



Integrating External Captive Portal with cnMaestro API



Table of contents

Chapter 1 Contents

Revision History.....	Error! Bookmark not defined.
Introduction.....	3
API supported (Login and Logout).....	4
Feature Details	5
Workflow.....	6
Configuration	7
Client connection of through Swagger API	9
Workflow in detail.....	9
Client login	9
Status codes and their details.....	11
Client logout.....	12
Debugging and Troubleshooting.....	14
Login Logs	15
Logout logs	15

Note: This document is applicable for both On-premises and Cloud cnMaestro version

Please refer the cnMaestro API document for more details on API infrastructure.

Introduction

Guest access WLAN is designed specifically for BYOD (Bring your own device) setup, where large organizations have both staff and guests running on same WLAN or similar WLANs. Cambium Networks Provides different options to the customers to achieve this based on where the **captive portal page is hosted** and **who will be validating and performing authentication process**.

They are 3 locations where the captive portal page can be hosted:

1. Internal Access Point (Limited customization like Logo and Background Image)
2. **External Hotspot (External 3rd party Web/Cloud hosted captive portal, fully customized)**
3. cnMaestro (Semi customized portal, with additional features like SMS Authentication, Payment Gateways and Vouchers)

Authentication Methods:

1. Clickthrough (Portal page with a button to accept terms & conditions and get internet access)
2. **RADIUS (External Authentication server like, Windows NPS / IAS or Free RADIUS)**
3. LDAP (Authenticate using LDAP/Active Directory)
4. Local Guest Account (Single username /password stored on Access Point)

In this document, we will be specifically talking about **External Hotspot** integrating with both on-premises and cloud version of cnMaestro to securely **POST** the user credentials to authenticate the user using **External RADIUS**

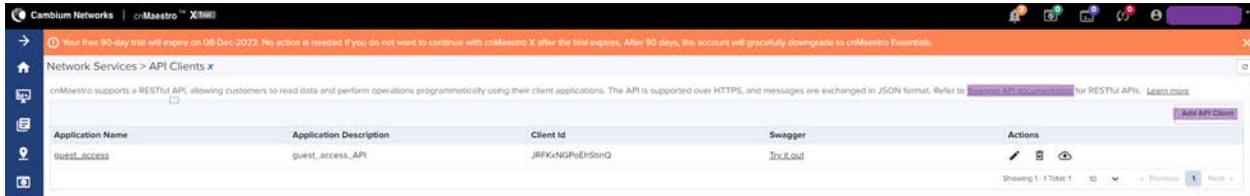
Since the secure **POST** needs a secure connection between cnMaestro and the Web server. RESTful API support on the cnMaestro server will facilitate the webserver to POST user credentials to cnMaestro securely.

An AP client should be added in the Network services >> RESTful API section of the cnMaestro and the API client id and secret should be added in the server from where the POST message will be triggered. (For more information on API client creating,

please refer cnMaestro RESTful API document
<https://docs.cloud.cambiumnetworks.com/api/3.1.0/index.html>)

How to create an API client and swagger documentation are available in cnMaestro network services section.

