IE invalid<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to invalid IE.	Get air capture during this issue.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: IE invalid: VAP not WPA/WPA2<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to IE invalid with reason: VAP not	Get air capture during this issue.

Event	Description	Action
	WPA/WPA2.	
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: IE invalid: IE length is too short<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to IE invalid with reason: IE length is too short.	Get air capture during this issue.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: IE invalid: bad version in IE<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to IE invalid with reason: bad version in IE.	Get air capture during this issue.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: IE invalid: multicast cipher mismatch<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to IE invalid with reason: multicast cipher mismatch.	Get air capture during this issue.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: IE invalid: unicast cipher data too short<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to IE invalid with reason: unicast cipher data too short.	Get air capture during this issue.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: IE invalid: unicast cipher set empty<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to IE invalid with reason: unicast cipher set empty.	Get air capture during this issue.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: IE invalid: key mgmt alg data too short<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to IE invalid with reason: key mgmt alg data too short.	Get air capture during this issue.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: IE invalid: no acceptable key mgmt alg<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to IE invalid with reason: no acceptable	Get air capture during this issue.

Event	Description	Action
	key mgmt alg.	
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Disassoc reason: MIC failure<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-association frame due to MIC failure.	Get air capture during this issue and also hotspad traces from controller and security traces on AP.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Deauth reason: Coord interbss handoff<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-authentication frame due to interbss handoff.	Get air capture during this issue and also coord traces from controller and security traces on AP.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Deauth reason: Coord deauth<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-authentication frame due to coordinator.	Get air capture during this issue and also coord traces from controller and security traces on AP.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Deauth reason: Coord removed Assignment<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-authentication frame as co-ordinator removes assignment.	Get air capture during this issue and also coord traces from controller and security traces on AP.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Deauth reason: Key Mismatch Error<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-authentication frame due to Key Mismatch error.	Get air capture during this issue and also hotspad traces from controller and security traces on AP.

Event	Description	Action
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | Deauth reason: Ssid Mismatch<AID=1><BSSID=00:0c:e6:f9:01:01>	AP sends 802.11 de-authentication frame due to Ssid Mismatch error.	Get air capture during this issue and also hostapd traces from controller and security traces on AP.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | HT Station, Non Wmm Capable<AID=1><BSSID=00:0c:e6:f9:01:01>	Non WMM capable station; only *abg* data rates can be achieved.	Informative Enable WMM to achieve MCS data rates.
2017-Oct-10 08:06:07.374741 | 00:40:96:b4:c7:26 | 802.11 State | 802.11r Fast Roam event<AID=1><BSSID=00:0c:e6:f9:01:01>	802.11r fast roaming.	Informative – Client connectivity status.
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 802.11 State | <AID=81>[ab](v0) 11r Fast roaming from <AP-11>, ch=36 B-BSSID=<00:0c:e6:9d:4f:be> to <AP-4>, ch=6 B-BSSID=<00:0c:e6:9d:4f:b1>	11r fast roaming.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 802.11 State | <AID=81>[ab](v0) (pre found) lost from assigned <AP=16> ESSID=corp-wifi Ch=6 B-BSSID=00:0c:e6:9d:4f:be reason=Station lost from AP	When lost message received from AP for Client. Client state gets changed to *Lost*.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 802.11 State | <AID=81>[ab](v0) (pre quasi found) found on unassigned <AP=11>(rssi=-256) ESSID=corp-wifi Ch=6 A-BSSID=00:0c:e6:9d:4f:be reason=Station discovered	When found message or probe indication received from AP for Lost or Pre-Quasi Found station. Station state gets changed to *Found* from *Lost* or *Pre-Quasi*.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> <auth method=WPA2_EAP>:<pkt type=EAPOL_START> recvd <ESSID=vcellwpa2> <BSSID=22:01:0f:3b:17:a9>	FortiWLC receives EAPOL_START message from a station associated to	Informative

Event	**Description**	**Action**
	ESSID::BSSID pair. There are two authentication methods; WAP2_EAP or WPA_EAP. The standard states this message is optional.	
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> <EAP code=request> <EAP ID=1> <EAP type=Identity> sent	FortiWLC tries this message up to 4 times with one second interval. As the authentication proceeds, the EAP ID increases by one.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> <pkt type=EAP_PACKET> <EAP code=response><EAP ID=1>	The EAP ID of response shall match the EAP ID of request.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> Radius <msg code=access_request><msg ID=178> sent <ip=192.168.101.17>:<port=1812>	FortiWLC forwards a station's request to the RADIUS Server IP::Port.	Informative

