

Wi-Fi AP Authentication Aruba Configuration

<https://campus.barracuda.com/doc/46209580/>

To authenticate users connected to Aruba access points, you must stream the syslog containing the authentication data to the Barracuda NextGen Firewall F-Series.

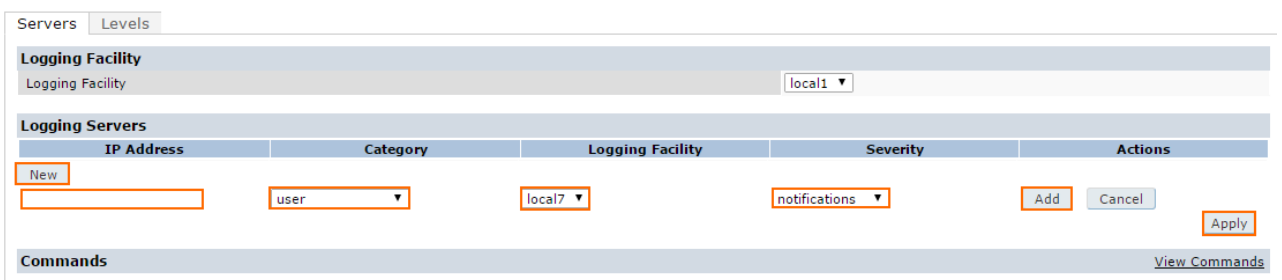
Reference devices/versions:

- Aruba Controller 651 Version 6.4.1.0
- Aruba AP 105
- Aruba Instant

Enable syslog streaming on the Aruba AP

1. Log into the Aruba Mobility Controller.
2. Click the **Configuration** tab.
3. In the **MANAGEMENT** section of the left menu, click **Logging**.
4. In the **Logging Servers** section, click **New**:
 - **IP Address** – Enter the management IP address of the Barracuda NextGen Firewall F-Series.
 - **Category** – Select **user**.
 - **Logging Facility** – Select the logging facility to be able to differentiate between multiple Aruba APs.
 - **Severity** – Select **notifications**.
5. Click **Add**.
6. Click **Apply**

Management > Logging Servers



The screenshot shows the 'Logging Servers' configuration page. At the top, there are tabs for 'Servers' and 'Levels'. Below this, the 'Logging Facility' section has a dropdown menu set to 'local1'. The 'Logging Servers' section contains a table with columns: IP Address, Category, Logging Facility, Severity, and Actions. A 'New' button is next to the table. Below the table, there are input fields for IP Address, a dropdown for Category (set to 'user'), a dropdown for Logging Facility (set to 'local7'), and a dropdown for Severity (set to 'notifications'). There are 'Add', 'Cancel', and 'Apply' buttons. At the bottom, there is a 'Commands' section with a 'View Commands' link.

IP Address	Category	Logging Facility	Severity	Actions
<input type="text"/>	user	local7	notifications	Add Cancel Apply

7. Click the **Levels** tab.
8. Set the **Logging Levels** in the **User logs** section to **notifications**.

<input type="checkbox"/>	User logs	notifications
<input type="checkbox"/>	all	notifications
<input type="checkbox"/>	captive-portal	notifications
<input type="checkbox"/>	vpn	notifications
<input type="checkbox"/>	dot1x	notifications
<input type="checkbox"/>	radius	notifications
<input type="checkbox"/>	voice	notifications
<input type="checkbox"/>	client-match	notifications
<input type="checkbox"/>	mapc	notifications
<input type="checkbox"/>	pan	notifications

9. Click **Apply**.

Verify that the Barracuda NextGen Firewall F-Series is receiving the syslog data

On the Barracuda NextGen Firewall F-Series, go to **LOGS** and open **Box > Control > AuthService_wifiap.log**. After successfully authenticating, you will see a logged in user <username> with IP <IP address> line in the log. The Wi-Fi access point name is also listed.

Box\Control\AuthService_wifiap < new Log >

Select Log File

Time	Type	TZ	Message
2015 09 23 11:00:02	Info	+02:00	[config] protocol: udp
2015 09 23 11:00:02	Info	+02:00	[config] model: aerohive
2015 09 23 11:00:02	Info	+02:00	[config] source-ip: 192.168.0.37
2015 09 23 11:00:02	Info	+02:00	[config] protocol: udp
2015 09 23 11:00:02	Info	+02:00	[config] model: aruba
2015 09 23 11:00:02	Info	+02:00	[config] source-ip: 10.17.133.103
2015 09 23 11:00:02	Info	+02:00	[config] protocol: udp
2015 09 23 11:00:03	Info	+02:00	[main] listening on udp 10.17.133.1:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on tcp 10.17.133.1:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on ssl 10.17.133.1:6514
2015 09 23 11:00:03	Info	+02:00	[main] listening on udp 10.17.76.133:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on tcp 10.17.76.133:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on ssl 10.17.76.133:6514
2015 09 23 11:00:03	Info	+02:00	[main] listening on udp 192.168.0.1:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on tcp 192.168.0.1:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on ssl 192.168.0.1:6514
2015 09 23 11:00:33	Info	+02:00	[auth] udp:10.17.133.103 (type aruba): logged in user user2 with IP 172.17.70.32

Figures

1. aruba01.png
2. aruba_03.png
3. aruba_Logs.png

© Barracuda Networks Inc., 2019 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.