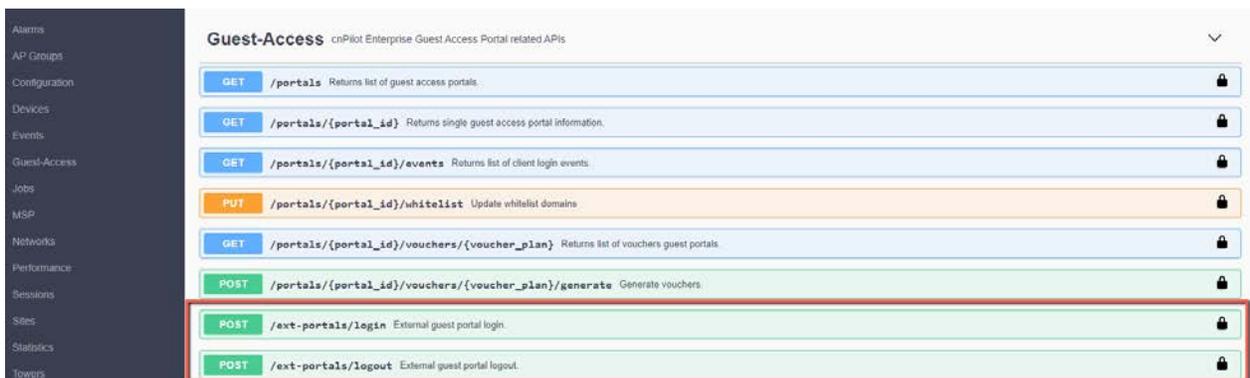
Please refer the screenshot below



API client creation and swagger documentation

Note: RESTful API is a licensed feature and need cnMaestro-X software for configuration.

API supported (Login and Logout)



Feature Details

Customers who wanted a secure communication channel to authenticate the user securely should choose to POST the user credentials to cnMaestro. To enable this feature, one must enable **External Portal Post Through cnMaestro** available in Guest Access.

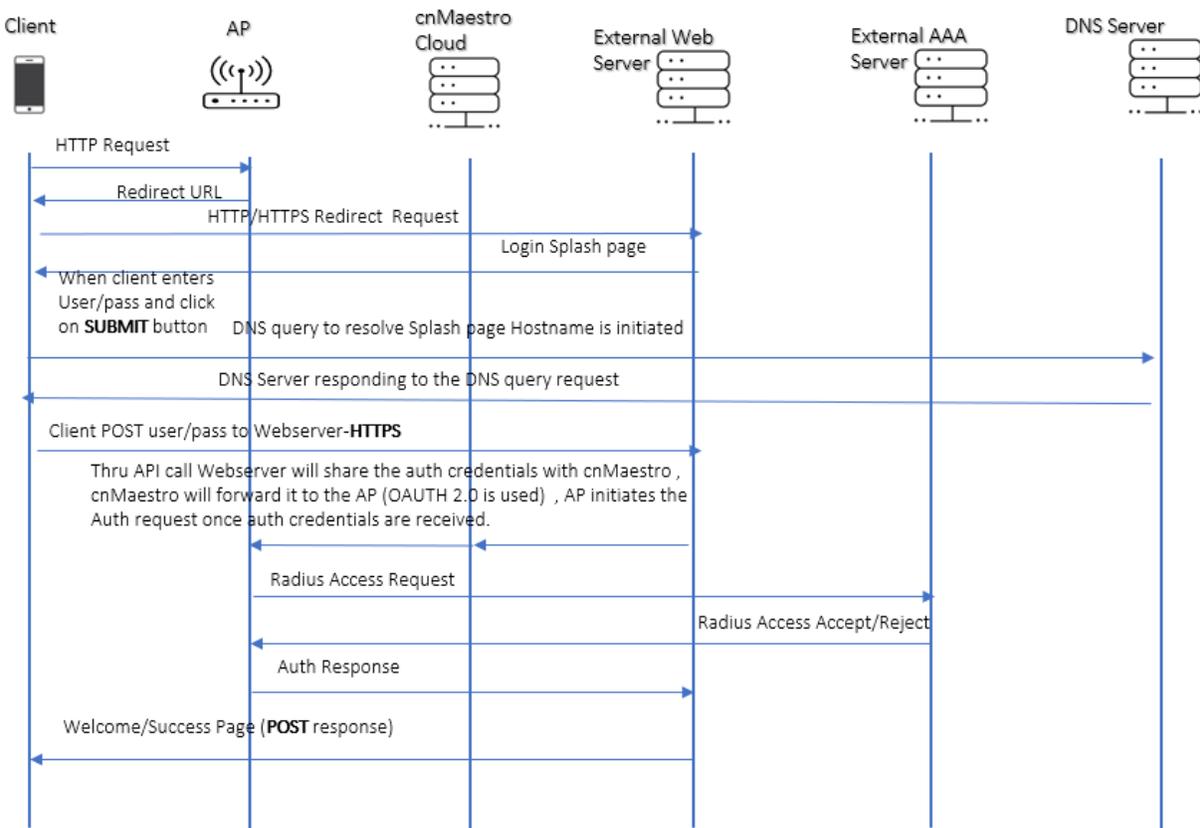
The screenshot displays the configuration page for **WLANs > Cloud_Guest_Access**. The left sidebar shows a navigation menu with options: Configuration, APs, WLAN, AAA Servers, Guest Access (selected), Access Control, Passpoint, and ePSK. The main content area is titled **Basic Settings** and includes the following configuration options:

- Enable:** Enable
- Portal Mode:** Internal Access Point, External Hotspot, cnMaestro
- Access Policy:** Clickthrough (Splash page where users accept terms and conditions to get on the network), RADIUS (Splash page with username and password, authenticated with a RADIUS server), LDAP (Redirect users to a login page for authentication by a LDAP server), Local Guest Account (Redirect users to a login page for authentication by local guest user account)
- AP Server Protocol:** HTTP (Use unsecured HTTP protocol for AP guest access server), HTTPS (Use secured HTTPS protocol for AP guest access server)
- Redirect Hostname:** Redirect Hostname for the splash page (up to 255 characters)
- WISPr Clients External Server Login
- External Page URL*:**
- External Portal Post Through cnMaestro
- External Portal Type:** External Portal Type Standard/XWF

Guest Access UI Screenshot:

Workflow

A general workflow when an external webserver and cnMaestro cloud is configured to accept **HTTPS POST** messages from client.



This setup consists of below main parts:

1. Supplicant (Wireless clients- Laptops, mobile phones etc)
2. External Web Server
3. DNS server
4. cnMaestro
5. Authenticator (Cambium Access Point)
6. Authentication Server (RADIUS)

Configuration

1. On cnPilot Access Points: Configure >> WLAN
2. On cnMaestro: Shared Settings/ WLANs and AP Groups >> WLANs

WLAN: Key in the **WLAN name** and **description**. By default, WLAN Name is taken as **SSID Name**.

The screenshot shows the configuration page for a WLAN named 'Cloud_Guest_Access'. The left sidebar lists various configuration categories: WLAN, AAA Servers, Guest Access, Access Control, Passpoint, and ePSK. The main content area is divided into two sections: 'Basic Information' and 'Basic Settings'. In 'Basic Information', the 'Type' is set to 'Enterprise Wi-Fi', the 'Name' is 'Cloud_Guest_Access', and the 'Description' is 'Common SSID'. In 'Basic Settings', the 'SSID' is 'enable', the 'SSID*' is '@@@Guest_Access_Cloud@@@', the 'Mesh' is 'Off', the 'VLAN*' is '10', the 'Security' is 'Open', and the 'Radios' are '2.4 GHz and 5 GHz'. Each field has a small text description to its right.

AAA Server: Key in the AAA server setting like **IP address (RADIUS server)** and **shared secret** (This shared secret should match to the secret created on RADIUS server).

The screenshot shows the configuration page for AAA Servers for the WLAN 'Cloud_Guest_Access'. The left sidebar lists configuration categories: WLAN, AAA Servers, Guest Access, Access Control, Passpoint, and ePSK. The main content area shows a warning: 'Warning: AAA Servers are configured separately for each WLAN.' Below this is the 'Authentication Server' section. It contains three rows for adding AAA servers, each with a 'Host' field and a 'Secret' field with a 'Show' button. The first row has '10.10.130.202' in the Host field. Below the rows are 'Timeout' and 'Attempts' fields. The 'Timeout' field is set to '3' and the 'Attempts' field is set to '1'. Each field has a small text description to its right.

Guest Access: Enter the URL of captive portal hosted on external web server and select other required parameters.

Note: If **cnMaestro On-Premises** is used for integration, please add the **cnMaestro URL/IP address** in the **whitelist**

Example External page URL

1. IP address: http://10.110.200.100:8000/login_cnMaestro.html
2. URL : <https://dev.xyznetworkmanager.com/portal/index.php?hotspotname=laCambium>

The external Page URL should contain a script running in it which will capture the information (user/pass) user enters and POST it back to the 3rd party webserver.