The causes of station's 802.11 state change from associated to unauthenticated are 1. A station gets aged out. The default aging out period is 30 minutes. The aging out period of 802.11 associated station is different from the aging out period of an assigned station. 2. A station voluntarily leaves a currently associated BSSID by sending 802.11 deauthentication frame. 3. A station moves from one BSSIDOLD to another BSSIDNEW. The associated state of BSSIDOLD is automatically cleared up. 4. In the multi-Controller environment, when an station moves from one ControllerOLD to another ControllerNEW and two Controllers are in the same subnet, the associated state of the station in ControllerOLD is automatically cleared up. 5. When a following 1x/WPA/WPA2 authentication fails due to RADIUS reject, a message time-out or unknown reason, the mobile's 802.11 state changes back to an unauthenticated state. A detail is explained in 2.5 1X/WPA/WPA2. 6. When a following key exchange fails due to Timeout or MIC failure, the mobile's 802.11 state changes back to an unauthenticated state. A detail is explained in Key Exchange.

Failure Cases

Sometimes, a mobile station fails to pass this stage. For some misconfigurations, a station can’t go through the 802.11 authentication/association. Here are some typical cases; 1. For the 802.11 Shared Key Authentication, the key in a station doesn’t match the key configured in Controller. The mismatch of WEP key length, either WEP64 or WEP128, pertains to this case. 2. A client is configured with manual Shared Key Authentication. However, the ESS, a mobile is connecting to , is configured with Shared Key Authentication off.

1X/WPA/WPA2

This stage is RADIUS-based User authentication. As shown in the following example sub-section, the message exchanged between a station and RADIUS server for an authentication is dependent on the authentication scheme. For example, if WPA-PEAP is used, 39 events are generated. If WPA-TLS is used, 27 events are generated.

Event	**Description**	**Action**
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> <pkt type=EAP_PACKET> <EAP code=request><EAP ID=2> <info=relay eap-request from Radius> sent	Authenticator forwards RADIUS Server's request to a station.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Radius ACCESS-ACCEPT received : Session Timeout: 3600 sec, VLAN Tag : 0, Filter id : [0], CUI : None	Authenticator receives RADIUS Access-Accept message from the RADIUS server.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Backend Authentication Timeout	RADIUS Server timeout, after this authentication switch to secondary RADIUS server from primary RADIUS server.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> Sending EAP Failure to station, (identifier 1)	There are three different cases to trigger this event; when a RADIUS message is timed out When a EAP message to a station is timed out. When a RADIUS Server sends a Reject message.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> Radius Access-Reject received	Authenticator receives RADIUS Access-Reject message from the RADIUS server.	Informative

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> Backend Authentication Failure	A message forwarded to a RADIUS server is timed out.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> M1 <msg type=EAPOL_KEY> PTK sent	Authenticator sends first key exchange message. FortiWLC tries transmission of it up to 4 times if there is no response, and then aborts the key exchange transaction.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> M2 <pkt type=EAPOL_KEY> MIC Verified	Authenticator receives a key exchange message, M2, from a station, and MIC is verified correctly.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> M3 <msg type=EAPOL_KEY> WPA PTK Negotiation sent	Authenticator sends a third key exchange message. FortiWLC tries transmission of it up to 4 times if there is no response, and then aborts the key exchange transaction.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> M4 <pkt type=EAPOL_KEY> <key type=Unicast Key> Key Pairwise	Authenticator receives a fourth key exchange message from a station.	Informative

Example

WPA-PEAP

This is a full event trace of WPA-PEAP client authentication.

```
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <EAP
code=request> <EAP ID=1> <EAP type=Identity> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <auth
method=WPA_EAP>:<pkt type=EAPOL_START> recvd <ESSID=vcellwpa2> <BSSID=1e:0b:0f:3b:17:a9>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <EAP
code=request> <EAP ID=1> <EAP type=Identity> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=1>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=178> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=2> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=2>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=179> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=3> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=3>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=180> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=4> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=4>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=181> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=5> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=5>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=182> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=6> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=6>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=183> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=7> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=7>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=184> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=8> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=8>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=185> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=9> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=9>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=186> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=10> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=10>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=187> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
```

```
type=EAP_PACKET> <EAP code=request><EAP ID=11> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=11>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=188> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=12> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=12>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=189> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius ACCESS-
ACCEPT received : Session Timeout: 3600 sec, VLAN Tag : 0, Filter id : , CUI : None
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=success><EAP ID=13> <info=relay eap-request from Radius> sent
```

