Accepted Syslog Formats From Wireless APs

https://campus.barracuda.com/doc/67176482/

This article includes examples from specific wireless AP devices Barracuda Networks has tested from which the Barracuda Web Security Gateway can accept syslog data. Since the manufacturers of these devices may change the format from time to time, Barracuda Networks recommends consulting with your device manufacturer to verify the current syslog output format.

The only fields required in syslog output from wireless AP devices by the Barracuda Web Security Gateway are shown in bold face. These fields identify the wireless AP device and the user for the syslog on the Barracuda Web Security Gateway.

- Meru
- Ruckus and Ruckus Cloudpath
- Aerohive
- Aruba
- Clearpass
- Cisco
- Cisco Aironet
- Cisco Meraki

Example syslog format for Meru

ALARM: 1388445713l | system | info | ALR | Station Info Update : MAC-Address : 74:e5:0b:b9:63:46, **User-Name**: dnoble, AP-Id: 1, AP-Name: Meru-AP, BSSID: 00:0c:e6:02:86:ae, ESSID: Meru, IP-Type: discovered, **IP-Address**: 184.15.21.123, L2-Mode: 802.1x, L3-Mode: clear, Vlan-Name: None, Vlan-Tag: 0

Example syslog formats for Ruckus

Format 1, for Ruckus:

Mar 3 18:32:13 stamgr: stamgr_send_log_v4():operation=add;seq=3;**sta_ip**=10.1.0.123;sta_mac=d8:30:62:8b:71:e0;zd/ap=24:c9:a1:24:ae:c8/54:3d:37:29:c2:a0;sta_ostype=iOS;**sta_name**=adnoble;stamgr_handle_remote_ipc

Format 2, for Ruckus Cloudpath:

ts=20171013 164450.444, lvl=FINE, action=RAD ACCOUNTING, radAcctType=Start, accountPk=1, **radClientIp=10.100.38.10**, radSessionId=59E0ED6B-37113000, **radUsername=bstrohm**, radClientMac=28:B2:BD:FB:27:FA, src=service.RadiusConnectionService

Example syslog format for Aerohive

INFO AUTH 12/9/2014 11:39:43 AM 10.1.0.184 10.1.0.184 ah_auth: Station 74e5:0bb9:6346 **ip** 10.1.31.123 **username** dnoble hostname BenZ570 OS n/a

Example syslog formats for Aruba

Format 1:

Oct 2 13:02:34 authmgr[3785]: <522008> <NOTI> |authmgr| User Authentication Successful: **username**=dnoble MAC=c4:62:ea:c1:e7:3f **IP**=10.213.50.$i role=ADMON_USER VLAN=15 AP=THE.GYM.1 SSID=CNG_WIRELESS AAA profile=CNG_WIRELESS-aaa_prof auth method=802.1x auth server=RADIUSCNG2"

Format 2:

Jul 25 13:25:25 stm[1454]: <501199> |AP ap-3175w-2f-web@10.7.7.42 stm| User authenticated, mac-18:af:61:5f:0d:27, **username**-rmathews, **IP**-10.6.124.216, method-4, role-affinity

Example syslog format for Clearpass

08-18-2014 10:42:43 Local1.Debug 192.168.100.27 2014-08-18 10:42:42,650 192.168.100.27 For Cuda Grab 78 1 0 **Common.Username**=dnoble,Common.Service=Ancillae_802.1x_Wireless,Common.Roles=Ancillae_FAC_STAFF_STU, [User Authenticated],Common.Host-MAC-Address=e4ce8f1d29de,RADIUS.Acct-Framed-IP-Address=10.50.45.103,**Common.NAS-IP-Address**=192.168.100.27,Common.Request-

Timestamp=2014

Example syslog format for Cisco

Wed Jun 22 07:00:00 COT 2016,""Wed Jun 22 07:00:00 COT 2016"","0s","**ICETEXV2\\apond**","74:46:A0:A4:7A:E7","","**10.1.235.2**","dot1x","PEAP (EAP-MSCHAPv2)","ICTX_WIRED >> ICTX-802.1X-WIRED >> Default","ICTX_WIRED >> ICTX-WIRED-USER","ICTX-PERMIT-ALL","","","","Started","","ictxsrvise1","0A01041B000064AB70CDEAC8","000017A3","10.1.4.27","GigabitEthernet1/0/30","N","0","0","0","0","","RADIUS","icetex.local","","ICETEXV2","",

Example syslog format for CISCO Aironet

wlc1_vabeach-exec_cflag: haSSOServiceTask2: May 17 13:21:41.809: %APF-3-AUTHENTICATION_TRAP: [SS] apf_80211.c:19558 Client Authenticated: MACAddress:9D:74:13:8A:7A:32 Base Radio MAC:9C:74:13:8A:7A:32 Slot:1 **{** }User Name:test_user{**}** ***Ip Address:10.36.1.55** SSID:CFEmployee

Example syslog format for CISCO Meraki

<15>Washworld_Network_wireless events **type=association** radio='1' vap='0' client_mac='B2:F5:0D:23:E9:01' **last_known_client_ip='10.31.132.141'** band='5' channel='44' rssi='43' **identity='qauser1'** aid='1234985199'

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.