Client connection of through Swagger API

Workflow in detail

In normal case when cloud API is used, when a wireless client connects to the AP, AP will redirect the client to the configured external 3rd party captive portal server. Client will fetch the splash page from the external 3rd party server and provide the user/pass to get authenticated. This user/pass information is captured by the webserver through a script and the API server running on the webserver POST this to the cnMaestro. Up on receiving the information through API's, cnMaestro will forward this to the AP and AP will initiate an authentication request to the AAA server. This flow is explained below through swagger API (inbuilt application available in cnMaestro).

Client login

Step 1: client connects to the AP and gets redirected to the splash page.

Client will be in non-authenticated state now on the AP.

Login to the cnMaestro and access swagger API, and go to Guest Access POST section of */api/v2/ext-portals/login*

Access the swagger API and key in the

AP MAC address	"ga_ap_mac"
Client MAC address	"ga_cmac"
Signature	"ga_Qv"
Username	"ga_user"
Password	"ga_pass"

Above details manually on the request body section. These details can be copied from the URL which is presented to the client by the webserver.

A sample URL is given below for reference.

```
http://10.110.130.202:8000/login.html?ga_ssid=%40%40%40Guest_Access_Cloud%40%40%40&ga_ap_mac=58-C1-7A-29-86-0C&ga_nas_id=E600-29860C&ga_srvr=ap-ne1-guest.cloud.cambiumnetworks.com&ga_cmac=E4-A7-A0-D4-31-C2&s=1NOF3YCYgA7w0lOw2W_wfQkQ3oa0VCbFjYPzljCpK5IA.&ga_Qv=eUROBR86HBgAGDEEVgQAGw4UWRUCACYVMgFPRy5ZXIFfUSVGWS9FVghZRyRLBhMUMww.
```

POST /ext-portals/login External guest portal login

Integrates external captive portal with the cambium AP while posting directly to cnMaestro. This API provides the support for the external captive portal to make login request.

Parameters Cancel

No parameters

Request body *required* application/json

```
{
  "ga_ap_mac": "54:00:04:00:00:00",
  "ga_cmac": "E4:00:04:00:00:00",
  "ga_qv": "eduroam",
  "ga_user": "anand",
  "ga_pass": "anand@123"
}
```

Execute

Responses

Code	Description	Links
200	OK	No links
400	Bad Request	No links
404	Not Found	No links
422	Request params are malformed	No links
5XX	Unexpected error	No links

Swagger API login request screenshot

Once all the requisite fields are keyed-in click on execute for swagger API to post this message to the cnMaestro.

Once execute is clicked, cnMaestro will receive this info and forward to the AP for authentication.

Responses

Curl

```
curl -X POST "https://ap-ne1-s1-epkfkdyg1.cloud.cambiumnetworks.com/api/v2/ext-portals/login" -H "accept: */*" -H "Authorization: Bearer f854b3568a96d4e64bb92bae84f8e9bee9150832" -H "Content-Type: application/json" -d "{\"ga_ap_mac\":\"5C2A\", \"ga_ov\":\"eUR\", \"ga_mac\":\"E-UMW\", \"ga_user\":\"anand\", \"ga_pass\":\"anand@123\"}"
```

Request URL

```
https://ap-ne1-s1-epkfkdyg1.cloud.cambiumnetworks.com/api/v2/ext-portals/login
```

Server response

Code	Details
200	<p>Response body</p> <pre>{ "data": { "atype": 3, "msgid": 28, "status": 0, "prefix0": false, "expiry": 28800, "action": 1, "cac": "4572658f5a04-80", "msg": "4572658f5a04-80", "extURL": "http://10.110.130.202:8000/welcome.html" } }</pre> <p>Response headers</p> <pre>content-encoding: gzip content-security-policy: frame-ancestors 'self' content-type: application/json; charset=utf-8 date: Wed, 26 Jan 2022 11:10:41 GMT ratelimit-limit: 3 ratelimit-remaining: 2 ratelimit-reset: 60 server: nginx vary: X-HTTP-Method-Override, Accept-Encoding x-content-type-options: nosniff x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block</pre>

Responses

Swagger API screenshot after executing done (response)

We can see that the response is 200 OK which means the client is authenticated successfully,

Status codes and their details

Status value as Integer and it's interpretation:

0: Login is successful

1: Invalid login request, the client is not currently associated to the AP which is being requested for login here.