WPA-TLS

This is a full event trace of WPA-TLS client authentication.

```
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <EAP
code=request> <EAP ID=1> <EAP type=Identity> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <auth
method=WPA_EAP>:<pkt type=EAPOL_START> recvd <ESSID=vcellwpa> <BSSID=1e:0b:0f:bb:4a:9c>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <EAP
code=request> <EAP ID=1> <EAP type=Identity> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=1>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=236> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=2> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=2>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=237> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=3> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=3>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=238> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=4> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=4>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=239> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=5> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=5>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=240> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=6> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=6>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=241> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=7> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
```

```
type=EAP_PACKET> <EAP code=response><EAP ID=7>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=242> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=request><EAP ID=8> <info=relay eap-request from Radius> sent
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=response><EAP ID=8>
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> Radius <msg
code=access_request><msg ID=243> sent <ip=192.168.101.17>:<port=1812>
2017-Oct-10 08:02:49.056279 | 00:16:6f:bb:4a:9c | 1X Authentication  | <AID=1> Radius ACCESS-
ACCEPT received : Session Timeout: 3600 sec, VLAN Tag : 0, Filter id : , CUI : None
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication  | <AID=1> <pkt
type=EAP_PACKET> <EAP code=success><EAP ID=8> <info=relay eap-request from Radius> sent
```

Key Exchange

A station goes through this stage when WPA, WPA2, WPA PSK, WPA2 PSK, MIXED or MIXED_PSK is enabled.

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> M5 <msg type=EAPOL_KEY> WPA GTK Rekey Negotiation sent	Authenticator sends a fifth key exchange message for WPA or WPA-PSK modes.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> M6 <pkt type=EAPOL_KEY> <key type=Group Key>	Authenticator receives a sixth key exchange message from a station for WPA or WPA-PSK modes. This is a last message of a key exchange for WPA or WPA-PSK. It is indicative of a successful key exchange. A station can proceed to a next stage.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> M3 <msg type=EAPOL_KEY> WPA2 PTK Negotiation sent	Authenticator sends a third key exchange message for WPA2 or WPA2-PSK modes. FortiWLC tries transmission of it up to 4 times, and then aborts the key exchange transaction if it doesn’t receive M2 message by sending 802.11	Informative

Event	Description	Action
	deauth.	
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> Sending Station Disconnect, Reason : MIC Failure, Auth Type 802.1X	The message sent by a station results in a MIC failure. 802.11 deauth to the station. For WPA-PSK, or WPA2-PSK, the wrong passphrase, or password, leads to this failure.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> Sending Station Disconnect, Reason : 4-way Handshake Timeout, Auth Type 802.1X	The key exchange aborts due to no response from a client. Authenticator tries the transmission of a key exchange message up to 6 times with one second interval. If no response comes from the station, it aborts the key exchange.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Sending Station Disconnect, Reason : Group Key Update Timeout, Auth Type	The lifespan of the session key used for encryption of station disconnected after the timeout if those keys are not re-negotiated.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> <pkt type=EAPOL_KEY> <error=Mic Failure> <key type=Unicast Key>	Mic failure at station side after M3.	Informative

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Session over. Client needs to re-authenticate	After session timeout the client needs to re authenticate with the RADIUS server.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Replay Counter Mismatch	GTK update sequence with station failed.	Informative

1X Authentication

This section describes the station log events generated for 1x authentication.

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> RC mismatch sm->M1MicFailedCount = 0	After RC mismatch M1 MIC failure count is zero.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> out of state 4-way handshake message	Authenticator State machine is not in sync with supplicant state machine.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Seen : MIC Failure	M2 from client validation fails.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Sending Station Disconnect, Reason : M4 decryption failed.	Decryption of M4 message fails.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Radius <DISCONNECT-REQUEST(DM) > Identifier=<1> received is dropped due to Invalid Shared Secret Key	Provided secret does not match with the configured secret in the RADIUS profile, Hence disconnect request is dropped.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Sent Successful(ACK) Response for DISCONNECT-REQUEST(DM) received from Radius Server with Identifier=<1> and FilterId= [0]	ACK sent after disconnect request from server to station.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Received Radius DISCONNECT(DM) REQUEST Message from Radius Server = [radius-test] with 1 as Identifier	Received RADIUS REQUEST Message from RADIUS Server	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> <EAP code=response> <info=relay eap-response from Radius> sent	EAP response from RADIUS server to the client.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> <msg type=EAPOL_KEY>	Send unicast key to the client after Rekey	Informative

