Wireless Access Point Integration With the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/41092783/

The Barracuda Web Security Gateway 310 and above running version 9.0 and above currently supports the following wireless access points (wireless APs) using RADIUS authentication:

- Aerohive
- Aruba
- Cisco AP
- Cisco Meraki
- Cisco Aironet
- Clearpass
- Meru
- Ruckus

The Barracuda Web Security Gateway 310 and above running version 7.x - 8.x currently supports only the Meru and Ruckus wireless access points. For accepted syslog outputs from these devices, see Accepted Syslog Formats From Wireless APs.

Wireless APs have become ubiquitous around corporate and academic campuses. These access points are typically connected to an authentication service such as a RADIUS server, for example, which enables end users to authenticate and gain access to a corporate or campus network. You can integrate one or more wireless APs with the Barracuda Web Security Gateway so that users surf the web as authenticated users after authenticating against their wireless AP. This means that the user only needs to enter their credentials once, and also that they are subject to policies you configure on the Barracuda Web Security Gateway.

Delegated administrators (Read-only, Manage, Monitor, Support) do not have permissions to enable Wireless AP Integration on the Barracuda Web Security Gateway. The **USER/GROUPS** tab is disabled for these users, so this feature is not visible.

How Wireless AP Integration Works

Each wireless AP can be configured to send its syslogs to the Barracuda Web Security Gateway on the network. With Wireless AP Integration enabled, the Barracuda Web Security Gateway listens for system logs coming from each wireless AP, and then parses the data for the username and IP address of the user that logged in. Policies you configure on the Barracuda Web Security Gateway are applied to these users by username, group (if applicable) and/or IP address, and report data reflects username and IP address pairs for all logged web traffic.

How to Configure Wireless AP Integration on the Barracuda Web Security Gateway

Use the following steps to configure all wireless APs to send syslogs to the Barracuda Web Security Gateway.

Go to the **USER/GROUPS > Configuration** page:

1. In the **Access Point Configuration** section, select the wireless provider in the **Access Point Provider** drop-down for the wireless AP that should send logs to the Barracuda Web Security Gateway. The Barracuda Web Security Gateway automatically listens for syslogs from that wireless AP and parses them to authenticate users that log in.
2. Set **Apply Session Parameters to Access Point Logins** to *Yes* if you want to apply session expiration and idle timeouts to wireless access point logins.

Using the manufacturer's instructions, configure your Wireless AP device to stream syslog data containing the authentication information collected to the Barracuda Web Security Gateway. For examples of syslog output from specific wireless AP devices Barracuda Networks has tested, see Accepted Syslog Formats From Wireless APs.

How to Disable Wireless AP Integration

1. Go to the **USER/GROUPS > Configuration** page, and select *None* from the **Access Point Provider** drop-down.
2. The Barracuda Web Security Gateway will stop listening and accepting syslogs from any wireless APs.
3. If there are any users still logged in from the wireless AP, after disabling wireless AP integration, those users remain logged in to the Barracuda Web Security Gateway.

Specific Policies Applied to Groups of Users

When users authenticate to the wireless AP, the username and IP address of the user is forwarded to the Barracuda Web Security Gateway to provide the user a similar browsing experience regardless of the device being used, and without the need to for authenticating to multiple systems. User policies are applied by user name, IP address or group membership as described above, and user data is consolidated for reporting purposes.