2: RADIUS reject due to invalid username/password

3: RADIUS timeout, AP didn't receive the RADIUS response.

4: Missing RADIUS server config on the WLAN config of the AP.

5: If LDAP configured on the AP for authentication, then LDAP server responded back with reject

6: LDAP timeout happened on the AP for the request

7: Missing LDAP configuration on the WLAN configuration of the AP.

8: Logout is successful

Debugging and Troubleshooting

If the client is not connecting, please go to Tools > Remote CLI on cnMaestro and run `service show client-cache` to verify client is connected

The screenshot shows the Remote CLI interface for device E600-29860C. The command `service show client-cache` has been executed, resulting in the following output:

```
Device > service show client-cache
Internal cache(AI:acct_itrvl, RI:radius srvr idx, HS:guest: CI:non-guest, SESS:session-time, RLU:ratelimit in Mbps
QT: Type and unit, 1=directional,2=directional gigword, 3=total, 4 total gigword; M=MB, G=GB
QLU: quota up limit, QLD: Quota down limit)
IDX]  Hostname[CLIENT-MAC]  VLAN HS CI  SESS EXPIRY RLU RLD QT QLU  QLD AI RI      SSID          MESSID          SESSID
0]  IN01[REDACTED]  0 0 0  0  0 0 0 0  0  0 1800 1  @@@Guest_Access_Cloud@@@ 1B602FDE87E0302CF161 58C17A29860CB61EF161
```

Here one can see that the HS bit is “0” means the client is connected but not authenticated.

Once user/pass is POST to the cnMaestro, “`service show debug-logs wifid live`” will display the authentication logs.