Event	Description	Action
<key=unicast> sent	period.	
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Sending Station Disconnect, Reason : Unspecified Reason, Auth Type	Sending Station Disconnect for Unspecified Reason	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Encryption | <AID=1> MIC Countermeasure invoked on Ess engwifi	Notifying AP to disconnect all existing client and stop accepting client connection for next 60 seconds.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | DHCP | <msg_type=DISCOVER><server_ip=255.255.255.255><server_mac=ff:ff:ff:ff:ff:ff><offered_ip=0.0.0.0>	Wncreg updates its table with stations virtual MAC address.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <msg_type=DISCOVER><server_ip=255.255.255.255><client_ip=10.101.64.1>	Server sends this message to station with the configuration parameters that it offers to station.	Informative
2018-08-02 03:09:50.191549 | e4:46:da:8d:6b:5b | 1X Authentication | <Multiple PSK> <ESSID=bp_mpsk> <APID=2> <PSKID=8db6fe4a65a8a786e9f640730fcfa164>	Client is successfully authenticated using the PSK key associated with the displayed PSK ID.	Informative

Encryption

This section describes the station log events generated for encryption.

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <msg_type=CONFIRM><server_ip=2001:DB8:3000:3000::42><server_mac=00:0e:84:85:33:00><Station_ip=2001:DB8:3000:3000::45>	Station sends this event to confirm if the IP address assigned to it is still valid.	Informative

DHCP and IP Discovery

This is a stage a mobile station obtains an IP address via DHCP. One thing to note, even though obvious, is that the crypto key established between a Fortinet and a station has to match. How two entities established a key depends on the security mode associated to the ESS. For WEP, a key is manually inserted. For the WPA or WPA2, a key is automatically derived. For the WPA-PSK or WPA2-PSK, a key is derived from a pass phase. There is one restriction on displaying DHCP events. When a mobile station is connected to a bridge mode ESS profile, these events are not generated. It is noted that a station doesn't not always go through a full DHCP transaction when it gets associated even if a station is configured DHCP. it is often observed a mobile doesn't go through it when it moves from one BSSID to another BSSID within a ESSID.

The IP discovery is the stage a Fortinet system first detects the IP address used by a station. An IP discovery method indicates how a FORTINET detects the IP address. If it is detected through a DHCP transaction between a client and DHCP server, the method is showed as DHCP. Otherwise, it is showed as dynamic. The IP discovery is initialized to None.

Event	**Description**	**Action**
2018-05-21 07:22:02.570364 | b8:e8:56:00:f0:2e | DHCP | <DHCPv6: msg_type=INFORMATION-REQUEST XID: 0xe42fd3><server_ip=ff02::1:2><server_mac=33:33:00:01:00:02><client_ip=fe80::bae8:56ff:fe00:f02e><Elapsed-time=0 ms><ClientID=000100011a21d9f7b8e85600f02e>	Station sends this to request only configuration parameters.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | DHCP | <msg_type=INFO><server_ip=10.101.64.1><server_mac=00:0e:84:85:33:00><offered_ip=10.101.66.25>	Station sends a DHCP information packet to the server.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <msg_type=DISCOVER><server_ip=255.255.255.255><client_ip=10.101.64.1>	DHCP discover message.	Informative
2018-05-21 07:04:26.463970 | b8:e8:56:00:f0:2e | DHCP | <msg_type=OFFER><server_ip=10.33.0.10><gateway_ip=10.33.56.1><offered_ip=10.33.56.30>	DHCP offer message.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <msg_type=CONFIRM><server_ip=2001:DB8:3000:3000::42><server_mac=00:0e:84:85:33:00><Station_ip=2001:DB	Station sends this event to confirm if the IP address assigned to it is still	Informative

Event	Description	Action
8:3000:3000::45>	valid.	
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <msg_type=DECLINE><server_ip=2001:DB8:3000:3000::42><server_mac=00:0e:84:85:33:00><Station_ip=2001:DB8:3000:3000::45>	Station sends this event to server if the IP address it assigned is already in use by Station.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <msg_type=SOLICIT><server_ip=2001:DB8:3000:3000::42><server_mac=00:0e:84:85:33:00><Station_ip=2001:DB8:3000:3000::45>	Station sends this event to locate DHCPv6 server.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <msg_type=REQUEST><server_ip=2001:DB8:3000:3000::42><server_mac=00:0e:84:85:33:00><Station_ip=2001:DB8:3000:3000::45>	Station sends this event to request for configuration parameters and IP addresses.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | IP Address Discovered | <Old IP discovery Method=none><Old IP=0.0.0.0><New IP discovery Method=dynamic><New IP=10.101.66.25>	A Mobile station's discovery method or IP address changes, and FortiWLC accepts the new IP address.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | IP Address Discovered | <IP = 10.101.64.100> fails due to one of local IPs on AP <MAC = 00:0c:e6:16:dd:39>.	A Mobile station is detected to use the IP address configured to Controller.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | IP Address Discovered | ip update not performed. <Client IP=10.101.64.1> is used by a wired station <00:0e:84:85:33:00>	A Mobile station is detected to use the IP being used by a wired station whose MAC address is shown.	Informative
2018-05-21 07:22:02.570364 | b8:e8:56:00:f0:2e | DHCP | <DHCPv6: msg_type=INFORMATION-REQUEST XID: 0xe42fd3><server_ip=ff02::1:2><server_mac=33:33:00:01:00:02><client_ip=fe80::bae8:56ff:fe00:f02e><Elapsed-	Station sends this to request only configuration parameters.	Informative

Event	Description	Action
time=0 ms><ClientID=000100011a21d9f7b8e85600f02e>		
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <msg_type=UNKNOWN><server_ip=2001:DB8:3000:3000::42><server_mac=00:0e:84:85:33:00><Station_ip=2001:DB8:3000:3000::45>	When the controller does not recognize the DHCP packet type coming from the station.	Information
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <msg_type=ADVERTISE><server_ip=2001:DB8:3000:3000::42><server_mac=00:0e:84:85:33:00><Station_ip=2001:DB8:3000:3000::45>	This message indicates that the server is ready for DHCP service.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <msg_type=REPLY><server_ip=2001:DB8:3000:3000::42><server_mac=00:0e:84:85:33:00><Station_ip=2001:DB8:3000:3000::45>	This message indicates/conveys different things in each case: 1. In response to Solicit, Request, Renew, Rebind or Information-Request: Conveys assigned addresses and configuration parameters 2. In response to Confirm: indicates confirmation or denial of addresses assigned to the Station as appropriate to the link which the Station is connected 3. In response to Release or Decline: indicates acknowledgment of receipt of such message Wncreg adds the IP-MAC association for this	Informative

Event	Description	Action
	station in its table.	
2018-05-21 07:10:32.698338 | d4:6a:6a:a1:67:13 | IP Address Discovered | IP discovery fails due to prefix mismatch <IP DISCOVERED = 10.33.156.30>Allowed Range : IP PREFIX = 10.33.56.0with NETMASK = 255.255.255.0 on AP <MAC = 00:0c:e6:0d:f3:59> meru interface.	Station tries to use the IP which is outside it's allowed range as per netmask.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | IP Address Discovered | <New HOME ICR IPv6 discovery Method=[static]<New IP=[10.32.3.1]>		Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | DHCP | <All vlans in vlan pool [vPool1] are exhausted. Forcing vlan 3 state to available>		Informative
2018-05-21 06:54:05.122543 | d4:6a:6a:a1:67:13 | IP Address Discovered | <IP = 169.254.25.188> fails due to un-assigned IP on AP <MAC = 00:0c:e6:0d:f3:59>.	Client tries to use Link Local IP address(169.254.x.x)	Informative
2018-05-21 06:57:43.146571 | d4:6a:6a:a1:67:13 | IP Address Discovered | <IP = 10.33.56.1> fails due to one of gateway IPs on AP <MAC = 00:0c:e6:0d:f3:59>	Client Tries to use Gateway IP.	Informative
2018-05-21 07:05:35.735684 | d4:6a:6a:a1:67:13 | IP Address Discovered | <IP discovery Method=dynamic> <IP=10.33.56.30> conflict with <b8:e8:56:00:f0:2e> <IP discovery Method=dhcp>	Wireless Client tries to use IP of another Client	Informative
2018-05-21 07:22:02.530790 | b8:e8:56:00:f0:2e | IP Address Discovered | <New IPv6 discovery Method=dynamic><New IP=[2001:470:ecfb:437:bae8:56ff:fe00:f02e]>	IPV6 address assignment.	Informative
2018-05-21 07:22:02.530790 | b8:e8:56:00:f0:2e | IP Address Discovered | < IP discovery Method=dynamic>< IP=[2001:470:ecfb:437:bae8:56ff:fe00:f02e]>< conflicts with IP address of< d4:6a:6a:a1:67:13 >	IPV6 address conflict	Informative
2018-05-21 07:05:35.735684 | d4:6a:6a:a1:67:13 | IP Address Discovered | <IP discovery Method=dynamic>	IPV4 address conflict	Informative

Event	**Description**	**Action**
<IP=10.33.56.30> conflict with <b8:e8:56:00:f0:2e> <IP discovery Method=dhcp>		

Captive Portal

A Captive portal stage is one a station goes through WEB-based user authentication.