Login Logs

```
Jan 26 18:20:12: lldp frame:dmac 01-80-C2-00-00-0E smac 58-C1-7A-FC-23-67 type 88cc
(lldp.c:89)
Jan 26 18:20:36: DA sent[261]: {"id": "12c323710e124693b5f12e7c3ec3fb50-W0", "msgId": 27, "ga_ap_mac": "58-C1-7A-29-86-0C", "ga
Jan 26 18:20:36: From cnmaestro rcvcd msg type[27], total rcvcd reply count[4] (cache.c:4080)
Jan 26 18:20:36: Ext CP msg sub type[27] received from cnmaestro (cache.c:3960)
Jan 26 18:20:36: EXT CP msg[27] from cnmaestro for client[E4-A7-A0-D4-31-C2] with id[12c323710e124693b5f12e7c3ec3fb50-W0] (cac
Jan 26 18:20:36: Login request received for client[E4-A7-A0-D4-31-C2] (hotspot.c:2232)
Jan 26 18:20:36: req type[0] with ID[12c323710e124693b5f12e7c3ec3fb50-W0] copied to hotspot session for access type[1] (hotspot
Jan 26 18:20:36: RAUTH 10.110.130.202[UP:0], [UP:0], [UP:0] (radius.c:685)
Jan 26 18:20:36: Initiated hotspot auth RADIUS authentication for client[E4-A7-A0-D4-31-C2] to radius server[0]:10.110.130.202
Jan 26 18:20:36: Handling hotspot login request for user[anand] (radius.c:3333)
Jan 26 18:20:36: Hotspot client[E4-A7-A0-D4-31-C2] rad acct sess id[58-C1-7A-29-86-0C-06-41-F1-61-E4-A7-A0-D4-31-C2] (radius.c:
Jan 26 18:20:36: Sending RADIUS authentication for client[E4-A7-A0-D4-31-C2] to radius server[10.110.130.202] (radius.c:3103)
Jan 26 18:20:36: Initiate hotspot radius exchange sta[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] using FD[43] (radius
Jan 26 18:20:36: RADIUS Server IP [10.110.130.202] (radius.c:3154)
Jan 26 18:20:36: Process RADIUS response for client[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] (radius.c:1432)
Jan 26 18:20:36: Client[E4-A7-A0-D4-31-C2] WG state[unknown] (radius.c:1154)
Jan 26 18:20:36: RADIUS[10.110.130.202] success for client[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] (radius.c:1613)
Jan 26 18:20:36: Hotspot Client[E4-A7-A0-D4-31-C2] on vlan[10] traffic policy skipped; dyn_vlan[0] (cache.c:810)
Jan 26 18:20:36: process RADIUS auth response code 2 for hotspot sta[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] (radi
Jan 26 18:20:36: process RADIUS response code 2 for hotspot sta[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] (radius.c:
Jan 26 18:20:36: hotspot_handle_radius_response is 2 (hotspot.c:2635)
Jan 26 18:20:36: RADIUS provided session time[0], idle timeout[0], reply-msg=2e7c3ec3fb50-W0 (hotspot.c:2636)
Jan 26 18:20:36: radio_idx=1, bss_idx=0, APD_NUM_RADIOS=2, APD_NUM_BSS_PER_RADIO=16 (apd.c:589)
Jan 26 18:20:36: client[E4-A7-A0-D4-31-C2] hostapd wlan=10 and wlan wlan=10 (cache.c:1841)
Jan 26 18:20:36: client[E4-A7-A0-D4-31-C2] on ssid @@@Guest_Access_Cloud@@@ wlan 10 state sync (type:2) sent, len[704] (cache.
Jan 26 18:20:36: client[E4-A7-A0-D4-31-C2] hotspot session updated ga_allowed[1] to coplane (hotspot.c:416)
Jan 26 18:20:36: Client[E4-A7-A0-D4-31-C2] EXT CP reply to controller for id[12c323710e124693b5f12e7c3ec3fb50-W0], status_code[
Jan 26 18:20:36: Sent ctrl ext cp login rsp for client[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] (cache.c:262)
Jan 26 18:20:36: Setup rate limit up[0] down[0] for client[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] (radius.c:1732)
Jan 26 18:20:36: client[E4-A7-A0-D4-31-C2] custom per client rate limit not in use, skip update to coplane (radius.c:516)
Jan 26 18:20:36: RADIUS exchange completed for client[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] closing FD[43] (radi

Jan 26 18:20:42: lldp frame:dmac 01-80-C2-00-00-0E smac 58-C1-7A-FC-23-67 type 88cc
(lldp.c:89)

E600-29860C(config)# service show client-cache
Internal cache(AI:acct_itrvl, RI:radius srvr idx, HS:guest: CI:non-guest, SESS:session-time, RLU:ratelimit in Mbps
QT: Type and unit, I=directional,2=directional gigword, 3=total, 4 total gigword; M=MB, G=GB
QLU: quota up limit, QLD: Quota down limit)
IDX] Hostname[CLIENT-MAC] VLAN HS CI SESS EXPIRY RLU RLD QT QLU QLD AI RI SSID MESSID SESSID
0] IN01[E4-A7-A0-D4-31-C2] 10 1 0 28800 28784 0 0 0 0 0 1800 1 @@@Guest_Access_Cloud@@@ A95ABR29B9EB9C43F161 58C17A29860C0641F161
```

Once the client is connected look for the HS bit set to “1” which indicates that the client is authenticated and data ready state.