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <User=user1> <ipaddr=10.24.1.2> Idle Timout expires. Resetting Authentication Status.	Captive portal configuration page has a value inactivity-timeout value after whose expiry the web authentication for that client will automatically be removed.	Informative, if needed the inactivity time out value can be changed
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <User=user1 > Radius User received smm-clear from wncreg.	The client has disconnected (first event) and l3 session timeout for the client has also expired (second event following first).	Check for what reason smm-clear is received and take decision accordingly.
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <User= user1> <ipaddr=" 10.35.6.1 "> Radius User Authentication fails. Radius Server rejects.	Once RADIUS reject is received the client will be prompted with the retry web page.	Check the captive portal primary and secondary RADIUS server's status. Also make client enters the right credentials.
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | DM/CoA Radius Request Message will be dropped due of Shared Secret Key Mismatch <TBNL>	Controller will not honour the request and will send a Nack to the server	Configure the right secret and check if the controller sends a ack.
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <User=user1> <ipaddr=10.3.2.1> Radius (DISCONNECT-REQUEST) ID = 11 was executed	When the COA disconnect request is sent from RADIUS	Informative, Just check if the Disconnect

Event	Description	Action
Successfully	server, controller will remove the webauth state of the client (l3state). Deauth is also sent to the client.	Request is expected
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <User=user2> <ipaddr=" 10.33.6.2 "> Radius (COA-REQUEST)Change of Authorization Request ID=11 Filter_Id =0 done Successfully	When COA-REQUEST is sent from any RADIUS server, controller will change the filter id for that particular client.	Informative (just check if the new filter id is updated)
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <User=user1> <ipaddr=" 10.34.1.3 "> Sent Guest User Authentication Request.	the CP user will be authenticated by the controller itself(only for internal CP)	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <Captive Portal Profile= cpProfile1> <User : user1> <ipaddr=> Sending User Authentication Request.	When the client is connected to captive portal enabled SSID, this message is seen after the client enters the username and password in the login page trying to autheticate.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <User=user1> <ipaddr=172.18.19.21> Sent Radius Authentication Request.	RADIUS request for User has been sent to RADIUS server.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <User=user1>	FortiWLC gets RADIUS Access	Informative

Event	**Description**	**Action**
<ipaddr=172.18.19.21> Radius User Authenticated Successfully <session_time=0> <idle_time=0>	Accept message for Captive Portal User.	
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <User=user3> <ipaddr=172.18.19.20> Radius User Authentication fails. Request Timeout.	A RADIUS request for Captive portal user sent to RADIUS server from Controller is timed out, The RADIUS servers are down for some reason due to which they are not sending a response and ultimately security module which initiated the request times out	Validate the Working of RADIUS servers or configure a different RADIUS server which is working

SIP

This section describes the station log events generated for SIP.

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | SIP | Registration expired for phone - 172.18.122.122:6723 UserName=5004	Registration expired for phone - %d%.d%.d%.d:%d UserName=%s	Bring the phone within the range of an AP and reboot. If the phone is in phone call then wait till the call is over
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | SIP | ERROR: Call Rejected,State(NOT YET ESTABLISHED)	Phone trying to make the call received the reject due to 1> Receiver rejecting the call 2> Call capacity of network exceeded.	In case of [2] the rectification may be to move to another AP and retry the call.
2017-Oct-10 08:02:49.056279 | 00:03:2a:00:65:b9 | SIP | Send<200_OK>(NOT YET ESTABLISHED):To: <sip:27@172.18.122.122>;tag=1352750932 Contact: <sip:27@172.18.17.17>	Message : 200 OK State : NOT YET ESTABLISHED SIP Server with IP 172.18.122.122 Sender : SIP Phone with Mac-address 00:03:2a:00:65:b9, IP address 172.18.17.17 and SIP User Name : 27	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | SIP | ERROR:Flow Aged Out,State(NOT YET ESTABLISHED)>	The resources reserved on air aged out. These resources are defined by the flow. The resources will age out after the call ends or there is communication between the 2	Informative

Event	Description	Action
	phones.	
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | SIP | ERROR: Registration AGED OUT,IP[172.18.122.122]>	REGISTRATION EXPIRED message received by a SIP phone This is received for UDP phones.	Bring the phone within the range of an AP and reboot. If the phone is in phone call then wait till the call is over.
2017-Oct-10 08:02:49.056279 | 00:03:2a:00:65:b9 | SIP | Receive<ACK>(ACTIVE):From: “5004” <sip:5004@172.18.122.122>;tag=407363379	Message: ACK State: ACTIVE Sender: SIP Phone with User Name 5004 Receiver: SIP Phone with Mac address 00:03:2a:00:65:b9, SIP Server ip: 172.18.122.122.	Informative
2017-Oct-10 08:02:49.056279 | 00:03:2a:02:50:34 | SIP | Send<INVITE>(ON HOLD):To: <sip:27@172.18.122.122>;tag=1352750932 Contact: <sip:5004@172.18.17.18>	Message : INVITE State : ON HOLD Sender : SIP Phone with Mac-address 00:03:2a:02:50:34 , ip address 172.18.17.18, User Name : 5004 Receiver : SIP Phone with User Name 27 SIP Server ip : 172.18.122.122	Informative
2017-Oct-10 08:02:49.056279 | 00:03:2a:00:65:b9 | SIP | Send<200_OK>(ON HOLD):To: <sip:27@172.18.122.122>;tag=1352750932 Contact: <sip:27@172.18.17.17>	Message : 200 OK State : ON HOLD SIP Server with ip 172.18.122.122, Sender : SIP Phone with Mac-address 00:03:2a:00:65:b9, IP address	Informative

Event	Description	Action
	172.18.17.17 and SIP User Name : 27	
2017-Oct-10 08:02:49.056279 | 00:03:2a:02:50:34 | SIP | Receive<200_OK>(ON HOLD):From: “5004” <sip:5004@172.18.122.122>;tag=4073633 79 Contact: <sip:5004@172.18.122.122:5060> Expires:180	Message : ACK State : ON HOLD Sender : SIP Phone with User Name 5004 Receiver : SIP Phone with Mac address 00:03:2a:00:65:b9, SIP Server ip : 172.18.122.122.	Informative
2017-Oct-10 08:02:49.056279 | 00:03:2a:02:50:34 | SIP | Receive<BYE>(ACTIVE):From: “5004” <sip:5004@172.18.122.122>;tag=407363379 Contact: <sip:27@172.18.122.122:5060>	Message : BYE State : ACTIVE SIP Server : 172.18.122.122 Sender : SIP Phone with Mac-address 00:03:2a:02:50:34 Receiver : SIP User Name 27	Informative
2017-Oct-10 08:02:49.056279 | 00:03:2a:02:50:34 | SIP | Send<BYE>(ACTIVE):To: <sip:27@172.18.122.122>;tag=1352750932	Message : BYE State : ACTIVE SIP Server : 172.18.122.122 Sender : SIP Phone with Mac-address 00:03:2a:02:50:34 Receiver : SIP User Name 27.	Informative
2017-Oct-10 08:02:49.056279 | 00:03:2a:00:65:b9 | SIP | Receive<BYE>:From: “5004” <sip:5004@172.18.122.122>;tag=407363379	Message : BYE State : ACTIVE Sender : SIP Phone with User Name 5004 Receiver : SIP Phone with Mac address 00:03:2a:00:65:b9 SIP Server ip : 172.18.122.122.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | SIP |	Registration expired	Bring the phone

Event	Description	Action
Registration expired for phone - 172.18.122.122:6723 UserName=5004	for phone - %d%.d%.d%.d:%d UserName=%s	within the range of an AP and reboot. If the phone is in phone call then wait till the call is over
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | SIP | ERROR: Call Rejected,State(NOT YET ESTABLISHED)	Phone trying to make the call received the reject due to 1> Receiver rejecting the call 2> Call capacity of network exceeded.	In case of [2] the rectification may be to move to another AP and retry the call.
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | SIP | ERROR:Abnormal Termination,State (TERMINATION IN PROGRESS)	Whenever there is a protocol error or data packet corruption.	Informative
2017-Oct-10 08:02:49.056279 | 00:03:2a:02:50:34 | SIP | Send<REGISTER>:To: “5004” <sip:5004@172.18.122.122> Contact: <sip:5004@172.18.17.18>;expires=3600	Message : REGISTER Sender : SIP Phone with Mac-address 00:03:2a:02:50:34 and ip address 172.18.17.18 and SIP User Name : 5004 SIP Server with ip 172.18.122.122	Informative
2017-Oct-10 08:02:49.056279 | 00:03:2a:02:50:34 | SIP | Receive<100_TRYING>:From: “5004” <sip:5004@172.18.122.122>;tag=698116279	Message : RESPONSE 100 TRYING SIP Server with ip 172.18.122.122 Receiver : SIP Phone with Mac-address 00:03:2a:02:50:34	Informative