Logout logs

```
E600-29860C(config)#
E600-29860C(config)# service show debug-logs wifid live
Jan 26 18:20:36: Sent ctrl ext cp login rsp for client[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] (cache.c:262)
Jan 26 18:20:36: Setup rate limit up[0] down[0] for client[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] (radius.c:1732)
Jan 26 18:20:36: client[E4-A7-A0-D4-31-C2] custom per client rate limit not in use, skip update to coplane (radius.c:516)
Jan 26 18:20:36: RADIUS exchange completed for client[E4-A7-A0-D4-31-C2] on ssid[@@@Guest_Access_Cloud@@@] closing FD[43] (radi
Jan 26 18:20:42: lldp frame:dmac 01-80-C2-00-00-0E smac 58-C1-7A-FC-23-67 type 88cc
(lldp.c:89)
Jan 26 18:20:55: radio0 intr num 49 intr cnt 226548 (main.c:1529)
Jan 26 18:20:55: radiol intr num 231 intr cnt 68917 (main.c:1529)
Jan 26 18:20:55: Loudest neighbours on 2.4GHz band (autocell.c:263)
Jan 26 18:20:55: Loudest neighbours on 5GHz band (autocell.c:263)

Jan 26 18:21:09: DA sent[217]: {"id": "4396d1eeae0349cb80f22fdd0c8a36e4-W0", "msgId": 29, "ga_ap_mac": "58-C1-7A-29-86-0C", "ga
Jan 26 18:21:09: From cnmaestro rcvcd msg type[29], total rcvcd reply count[5] (cache.c:4080)
Jan 26 18:21:09: Ext CP msg sub type[29] received from cnmaestro (cache.c:3960)
Jan 26 18:21:09: EXT CP msg[29] from cnmaestro for client[E4-A7-A0-D4-31-C2] with id[4396d1eeae0349cb80f22fdd0c8a36e4-W0] (cac
Jan 26 18:21:09: Logout request received for client[E4-A7-A0-D4-31-C2] (hotspot.c:2232)
Jan 26 18:21:09: client[E4-A7-A0-D4-31-C2] acct stop; acct running[0], roamed away[0] (radius.c:3823)
Jan 26 18:21:09: client[E4-A7-A0-D4-31-C2] crx[0];otrx[0], otx[0];orx[0], ntx[28];nrx[38] (wifi_stats.c:97)
Jan 26 18:21:09: radio_idx=1, bss_idx=0, APD_NUM_RADIOS=2, APD_NUM_BSS_PER_RADIO=16 (apd.c:589)
Jan 26 18:21:09: client[E4-A7-A0-D4-31-C2] hostapd wlan=10 and wlan wlan=10 (cache.c:1841)
Jan 26 18:21:09: client[E4-A7-A0-D4-31-C2] on ssid @@@Guest_Access_Cloud@@@ wlan 10 state sync (type:2) sent, len[704] (cache.
Jan 26 18:21:09: client[E4-A7-A0-D4-31-C2] hotspot session updated ga_allowed[0] to coplane (hotspot.c:416)
Jan 26 18:21:09: Client[E4-A7-A0-D4-31-C2] EXT CP reply to controller for id[4396d1eeae0349cb80f22fdd0c8a36e4-W0], status_code[
Jan 26 18:21:09: Sent ctrl ext cp logout rsp for client[E4-A7-A0-D4-31-C2] on ssid[@@@] (cache.c:262)

Jan 26 18:21:12: lldp frame:dmac 01-80-C2-00-00-0E smac 58-C1-7A-FC-23-67 type 88cc
(lldp.c:89)

E600-29860C(config)# service show client-cache
Internal cache(AI:acct_itrvl, RI:radius srvr idx, HS:guest: CI:non-guest, SESS:session-time, RLU:ratelimit in Mbps
QT: Type and unit, I=directional,2=directional gigword, 3=total, 4 total gigword; M=MB, G=GB
QLU: quota up limit, QLD: Quota down limit)
IDX] Hostname[CLIENT-MAC] VLAN HS CI SESS EXPIRY RLU RLD QT QLU QLD AI RI SSID MESSID SESSID
0] IN01[E4-A7-A0-D4-31-C2] 0 0 0 0 0 0 0 0 0 0 0 1800 1 @@@Guest_Access_Cloud@@@ A95ABR29B9EB9C43F161 58C17A29860C0641F161
```

Once the client is disconnected look for the HS bit set to “0” which indicates that the client is not in authenticated state