Event	Description	Action
	and ip	
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | SIP | Send<INVITE>(NOT YET ESTABLISHED):To:<sip:27@172.18.122.122> Contact:<sip:5004@172.18.17.18> Expires: 180	Message : INVITE State : NOT YET ESTABLISHED Sender : SIP Phone with Mac-address 00:03:2a:02:50:34 , ip address 172.18.17.18, User Name : 5004 Receiver : SIP Phone with User Name 27 SIP Server ip : 172.18.122.122	Informative
2017-Oct-10 08:02:49.056279 | 00:03:2a:00:65:b9 | SIP | Receive<INVITE>(NOT YET ESTABLISHED):From: “5004” <sip:5004@172.18.122.122>;tag=4073633 79 Contact: <sip:5004@172.18.122.122:5060> Expires:180	Message : INVITE State : NOT YET ESTABLISHED Sender : SIP Phone with User Name 5004 Receiver : SIP Phone with Mac address 00:03:2a:00:65:b9, SIP Server ip : 172.18.122.122	Informative

Diagnostics

This section describes the station log events generated for diagnostics.

Event	**Description**	**Action**
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Diagnostics | ResetNumAssignedSTA: ATS [00:0c:e6:16:dd:39] ch=36 has assigned 77->77	Resets AssignedStaList to zero , for the channel passed as argument	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Diagnostics | IncNumAssignedSTA: ATS [00:0c:e6:16:dd:39] ch=36 has assigned 99->100 STA [00:40:96:ad:d4:3c]	Adds station to the assignedStaList for the BSSID.	Informative

inference

New Melf Entries

This section describes the new station log events for FortiWLC.

Event	Description	Action
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | CP User Authentication | <Captive Portal Profile= profile-1> <User : user1> <ipaddr=: 172.18.122.122> Authentication bypassed for cp roamed client	A captive portal authenticated client roams from home controller to foreign controller and the captive portal state of the client is retained. This occurs when the client is roaming from one controller to another in a network where captive portal and ICR are enabled.	Information
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | <User=user1> received mac user removal from wncreg.	Received Zero IP address update from kernel and security module will remove this particular client as a result of update. This occurs commonly when a client disconnects from a MAC filtering enabled profile.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | 1X Authentication | <AID=1> Radius ACCESS-ACCEPT received : Session Timeout: 3600 sec, VLAN Pool name: 0, Filter id : 1, CUI : None	FortiWLC receives RADIUS Access-Accept message from the RADIUS server.	Informative
2017-Oct-10 08:02:49.056279 | 00:16:6f:3b:17:a9 | 1X Authentication | <AID=1> Radius <msg	FortiWLC forwards a station's request to	Informative

Event	Description	Action
code=access_request><msg ID=178> sent to relay ap <APID =16>:<port=1812>	the RADIUS Server IP::Port.	
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Trying to accept the Wired Client for Cp Bypass <00:40:96:ad:d4:3c>	MAC filtering has failed and wired client has to go through CP authentication to get access to internet. Client is given assignment as it is CP bypass profile.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Mac-Filtering Failed, But trying to accept the Wireless Client for Cp Bypass <00:40:96:ad:d4:3c>	MAC filtering has failed and client has to go through CP authentication to get access to internet. Client is given assignment as it is cpbypass profile.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Mac-Filtering is Success and Captive Portal is Bypassed for Wired Client <00:40:96:ad:d4:3c>	Wired client has connected to a captive portal bypass profile; MAC filtering is successful and client bypasses CP.	Informative
2017-Oct-10 08:02:49.056279 | 00:40:96:ad:d4:3c | Mac Filtering | Mac-Filtering is Success and Captive Portal is Bypassed for Wireless Client <00:40:96:ad:d4:3c>	Wireless client has connected to a captive portal bypass profile; MAC filtering is successful and client bypasses CP.	Informative

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.